

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7670836号
(P7670836)

(45)発行日 令和7年4月30日(2025.4.30)

(24)登録日 令和7年4月21日(2025.4.21)

(51)国際特許分類

F I

H O 4 L 9/08 (2006.01) H O 4 L 9/08 C

H O 4 L 9/32 (2006.01) H O 4 L 9/32 2 0 0 E

G O 6 F 21/44 (2013.01) G O 6 F 21/44

請求項の数 8 (全43頁)

(21)出願番号	特願2023-540650(P2023-540650)	(73)特許権者	524397185
(86)(22)出願日	令和2年12月31日(2020.12.31)		深▲ジェン▼引望智能技術有限公司
(65)公表番号	特表2024-501578(P2024-501578 A)		中国 5 1 8 1 2 9 グアンドン シェン
(43)公表日	令和6年1月12日(2024.1.12)		チェン ロンガン・ディストリクト バン
(86)国際出願番号	PCT/CN2020/142507		ティエン・ストリート ヴァンケ・シテ
(87)国際公開番号	WO2022/141574		イー・コミュニティ ホアウェイ ホアウ
(87)国際公開日	令和4年7月7日(2022.7.7)		エイ・ヘッドクォーターズ・オフィス・
審査請求日	令和5年8月15日(2023.8.15)	(74)代理人	ビルディング ルーム1 0 1
			110004381
			弁理士法人I T O H
		(72)発明者	カン, スク イン
			シンガポール共和国, シンガポール 1
			3 8 5 8 9 ザ・メトロポリス・タワー
			・ 2, # 1 7 - 0 8, 1 1 ノース・ブ
			オナ・ヴィスタ・ドライブ, ファーウェ
			最終頁に続く

(54)【発明の名称】 鍵プロビジョニング方法及び関連製品

(57)【特許請求の範囲】

【請求項1】

第1のデバイスによって実装される鍵プロビジョニング方法であって、前記第1のデバイスは、車両に搭載され、

前記第1のデバイスへのアクセスを要求するアクセス要求を第2のデバイスから受信することと、

前記アクセス要求に基づいて、前記第2のデバイスが前記第1のデバイスへのアクセスを許可されているかどうかを判定することと、

前記判定に基づいて、前記第2のデバイスにアクセス応答を送信することと、

前記第2のデバイスから第1のプロビジョニング・メッセージを受信することであって、前記第1のプロビジョニング・メッセージは、グループ鍵を生成するためのプロビジョニング・データを含み、前記グループ鍵は、前記車両内の第1のデバイス間で共有される、ことと、

前記プロビジョニング・データに従って、グループ鍵を生成することと、を含み、

前記アクセス要求を前記第2のデバイスから受信する前に、

サーバからローカル・プロビジョニング・データを取得することであって、前記ローカル・プロビジョニング・データは、プロビジョニング鍵、公開鍵、及びローカル・タイムスタンプを含み、前記プロビジョニング鍵は、前記グループ鍵を生成するように構成されており、前記公開鍵は、前記第2のデバイスの権限を検証するように構成されており、前記ローカル・タイムスタンプは、前記生成されたプロビジョニング鍵の有効性を検証する

ように構成されている、ことをさらに含む、方法。

【請求項 2】

前記アクセス要求に基づいて、前記第 2 のデバイスが前記第 1 のデバイスへのアクセスを許可されているかどうかを判定することは、

前記アクセス要求がトリガされると、前記第 2 のデバイスの権限を検証するための認証要求を前記第 2 のデバイスに送信することと、

前記認証要求と一致するアクセス・トークンを前記第 2 のデバイスから受信することと、

前記受信したアクセス・トークンが有効であるかどうかを判定することと、を含み、

前記判定に基づいて、前記第 2 のデバイスに前記アクセス応答を送信することは、

前記受信したアクセス・トークンが有効であると判定すると、肯定的なアクセス応答を前記第 2 のデバイスに送信することと、

前記受信したアクセス・トークンが無効であると判定すると、否定的なアクセス応答を前記第 2 のデバイスに送信することと、を含む、請求項 1 に記載の方法。

【請求項 3】

前記プロビジョニング・データは、前記プロビジョニング鍵によって暗号化されたランダム・ストリング、前記プロビジョニング鍵によって暗号化されたプロビジョニング・タイムスタンプ、及び検証署名を含み、

前記プロビジョニング・データに従って前記グループ鍵を生成することは、

前記プロビジョニング鍵を使用して、前記プロビジョニング・データを復号し、前記ランダム・ストリング及び前記プロビジョニング・タイムスタンプを取得することと、

前記ランダム・ストリング及び前記プロビジョニング・タイムスタンプに従って、前記グループ鍵を生成することと、

前記検証署名に従って、前記生成されたプロビジョニング鍵の有効性を検証することと、を含む、請求項 2 に記載の方法。

【請求項 4】

前記アクセス・トークンは、第 1 の事前定義されたアルゴリズムに基づいて生成された検証対象クレデンシャル、検証対象カウンタ、検証対象タイムスタンプ、少なくとも 1 つの検証対象車両アイデンティティ、及び検証対象署名を含み、

前記受信したアクセス・トークンが有効であるかどうかを判定することは、

条件が満たされる場合、前記受信したアクセス・トークンが無効であると判定することであって、前記条件は、ローカル・カウンタ及び前記第 1 の事前定義されたアルゴリズムに基づいて生成されたローカル・クレデンシャル及び第 1 の所定のアルゴリズムが前記検証対象クレデンシャルと不整合であること、前記ローカル・カウンタが前記検証対象カウンタと不整合であること、前記ローカル・タイムスタンプが前記検証対象タイムスタンプよりも遅いこと、第 1 のデバイスが属する車両のアイデンティティが前記少なくとも 1 つの検証対象車両アイデンティティと不整合であること、及び前記検証対象署名を前記公開鍵でチェックすることに失敗することのうちのいずれか 1 つ以上を含む、請求項 3 に記載の方法。

【請求項 5】

前記アクセス・トークンは、車両タイプ、デバイス・タイプ及びデバイス識別子のリストのうちのいずれか 1 つ以上を含む、請求項 4 に記載の方法。

【請求項 6】

前記認証要求は、前記ローカル・カウンタを含み、前記ローカル・カウンタは、前記第 1 のデバイスのプロビジョニング状態を反映するように構成されており、前記カウンタの値は、前記第 1 のデバイスのプロビジョニング状態が変更されると、前記第 1 のデバイスによりプリセットされた規則に基づいて変更される、請求項 4 又は 5 に記載の方法。

【請求項 7】

請求項 1 ～ 6 のいずれか一項に記載の方法を実行するように構成されている第 1 のデバイス。

【請求項 8】

請求項 7 に記載の第 1 のデバイスを含む車両。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、V2X 技術の技術分野に関連し、特に、鍵プロビジョニング方法及び関連製品に関連する。

【背景技術】

【0002】

ビークル・ツー・エブリシング (V2X) は、ビークル・ツー・ビークル (V2V) 通信及びビークル・ツー・インフラストラクチャ (V2I) 通信を指すことがあるが、これは、車両とその周辺環境との間でデータ交換を可能にすることを目的とした無線技術である。

【0003】

V2X 技術に関連する複数のアプリケーションの中で、車両のセキュリティ問題にますます注意が向けられており、これらの問題の 1 つが車両の鍵プロビジョニングであることがある。鍵プロビジョニングとは、車両内のデバイスに初期秘密鍵をセッティングするための特定の作業を表す。鍵プロビジョニング・プロセスは、「鍵セッティング」、「鍵配布」、「鍵初期化」、又は「鍵設定」とも呼ばれることがあるが、鍵は、データの機密性と完全性のために使用されるか、又は他の秘密鍵を保護するために使用される何らかの秘密情報を示唆する。これらの用語は、特に明記しない限り、本明細書において交換可能に使用される。

【0004】

サイバー攻撃の増加に伴い、これらの鍵セッティングが不可欠になっている。特に、すべての車両は、セキュリティへの影響を最小限に抑えるために一意の鍵を持たなければならない。すなわち、たとえ攻撃者が車両の鍵を入手したとしても、他の車両に影響を与えるべきではない。追加的に、現在の車両は、自律走行及びコネクテッドカー機能のための多くのデバイス及びアプリケーションを有し、セキュリティを強化するためにゲートウェイに基づいて分離されたネットワークを有する。したがって、各デバイスに多くの秘密鍵をセッティングする必要がある。

【0005】

この背景技術の情報は、本開示に関係する可能性があるという出願人が信じる情報を明らかにするために提供される。先行する情報のいずれかが本開示に対する先行技術を構成することを必ずしも認めることは意図されていないし、そのように解釈されるべきでもない。

【発明の概要】

【0006】

上記を考慮して、本発明は、上記の課題を解決するために、鍵プロビジョニング方法及び関連製品を提供する。

【0007】

前述の目的及び他の目的は、独立請求項の主題事項によって達成される。さらなる実装は、従属請求項、明細書及び図面から明らかである。

【0008】

本開示の第 1 の態様は、第 1 のデバイスによって実装される鍵プロビジョニング方法であって、第 1 のデバイスは、車両に搭載され、第 1 のデバイスへのアクセスを要求するアクセス要求を第 2 のデバイスから受信することと、アクセス要求に基づいて、第 2 のデバイスが第 1 のデバイスへのアクセスを許可されているかどうかを判定することと、判定に基づいて、第 2 のデバイスにアクセス応答を送信することと、第 2 のデバイスから第 1 のプロビジョニング・メッセージを受信することであって、第 1 のプロビジョニング・メッセージは、グループ鍵を生成するためのプロビジョニング・データを含み、グループ鍵は、車両内の第 1 のデバイス間で共有される、ことと、プロビジョニング・データに従って、グループ鍵を生成することと、を含む、方法に関連する。

【0009】

本開示によって提供される解決策によれば、車両内のすべての第1のデバイス、例えばすべてのECUデバイスに、プロビジョニング・データを含む1つのプロビジョニング・メッセージによってグループ鍵をプロビジョニングすることができる。このようにして、鍵プロビジョニングの効率が改善され、プロビジョニング・コストが低減される。生成されたグループ鍵を使用して、ECUデバイスに関連付けられたデータ通信のセキュリティが確保される。さらに、ECUデバイスにおいて鍵を自己生成することにより、情報が限定されたデータサイズの縮小が達成され、複数のデバイスに対して同時に鍵をセッティングすることも可能である。第1のデバイスは、車両に搭載された任意のデバイスであってもよく、ECUデバイスは、例示的な目的のために一例として解釈されるだけである。また、ここでのグループ鍵は、同じ車両内の第1のデバイス間で共有されるが、車両が異なる第1のデバイスは異なるグループ鍵を有する。

10

【0010】

第1の態様による方法の可能な実装形態では、アクセス要求に基づいて、第2のデバイスが第1のデバイスへのアクセスを許可されているかどうかを判定することは、第2のデバイスの権限を検証するための認証要求を第2のデバイスに送信することと、認証要求と一致するアクセス・トークンを第2のデバイスから受信することと、受信したアクセス・トークンが有効であるかどうかを判定することと、を含み、判定に基づいて、第2のデバイスにアクセス応答を送信することは、受信したアクセス・トークンが有効であると判定すると、肯定的なアクセス応答を第2のデバイスに送信することと、受信したアクセス・トークンが無効であると判定すると、否定的なアクセス応答を第2のデバイスに送信することと、を含む。

20

【0011】

トークンベースの認証は、車両デバイスとKMSサーバとの間のエンドツーエンド・セキュリティを提供するだけでなく、各車両に対する鍵独立性及びKMSの署名からの鍵認証を提供する。

【0012】

第1の態様による方法の可能な実施形態では、方法は、アクセス要求のトリガがあると、第1のプロビジョニング応答を第2のデバイスに送信することと、第2のデバイスから、第1のデバイスに対する機能秘密鍵をプロビジョニングするためのプロビジョニング要求を受信することと、グループ鍵及び事前記憶されたデータに基づいて、機能秘密鍵を生成することと、第2のプロビジョニング応答を第2のデバイスに送信することと、をさらに含む。

30

【0013】

機能秘密鍵は、生成されたグループ鍵に基づいてさらに生成されてもよく、この機能秘密鍵を用いて、何らかの特定のグループ（セキュア・オンボード通信（SecOC）、トランスポート層セキュア（TLS）など、用途又は目的で区別化され得る）の各ECUによる機能秘密鍵の自己生成により、各ECU機器を機能の観点から区別することが可能となり、車両内でセキュア通信においてより柔軟性が提供される。

【0014】

第1の態様による方法の可能な実装形態では、方法は、第3のデバイスから鍵確認チャレンジを受信することと、第2のデバイスから機能秘密鍵が正しく生成されたかを確認するための鍵確認要求を受信すると、鍵確認チャレンジが第3のデバイスによって送信される、ことと、鍵確認チャレンジ、機能秘密鍵、及び第2の事前定義されたアルゴリズムに従って、鍵確認応答を生成することと、鍵確認応答を第3のデバイスに送信することと、をさらに含む。

40

【0015】

ECUデバイスによって機能秘密鍵が生成されるときに、ECUデバイスによって機能秘密鍵が正しく生成されることを確実にするために、生成された機能秘密鍵が、ゲートウェイによって検証されるべきである。

50

【0016】

本開示の第2の態様は、第2のデバイスによって実装される鍵プロビジョニング方法であって、第1のデバイスに第1のデバイスへのアクセスを要求するためのアクセス要求を送信することであって、第1のデバイスは、車両に搭載される、ことと、第1のデバイスからアクセス応答を受信することであって、アクセス応答は、アクセス要求に基づいて第1のデバイスによって返される、ことと、第1のプロビジョニング・メッセージを第1のデバイスに送信することであって、第1のプロビジョニング・メッセージは、第1のデバイスによって、グループ鍵を生成するためのプロビジョニング・データを含み、グループ鍵は、車両内の第1のデバイス間で共有される、ことと、を含む、方法に関連する。

【0017】

第2の態様による方法の可能な実装形態では、方法は、第1のデバイスに第1のデバイスへのアクセスを要求するためのアクセス要求を送信する前に、グループ鍵に対応するアクセス・トークンを要求するためのトークン要求をサーバに送信することであって、トークン要求は、第2のデバイスがプロビジョニングしようとしている複数の車両の1つ以上のアイデンティティを含み、第1のデバイスが属する車両は、複数の車両に含まれる、ことと、サーバから、グループ鍵に対応するアクセス・トークン及びアクセス・トークンに対応する第2のプロビジョニング・メッセージを受信することと、をさらに含む。

【0018】

第2の態様による方法の可能な実装形態では、方法は、第1のデバイスからアクセス応答を受信する前に、第1のデバイスから、第2のデバイスの権限を検証するための認証要求を受信することと、認証要求と一致するアクセス・トークンを判定することと、認証要求と一致するアクセス・トークンを第1のデバイスに送信することと、をさらに含む。

【0019】

第2の態様による方法の可能な実装形態では、認証要求と一致するアクセス・トークンを判定することは、認証要求に従って、第1のデバイスのプロビジョニング状態を判定することと、第1のデバイスのグループ鍵が第1のデバイスによって生成されていないと判定すると、グループ鍵に対応するアクセス・トークンを、認証要求に一致するアクセス・トークンとして使用することと、を含む。

【0020】

第2の態様による方法の可能な実装形態では、第1のデバイスからアクセス応答を受信することは、第1のデバイスから否定的なアクセス応答を受信することを含み、方法は、第1のプロビジョニング・メッセージを第1のデバイスに送信する前に、第1のデバイスのアクセス・トークンを更新するためのトークン更新要求をサーバに送信し、サーバからグループ鍵に対応するアクセス・トークンとして、更新されたアクセス・トークンを受信することをさらに含む。

【0021】

第2の態様による方法の可能な実装形態では、方法は、第1のデバイスから第1のプロビジョニング応答を受信することと、第1のプロビジョニング応答が、グループ鍵が第1のデバイスによって正常に生成されたことを示すときに、第1のデバイスに対して機能秘密鍵をプロビジョニングするためのプロビジョニング要求を送信することと、第2のプロビジョニング応答を第1のデバイスから受信することと、をさらに含む。

【0022】

第2の観点による方法の可能な実装形態では、方法は、第1のデバイスの交換デバイスに対するアクセス・トークンを要求するための要求をサーバに送信することと、サーバから、グループ鍵に対応するアクセス・トークンを受信することと、受信したアクセス・トークンを使用して、交換デバイスをプロビジョニングすることと、をさらに含む。可能な実装形態では、アクセス・トークンは、交換デバイスのアイデンティティを含んでもよく、第2のデバイスが、このアクセス・トークンを使用して交換デバイスにアクセスすることができるようになる。ここで、交換デバイスのプロビジョニングは、第1のデバイスのプロビジョニングと同じように行われてもよい。

10

20

30

40

50

【0023】

第2の観点による方法の可能な実施形態では、方法は、第1のデバイスの機能秘密鍵を更新するための機能秘密アクセス・トークンを要求するための要求をサーバに送信することと、サーバから機能秘密アクセス・トークン及び対応する更新データを受信することと、第1のデバイスの機能秘密鍵を更新することと、をさらに含む。ここで、機能秘密鍵の更新は、第1のデバイスに対する機能秘密鍵のプロビジョニングと同じように行われてもよい。

【0024】

本開示の第3の態様は、サーバによって実装される鍵プロビジョニング方法であって、第4のデバイスから第1のデバイスを設定するための設定要求を受信することであって、設定要求は、第1のデバイスが属する車両のアイデンティティを含み、第1のデバイスは、車両に搭載される、ことと、第4のデバイスにローカル・プロビジョニング・データを送信することであって、ローカル・プロビジョニング・データは、第1のデバイスのグループ鍵を生成するように構成されており、グループ鍵は、車両内の第1のデバイス間で共有される、ことと、を含む、方法に関連する。

【0025】

本開示の第4の態様は、受信モジュール、判定モジュール、送信モジュール及び生成モジュールを含む、車両に搭載される第1のデバイスに関連する。受信モジュールは、第1のデバイスへのアクセスを要求するアクセス要求を第2のデバイスから受信するように構成されており、判定モジュールは、アクセス要求に基づいて、第2のデバイスが第1のデバイスへのアクセスを許可されているかどうかを判定するように構成されており、送信モジュールは、判定に基づいて、第2のデバイスにアクセス応答を送信するように構成されており、受信モジュールは、第2のデバイスから第1のプロビジョニング・メッセージを受信するようにさらに構成されており、第1のプロビジョニング・メッセージは、グループ鍵を生成するためのプロビジョニング・データを含み、グループ鍵は、車両内の第1のデバイス間で共有され、生成モジュールは、プロビジョニング・データに従って、グループ鍵を生成するように構成されている。

【0026】

本開示の第5の態様は、送信モジュール及び受信モジュールを含む第2のデバイスに関連する。送信モジュールは、第1のデバイスに第1のデバイスへのアクセスを要求するためのアクセス要求を送信するように構成されており、第1のデバイスは、車両に搭載され、受信モジュールは、第1のデバイスからアクセス応答を受信するように構成されており、アクセス応答は、アクセス要求に基づいて、第1のデバイスによって返され、送信モジュールは、第1のプロビジョニング・メッセージを第1のデバイスに送信するようにさらに構成されており、第1のプロビジョニング・メッセージは、第1のデバイスによって、グループ鍵を生成するためのプロビジョニング・データを含み、グループ鍵は、車両内の第1のデバイス間で共有される。

【0027】

本開示の第6の態様は、受信モジュール及び送信モジュールを含むサーバに関連する。受信モジュールは、第4のデバイスから第1のデバイスを設定するための設定要求を受信するように構成されており、設定要求は、第1のデバイスが属する車両のアイデンティティを含み、第1のデバイスは、車両に搭載され、送信モジュールは、第4のデバイスにローカル・プロビジョニング・データを送信するように構成されており、ローカル・プロビジョニング・データは、第1のデバイスのグループ鍵を生成するように構成されており、グループ鍵は、車両内の第1のデバイス間で共有される。

【0028】

本開示の第7の態様は、メモリ、プロセッサ、入力インターフェース及び出力インターフェースを含む第1のデバイスに関連する。メモリ、プロセッサ、入力インターフェース、及び出力インターフェースは、バス・システムによって接続されている。メモリは、命令を記憶するように構成されており、プロセッサは、上述した第1の態様の方法又は第1

10

20

30

40

50

の態様の任意の可能な実装を実行するためにメモリに記憶された命令を実行するように構成されている。

【0029】

本開示の第8の態様は、メモリ、プロセッサ、入力インターフェース及び出力インターフェースを含む第2のデバイスに関連する。メモリ、プロセッサ、入力インターフェース、及び出力インターフェースはバス・システムによって接続されている。メモリは、命令を記憶するように構成されており、プロセッサは、上述した第2の態様の方法又は第2の態様の任意の可能な実装を実行するためにメモリに記憶された命令を実行するように構成されている。

【0030】

本開示の第9の態様は、メモリ、プロセッサ、入力インターフェース及び出力インターフェースを含むサーバに関連する。

メモリ、プロセッサ、入力インターフェース、及び出力インターフェースはバス・システムによって接続されている。メモリは、命令を記憶するように構成されており、プロセッサは、上述した第3の態様の方法又は第3の態様の任意の可能な実装を実行するためにメモリに記憶された命令を実行するように構成されている。

【0031】

本開示の第10の態様は、コンピュータ実行可能な命令を記憶するコンピュータ記憶媒体に関連し、このコンピュータ実行可能な命令は、実行されるときに、本開示の第1、第2又は第3の態様及びそれらの任意の可能な実装による方法を実装する。

【0032】

本開示の第11の態様は、命令を含むコンピュータ・プログラム製品に関連し、この命令は、コンピュータ上で実行されるときに、コンピュータに上述の第1、第2若しくは第3の態様又はそれらの任意の可能な実装における方法を実行させる。

【図面の簡単な説明】

【0033】

【図1】本開示の一実施形態によって提供される鍵を示す。

【図2a】本開示の一実施形態による、鍵プロビジョニング・システムを示す。

【図2b】本開示の一実施形態による、図2aに示す鍵プロビジョニング・システムに関する一般的なプロビジョニング・プロセスを示す。

【図3a】本開示の一実施形態による、鍵プロビジョニング方法における第1のデバイス設定の概略フローチャートを示す。

【図3b】本開示の一実施形態による、鍵プロビジョニング方法における第1のデバイス設定の概略フローチャートを示す。

【図4a】本開示の一実施形態による、鍵プロビジョニング方法における第2のデバイス設定の概略フローチャートを示す。

【図4b】本開示の一実施形態による、鍵プロビジョニング方法における第2のデバイス設定の概略フローチャートを示す。

【図5】本開示の一実施形態による、鍵プロビジョニング方法における自己鍵生成の概略フローチャートを示す。

【図6a】本開示の一実施形態による、鍵プロビジョニング方法における自己鍵生成の概略フローチャートを示す。

【図6b】本開示の一実施形態による、鍵プロビジョニング方法における自己鍵生成の概略フローチャートを示す。

【図6c】本開示の一実施形態による、鍵プロビジョニング方法における自己鍵生成の概略フローチャートを示す。

【図7a】本開示の一実施形態による、機能秘密鍵の生成の概略フローチャートを示す。

【図7b】本開示の一実施形態による、機能秘密鍵の例を示す。

【図8】ECUデバイスにおける自己鍵生成器の例示的な構造を示す。

【図9a】本開示の一実施形態による、鍵プロビジョニング方法におけるトークンベース

10

20

30

40

50

認証の概略フローチャートを示す。

【図 9 b】本開示の一実施形態による、鍵プロビジョニング方法におけるトークンベース認証の概略フローチャートを示す。

【図 1 0】本発明の一実施形態による、アクセス・トークンの例示的な構造を示す。

【図 1 1】E C U デバイス又はゲートウェイのための認証ロジックを示す。

【図 1 2】本開示の一実施形態による、認証及び認可の検証のための例示的なプロセスを示す。

【図 1 3】ディーラーシップ・プロビジョニング・ツールの例示的な使用例を示す。

【図 1 4】ディーラーシップ・プロビジョニング・ツールの例示的な使用例を示す。

【図 1 5】本開示の一実施形態による、第 1 のデバイスの概略構造図を示す。

10

【図 1 6】本開示の一実施形態による、第 2 のデバイスの概略構造図を示す。

【図 1 7】本開示の一実施形態による、サーバの概略構造図である。

【図 1 8】本開示の一実施形態による、第 1 のデバイスの概略ブロック図である。

【図 1 9】本開示の一実施形態による、第 2 のデバイスの概略ブロック図である。

【図 2 0】本開示の一実施形態による、サーバの概略ブロック図である。

【発明を実施するための形態】

【0 0 3 4】

以下の説明では、本開示の一部を形成し、かつ本開示の実施形態の特定の態様又は本開示の実施形態が使用され得る特定の態様を例示として示す添付の図面を参照する。本開示の実施形態は、他の態様で使用され、かつ図に示されていない構造的又は論理的要素を含んでもよいことが理解される。したがって、以下の詳細な説明は、限定的な意味で解釈されるべきではなく、本開示の範囲は、添付の特許請求の範囲によって定義される。

20

【0 0 3 5】

背景技術の部分で説明したように、車両における電子制御ユニット（E C U）装置に対する鍵プロビジョニングは非常に重要である。秘密鍵は、攻撃者がチャンネルを盗聴し、任意のメッセージを操作するから保護するとともに、基本的なシステムセキュリティを提供する。秘密鍵のセキュリティ・カバレッジは、以下が含む（が、これらに限定されない）。

【0 0 3 6】

1) 車両内外の通信セキュリティ：E C U デバイス間、又はセキュアな接続、具体的には、セキュアなオンボード通信（S e c O C）及びトランスポート層セキュリティ（T L S）／データグラム・トランスポート層セキュリティ（D T L S）を確立するための秘密鍵を使用したメッセージ暗号化及び認証。

30

【0 0 3 7】

2) システム及びソフトウェアの完全性チェック：ファームウェア又はブートローダを検証することによる秘密鍵を使用したリモート認証、又はセキュアな無線アップデート及びセキュアな再プログラミングのためのバンドル復号の更新及び完全性チェック。

【0 0 3 8】

上記のアプリケーション・シナリオは、単に本開示の実施形態を例示することを目的とし、その限定として解釈されるべきではないと留意されたい。

【0 0 3 9】

40

鍵プロビジョニングを目的とした様々な既存の解決策がある。具体的には、既存の解決策は、「単一のデバイス」への一意鍵のプロビジョニングに焦点を当てている。鍵プロビジョニング方式では、メッセージの送信者と受信者の両方によって共有及び使用される対称鍵を使用して、メッセージを暗号化及び復号する。鍵生成サーバは、ハードウェア・デバイスに対してランダムなデバイス一意鍵を選択し、ハードウェア・デバイスのみがデバイス一意鍵を復号できるように、各ハードウェア・デバイスに埋め込まれた共通鍵でデバイス一意鍵を暗号化する。すべてのデバイスが異なる鍵を持っているため、サーバは、多くのデバイスに対して異なる暗号化されたメッセージを作るべきである。

【0 0 4 0】

別の解決策は、オンチップ・キーの想定に依存し、これは、チップ製造業者によって暗

50

号化された形態でセキュアな場所にプロビジョニング鍵を保存する。したがって、前の製造ステップで事前に保存された他の鍵に依存する。プロビジョニング鍵自体は、オンチップ鍵で暗号化され、暗号化された形態で「デバイス製造業者」に暗号化された形態で送信され得る。したがって、このプロビジョニング鍵は、「プロセッサ製造業者」によって決定される。

【0041】

既存の解決策は、デバイス製造業者に焦点を当てて、独自のプロビジョニング鍵をセッティングする方法を提供しているが、我々の新しいアイデアは、「車両メーカ」に焦点を当てて、自己鍵生成に基づいて車両上の多くのデバイスに車両鍵をセッティングする方法を提供する。したがって、既存の解決策は、我々の解決策が実行される前の早い段階で採用され得る。サプライヤ製造の既存の方法を取って、車両を製造する前にプロビジョニング鍵を各ECUデバイスに記憶することができる。

10

【0042】

しかしながら、既存の解決策は、独自の制限を有する。例えば、以下のようである。

【0043】

1) それらは、1つのデバイスに対して展開される。

【0044】

時間は、車両製造システムにおいて最も重要なものの1つであるからである。それが多くのデバイスを有する車両に展開される場合、各デバイスのセッティングに多くの時間がかかるだろう。車両側に適用される既存の解決策を改良又は拡張したい場合、時間を節約可能な新しいプロトコル及びシステムが設計されなければならない。

20

【0045】

2) それらは、サーバから各デバイスに対して暗号化された鍵としての鍵配布に基づく。

【0046】

各端末に対して、暗号化された形態を有する多くのメッセージを必要とするため、各端末に対して、暗号化されたメッセージを配布する際の通信トラフィックが増加する。その結果、追加的に遅延が発生する。さらに、管理サーバと中間ツールは、複雑な設定データを管理しなければならない。

【0047】

3) それらは、サーバへの直接オンライン接続が必要

30

【0048】

製造システムは、スケジュールされた時間及びプロセスに従って生産プロセスを正確に実施するものとする。通常、工場は、この種のセキュアな鍵ストレージを持たず、従って、外部のセキュアな鍵サーバに接続する必要がある。各デバイスに対して、新しい鍵を取得するためにリアルタイム接続に依存することは、製造システムが製造中にオンラインサーバに常に確実に接続することを期待することが困難であるため、生産スケジュールには好適ではないことがある。

【0049】

このような問題を目的として、目標は、車両内のデバイス（すなわち、車両内のすべてのECUデバイス）に初期一意グループ鍵を確実にセッティングすることであり、従って、他車両に属する機器はこれらの鍵を知ることができない。この技法は、各車両の各デバイスに対して鍵をセッティングするために多くの時間、及び埋め込まれたデフォルト鍵や所望の鍵などのデバイス状態が異なる複雑な鍵管理プロトコルを必要とする。さらに、ロットサプライヤからデバイス情報を収集し管理するためには、面倒な管理システムが必要である。車両におけるデバイスは、ECUデバイス以外のデバイスであってもよく、これは、本開示において限定されないことに留意されたい。

40

【0050】

本開示は、鍵プロビジョニング方法及び関連製品を提供する。第1に、本開示は、車両のECUデバイスに鍵をセキュアにプロビジョニングする方法と、プロビジョニング・ツ

50

ール、システム、及び受信したメッセージを検証する認証方法とを提供し、それによりセキュアな鍵セッティング（認証された鍵プロビジョニング）を達成する。第2に、本開示は、車両のすべてのデバイスに対して1つのメッセージを用いて鍵の自己生成を使用する。多くのデバイス及び多くの車両に展開されている場合でも、トラフィック・オーバーヘッド並びにネットワーク伝送及び動作の遅延を低減し、それにより最小レイテンシで高速動作を実現するのに役立つ。第3に、本明細書で提供される解決策は、車両標準プロトコル上で多くの鍵を展開するためにスケーラブルである。実際、本開示は、プロビジョニング・ツールに対して「トークンベース認証」を適用することによって、サーバへのオンライン接続を必要とせず、オンライン接続に依存することなくECUデバイスにアクセスすることを可能にする。さらに、標準的な自動車プロトコル上で、各車両設定に対してただ1つのみのメッセージを用いてスケーラビリティを提供する。これは、実際の車両生産及びディーラーシップ及びメカニック環境を反映しており、様々な種のシステム及び利害関係者に対して容易な管理が要求される。

10

【0051】

以下、本開示の実施形態は、添付図面を参照して詳細に述べられる。

【0052】

本開示の詳細な実装を述べる前に、本明細書で使用されることがあるいくつか鍵を最初に簡単に説明する。

【0053】

本明細書で説明される方法は、すべてのデバイスが事前共有秘密鍵としてプロビジョニング鍵（PVK）をセキュアに保持し、PVKは、グループ鍵とも呼ばれ、これらの2つの用語は、特に明記しない限り、交換可能に使用されるという想定の下で開始されてもよい。提案した方法により、各ECUデバイスは、1）車両固有秘密鍵（VSK）とも呼ばれるグループ鍵と、2）機能秘密鍵（FSK）の2種の秘密鍵を入手する。

20

【0054】

PVKは、サプライヤ生産を通じてすべてのECUで事前共有され、例えば、それは、サプライヤ側のプロビジョニング・ツールによって注入されてもよい。PVKは、一般に車両製造業者（OEM）から取得されてもよく、PVK配布に関するポリシーは、OEMによって特別に決定され管理され得る。可能な実装では、PVKが車両タイプ又はモデルに従って区別化されると想定する。

30

【0055】

VSKは、車両内の各ECUによって、例えばPVK及びKMS（キー管理システム）から受信した何らかのランダム・ストリングを使用して自己生成される。VSKは、車両ごとに異なる（VINに一意）。

【0056】

FSKは、何らかの特定のグループの各ECUによって、例えばVSK並びに事前定義された特定のストリング及び値を使用して自己生成される。そのグループは、セキュアなオンボード通信（SecOC）及びトランスポート層セキュリティ（TLS）など、その用途又は目的によって区別化され得る。

【0057】

OEMの公開鍵（キー管理システム（KMS）のための）は、受信したプロビジョニング・データを検証するために使用される。

40

【0058】

図1に示すように、車両1のデバイスでは、すべてのデバイスがVSK1を共有し、デバイスは2つのグループに分割され、各グループがFSK、すなわち、FSK1及びFSK2を所有し、車両2のデバイスでは、すべてのデバイスがVSK2を共有し、これらのデバイスに対してFSKはプロビジョニングされていない。VSKは、車両によって異なるため、VSK1は、VSK2に等しくない。

【0059】

図2aは、本開示の一実施形態による、鍵プロビジョニング・システムを示し、図2b

50

は、本開示の一実施形態による、図 2 a に示す鍵プロビジョニング・システムに関する一般的なプロビジョニング・プロセスを示す。

【0060】

図 2 a に示すように、鍵プロビジョニング・システムは、OEM KMS、サプライヤ工場プロビジョニング・システム、及び車両側のプロビジョニング・ツールを含む 3 つの主要なパーティからなり得る。最初に、KMS は、プロビジョニング・メッセージを生成する役割を有する。プロビジョニング・ツールは、このメッセージをデバイスに伝送する役割を果たす。プロビジョニング・ツールは、鍵に関するいかなる情報も有さないため、ツールがデバイスにセキュアにアクセスすることはない。「アクセス・トークン」は、プロビジョニング・ツールが車両のデバイスへのアクセスを獲得することを可能にする。それは、KMS によっても提供され、鍵セッティングに対してのみ一度だけ使用することができる。すべてのデバイスは、「カウンタ」値を用いて現在のプロビジョニング状態をチェックでき、この値は、鍵プロビジョニング状態が変更されるたびに増加する。カウンタとアクセス・トークンについては後の部分で説明される。

【0061】

KMS は、プロビジョニング・ツールを設定するだけでなく、ECU デバイスを設定することも担当する。サプライヤ側では、ECU デバイスは、ECU 生産中（サプライヤ生産段階）にサプライヤ工場プロビジョニング・システムで設定される。プロビジョニング・ツールは、デバイス診断のための典型的なデバイス又はプログラムであり、これは、OEM 側の特別化された車両テスト・デバイス、ディーラーシップ診断ツール／スキャナ、又はポータブル・デバイス（携帯電話及びパッド）上で実行されるアプリケーションなどのハードウェア・デバイス又はソフトウェア・プログラムであってもよい。プロビジョニング・ツールは、一般的、これらの前述の鍵について何も知らない。この用語は、説明を容易にするためだけに本明細書で導入されたものであり、プロビジョニング・ツールに特定の制限はない。

【0062】

図 2 b は、システム構成要素及び関係を示す。図において、サプライヤと KMS サーバとの間、及びプロビジョニング・ツールと KMS サーバとの間のセキュア・チャンネルは、例えば既存の技術を使用して確立されると想定される。これらのセキュア・チャンネルの確立は、本開示の焦点ではない。TLS、サプライヤ管理システム（ECU サプライヤ工場プロビジョニング・システム）などのセキュアなチャンネルが少なくともなくてはならないことを想定している。したがって、それらは、第 1 及び第 2 のステップにおいて何らかの情報を共有してもよい。これに関するセキュリティ上の考慮事項については、後のセクションで説明する。また、図 2 b の点線のボックスは、他のパーティから取得した情報を指し、図 2 b の実線のボックスは、事前記憶されたローカル情報を指す。

【0063】

4 種の主要なコンポーネントがある。セキュリティ全体は、プロビジョニング・データ、検証鍵、アクセス・トークンを管理する KMS に依存する。サプライヤ・システム（図 2 a 及び図 2 b に示す ECU サプライヤ工場プロビジョニング・システム）も、特定の情報（キー、タイムスタンプ、車両、デバイスなど）をそれらの製品に注入するためのセキュアなツールを有している。ECU デバイス製品は、プロビジョニング鍵及び自己生成機能をセキュアに保持するために、何らかの保護メモリを有するべきである。例えば、デバイスは、階層ストレージ管理（HSM）又はトラステッド実行環境（TEE）に基づくセキュアなストレージを有するべきである。テスター・ツール（プロビジョニング・ツール／システムとも呼ばれ、これら 2 つの用語は、特に明記しない限り、交換可能に使用される）は、KMS から受信したアクセス・トークン及びプロビジョニング・メッセージのみを有する。主な役割は、プロビジョニング・メッセージを ECU に送達することである。

【0064】

プロビジョニング・プロセスは、3 つのステップ、すなわち、1) ECU 設定、2) プロビジョニング・ツール設定、3) 自己鍵生成に分割される。第 1 のステップは、KMS

とサプライヤ工場プロビジョニング・システムとの間で実装され、これは、サプライヤ生産におけるデバイス設定のためのものであり、一部のエンジニア又はシステムがECU内部に秘密情報を注入する。KMSとプロビジョニング・ツールとの間で実装される第2のステップでは、KMSは、車両鍵設定のためのプロビジョニング・データを用いてプロビジョニング・ツールを提供する。プロビジョニング・ツールの主な役割は、このデータをECUデバイスに送信するだけである。サプライヤ工場プロビジョニング・システムとプロビジョニング・ツールとの間で実装される最後のステップとして、受信したプロビジョニング・データを使用して各デバイスで自己鍵生成が実行されて、VSK及びFSKを取得する。

【0065】

車両のECUデバイスに対するプロビジョニング・プロセス全体は、以下のとおりであってもよい。

【0066】

1) サプライヤ生産ツールは、その製品にローカル・プロビジョニング・データをインポートし、例えば、ローカル・プロビジョニング・データは、プロビジョニング鍵、OEMの公開鍵、タイムスタンプ、車に関する他の情報を含んでもよい。ここで列挙された上記のデータは、例示的な目的のためだけであり、詳細な実装は、以下の実施形態で説明されることに留意されたい。

2) プロビジョニング・ツールは、KMSから受信したアクセス・トークンを用いて車両のすべてのECUへのアクセスを獲得し、プロビジョニング・メッセージをそれらに送信する。

3) 車両内のすべてのECUは、プロビジョニング・ツールによって伝送され、かつ署名及び公開鍵で認証されたプロビジョニング・メッセージを使用して、車両固有秘密鍵を自己生成する。

4) 車両内のすべてのECUは、自己生成及び検証された車両固有秘密鍵に基づいて、他の機能秘密鍵を自己生成する。

5) 車両のゲートウェイは、すべてのECUが鍵プロビジョニング・プロセスを完了することを確認し、プロビジョニング・ツールを介してその結果をサーバに通知する。

6) ゲートウェイ(GW)を除くすべてのECUは、プロビジョニング鍵及び自己鍵生成機能を削除する。本開示によって提供される鍵プロビジョニング方法は、図2bに示す詳細情報と組み合わせて説明される。

【0067】

図3a及び図3bは、本開示の一実施形態による、鍵プロビジョニング方法における第1のデバイス設定の概略フローチャートを示す。図3a及び図3bは、前述の第1のステップにおける特定の処理、サプライヤ生産におけるECU設定を示す。この方法は、OEM側のサーバと、サプライヤ側のサプライヤ・デバイス（後の説明においては第4のデバイスとも呼ばれ、これら2つの用語は、特に明記しない限り、交換可能に使用される）とによって実行されてもよい。このフローチャートは、図2a及び図2bに示す第1のステップに関連し、ECUデバイスを設定するように機能し、第1のデバイスは、図2bに示すECUデバイスであってもよい。

【0068】

このプロセスは、サプライヤ製造システムで実行されると想定される。追加的に、前述したように、サーバ(OEM KMS)とサプライヤ・デバイス(サプライヤ製造システムで提供される)は相互認証を行い、互いを検証し、セキュアな通信のためのセキュアなチャネルを確立すると想定される。

【0069】

方法は、以下を含んでもよい。

【0070】

S301: サプライヤ・デバイスは、第1のデバイスを設定するための設定要求をサーバに送信し、サーバは、サプライヤ・デバイスからの設定要求を受信する。

10

20

30

40

50

【0071】

確立されたセキュア・チャネルを介して、サプライヤ・デバイスは、KMSサーバに設定要求を送信し、設定要求は、第1のデバイスが属する車両、すなわち第1のデバイス（図2aに示すECUデバイス）が搭載されている車両のアイデンティティを含んでもよい。

【0072】

例えば、サプライヤ・デバイスは、設定要求に補足情報、すなわち、車両タイプ、製品タイプ、サプライヤ識別情報などの製品に関する情報を含んで、ECUデバイスに対するローカル・プロビジョニング・データを取得してもよい。

【0073】

実際のアプリケーションでは、KMSサーバは、プロビジョニング・データを配布するための独自のポリシーを定義できるが、ポリシーは、OEMの選択に応じて変動してもよい。

【0074】

S302：サーバは、サプライヤ・デバイスにローカル・プロビジョニング・データを送信し、サプライヤ・デバイスは、ローカル・プロビジョニング・データを受信する。

【0075】

例示的には、図2bを参照すると、車両のアイデンティティを取得すると、KMSサーバは、ECUデバイスと一致する適切なプロビジョニング・データ、すなわちローカル・プロビジョニング・データをサプライヤ・デバイスに応答してもよく、このローカル・プロビジョニング・データは、1）プロビジョニング鍵（図2bに示すプロビジョニング鍵）、2）公開鍵（図2bに示すOEM公開鍵、ECUにおける署名検証鍵とも呼ばれる）、及び3）ローカル・タイムスタンプを含んでもよく、プロビジョニング鍵は、後の段階においてECUデバイスに対するグループ鍵を生成するように構成されており、公開鍵は、プロビジョニング・メッセージをECUデバイスに送信するプロビジョニング・ツールが提供される第2のデバイスの権限を検証するように構成されており、実際には、受信したメッセージがKMSによって生成されたものであることを確認するための検証に使用され、ローカル・タイムスタンプは、生成されたプロビジョニング鍵の有効性を検証するように構成されており、実際には、廃止されたメッセージ又はリプレイされたメッセージを許可しないように新鮮さのために使用され、可能な実装として、ローカル・タイムスタンプは、現在時刻であってもよい。

【0076】

S303：サプライヤ・デバイスは、ローカル・プロビジョニング・データを第1のデバイスに注入する。

【0077】

注入は、セキュアなデバッグ・ツールのようなサプライヤ自身のセキュアな方法で行われてもよい。第1のデバイスは、HSM又はTEEによって提供されるセキュアなストレージのような保護されたメモリにデータを記憶する。

【0078】

これに対応して、第1のデバイス側では、第1のデバイスがローカル・プロビジョニング・データを取得してもよい。

【0079】

例示的には、図2bに示すように、サプライヤ・デバイス及びサーバは、TLSハイパー・テキスト・トランスファー・プロトコル・セキュア（HTTPS）などの一定のプロトコルに基づいて確立されたセキュアなチャネルを介して通信してもよく、ECUサプライヤ工場プロビジョニング・システムを用いて実装されたサプライヤ・デバイスは、プロビジョニング鍵及びOEM公開鍵を受信し、次いで、プロビジョニング鍵、公開鍵及び現在のタイムスタンプをECUに注入し、それによりECUデバイスの設定を完了してもよい。

【0080】

図4a及び図4bは、本開示の一実施形態による、鍵プロビジョニング方法における第

10

20

30

40

50

2のデバイス設定の概略フローチャートを示す。図4b及び図4bは、前述の第2のステップ、プロビジョニング・ツール設定の特定の処理を示し、ECUデバイスにアクセスするために第2のデバイスにおいて提供されるプロビジョニング・ツールを準備するようにする。図4bは、図4aと比較して詳細なパラメータを特定する。上記のように、プロビジョニング・ツールの主な役割は、ECUデバイスにアクセスし、KMSサーバから受信したプロビジョニング・データをECUデバイスに渡すことである。図4に示すフローは、OEM側で、特に、OEM側のサーバと、OEM側でプロビジョニング・ツールが提供されてもよい第2のデバイスとの間で行われる。このフローチャートは、図2a及び図2bに示す第2のステップに関連し、以下の説明における第1のデバイスは、図2bに示すECUデバイスであってもよい。さらに、プロビジョニング・ツールは、ソフトウェア機能又はハードウェアとして第2のデバイスに提供されてもよいし、プロビジョニング・ツールは、第2のデバイスとして実装されてもよく、従って、プロビジョニング・ツールの構成は、第2のデバイスの構成と等価であり、説明全体を通じて第2のデバイスによって行われる動作もプロビジョニング・ツールによって行われる動作とみなすことができる。

【0081】

S401：第2のデバイスは、グループ鍵に対応するアクセス・トークンを要求するためのトークン要求をサーバに送信し、サーバは、トークン要求を受信する。

【0082】

S402：サーバは、第2のデバイスに、トークン要求に対応するアクセス・トークン、及びアクセス・トークンに対応する第2のプロビジョニング・メッセージを送信する。

【0083】

第1のデバイスにアクセスする前に、第2のデバイスは、最初にグループ鍵（VSK）に対応するアクセス・トークンを取得し、アクセス・トークンは、第1のデバイスがグループ鍵を生成できるように第1のデバイスにアクセスするために第2のデバイスによって使用される。

【0084】

トークン要求は、第2のデバイスがプロビジョニングしようとしている1つ以上の車両のアイデンティティを含んでもよく、第1のデバイスが属する車両は、それらの車両に含まれる。可能な実装では、トークン要求は、単に、第1のデバイスが属する車両の1つのアイデンティティを含んでもよい。別の実装では、トークン要求は、第2のデバイスがプロビジョニングしようとしているいくつかの車両のアイデンティティを含んでもよく、第1のデバイスが属する車両は、それらの車両に含まれる。いくつかの車両のアイデンティティは、任意選択でリストの形態であってもよい。

【0085】

トークン要求が単に第1のデバイスが属する1つの車両のアイデンティティを含むときに、サーバは、第1のデバイスが属する車両のアイデンティティに対応するアクセス・トークン、及び車両のプロビジョニング・データを含む第2のプロビジョニング・メッセージを返す。さらに、第2のデバイスがいくつかの車両にプロビジョニングすることを目的とすることも可能であり、このようにして、第2のデバイスは、トークン要求に車両のアイデンティティのリストを含んでもよく、今度は、サーバは、第2のデバイスに、トークン要求に対応するアクセス・トークン、及び車両に対するプロビジョニング・データを含む第2のプロビジョニング・メッセージを送信してもよい。このアクセス・トークンを使用して、第2の車両は、リスト内の車両にアクセスすることができてよい。

【0086】

例示的には、図2bに示すように、プロビジョニング・ツールとKMSサーバの両方がOEMに属する場合であっても、それらは、地理的に分離されてもよく、これは、プロビジョニング・ツール（おそらくは、ポータブル・デバイス又はプログラム）が、「工場側システム／ツール」及び「クラウドベースのKMSサーバ」などの物理的距離でKMSサーバから分離されることを意味する。したがって、KMSサーバ及び第2のデバイスは、何らかの情報を共有するためのセキュアなチャンネルが必要である。図2bに示すように、

セキュア・チャネルは、T L S 及び H T T P S を使用して確立されてもよい。提案された方法は、O E M の管理下でないアフターマーケット・ディーラーシップ・テスター・ツールも考慮する（このユース・ケースについては、後の部分で説明される）。

【0087】

プロビジョニング・ツールは、確立されたセキュアで認証されたチャネルを介して、プロビジョニングされた車両識別情報と共にプロビジョニング・データ及びアクセス・トークンに対するトークン要求をK M S サーバに送信して、どのデータを転送すべきかをサーバに知らせ決定させる。プロビジョニング・ツールは、製造管理システム、生産スケジュール、又は車両への直接アクセスなどから、どの車両がプロビジョニングされるかを認識している。それは、車両及びそれらがプロビジョニングのためにアクセスしたいE C U デバイスのリストを転送する。要求者（第2のデバイス）がターゲット車両アイデンティティ（V I N）に対する認可を有することを確認した後、サーバは、権利提供メッセージを生成し、第2のデバイスに送信する。サーバ伝送は、2種のデータを含む。

【0088】

1）アクセス・トークン：これは、E C U デバイス（第1のデバイス）にアクセスするために使用される。このツールは、アクセスできる車両を特定する1つのアクセス・トークンのみを有するであろう。可能な実装では、アクセス・トークンは、アクセスできるデバイスを特定してもよい。異なる構造を有するアクセス・トークンは、異なる機能を達成してもよく、これは、後の部分で説明される。

2）プロビジョニング・データ：それは、第2のデバイス（又はプロビジョニング・ツール）がプロビジョニングのために第1のデバイスに転送すべきものであり、単に車両ごとに1つのメッセージが割り当てられる。それは、以下のデータ、すなわち、プロビジョニング鍵（E C U 内のプロビジョニング鍵P V K を指す）によって暗号化されたランダム・ストリングと、プロビジョニング鍵によって暗号化されたプロビジョニング・タイムスタンプ（O E M サーバからE C U デバイスまでの現在のタイムスタンプを指す）とからなり、ランダム・ストリングとプロビジョニング・タイムスタンプは、E C U デバイスによってプロビジョニング鍵を生成するために使用されてもよく、検証署名は、E C U デバイスによって生成されたプロビジョニング鍵の有効性を検証するために使用されてもよい。

【0089】

可能な実装では、ランダム・ストリングR S_i及びプロビジョニング・タイムスタンプT S_iは、暗号テキストC_iに含まれてもよい。

【0090】

上述のように、トークン要求が複数の車両のアイデンティティを含む場合、サーバは、異なる車両に対するプロビジョニング・データを含むいくつかの第2プロビジョニング・メッセージで応答することができ、従って、ステップS 402で返されるプロビジョニング・データは、インデックスiで表されてもよく、ここで、iは、ターゲット車両iの識別子（ターゲット車両アイデンティティ）を意味する。例えば、サーバによって返されるプロビジョニング・データは、プロビジョニング鍵によって暗号化されたランダム・ストリングR S_iと、プロビジョニング鍵によって暗号化されたプロビジョニング・タイムスタンプT S_iと、検証署名σ_iと、を含んでもよい。サーバはまた、プロビジョニング・データにV I N_{-i}（ターゲット車両のアイデンティティ）を含めて、どのプロビジョニング・データがどの車両に対応しているかを第2のデバイスに知らせるようにすることができる。この場合、検証シグネチャσ_iは、V S K_i、R S_i及びT S_iのデータに対するシグネチャを意味し、V S K_iは、E C U デバイスが専用ビークルiに対する自己鍵生成によって取得する所望のキーである。代替的には、サーバ及び第2のデバイスはまた、プロビジョニング・ツールの設定の前に、トークン要求と第2のプロビジョニング・メッセージとの間の対応を交渉することができ、例えば、トークン要求がいくつかのアイデンティティを含むときに、サーバは、第2のプロビジョニング・メッセージに含まれるプロビジョニング・データにV I N_{-i}を含めることなく、どの第2のプロビジョニング・メッセージがどの車両に対応するかを第2のデバイスが知るように、事前定義された順序で第

2 のプロビジョニング・メッセージを返してもよい。この場合、検証署名 σ_i は、 VSK_i 、 VIN_i 、 RS_i 、 TS_i のデータに対する署名を意味する。

【0091】

上記の方法では、第2のデバイス内のプロビジョニング・ツールが設定され、ターゲット車両にプロビジョニングを実行するように準備されてもよい。

【0092】

図5は、本開示の一実施形態による、鍵プロビジョニング方法における自己鍵生成の概略フローチャートを示す。図5は、前述の第3のステップ、プロビジョニング・データに基づく鍵生成の特定の処理を示す。図5に示すフローは、第1のデバイス（ECUデバイス）と第2のデバイス（プロビジョニング・ツールが提供される）との間、特に、車両に搭載されたECUデバイスとOEM側でプロビジョニング・ツールが提供され得る第2のデバイスとの間で行われる。このフローチャートは、図2a及び図2bに示す第3のステップに関連し、以下の説明における第1のデバイスは、図2bに示すECUデバイスであってもよい。図5に示す処理の前に、第1のデバイスは、図3aに示す方法で設定されており、第2のデバイスも、図4aに示す方法で設定されている。

【0093】

S501：第2のデバイスは、第1のデバイスに、第1のデバイスへのアクセスを要求するためのアクセス要求を送信し、第1のデバイスは、第2のデバイスからアクセス要求を受信する。

【0094】

可能な実装では、アクセス要求は、単に第1のデバイスにデータを書き込むための要求だけであってもよい。アクセス要求は、第1のデバイスによって第2のデバイスの認証をトリガするために使用される。

【0095】

S502：第1のデバイスは、第2のデバイスが第1のデバイスへのアクセスを許可されているかどうかを判定する。

【0096】

第1のデバイスは、アクセス要求を受信すると、セキュリティのために第2のデバイスが第1のデバイスにアクセスすることを許可されているかどうかを判定してもよい。言い換えれば、アクセス権限の判定は、アクセス要求によってトリガされる。

【0097】

S503：第1のデバイスは、判定に基づいて、第2のデバイスにアクセス応答を送信し、第2のデバイスは、第1のデバイスからアクセス応答を受信する。

【0098】

可能な実装では、第1のデバイスは、第2のデバイスが第1のデバイスへのアクセスを許可されていると分かるときに、それは、肯定的な応答で応答してもよく、そうでない場合、それは、否定的な応答で応答してもよい。したがって、アクセス応答は、アクセス要求に基づいて、第1のデバイスによって返される。

【0099】

S504：第2のデバイスは、第1のデバイスに第1のプロビジョニング・メッセージを送信し、第1のデバイスは、第2のデバイスから第1のプロビジョニング・メッセージを受信する。

【0100】

第1のデバイスからアクセス応答を受信すると、第2のデバイスは、第1のプロビジョニング・メッセージを第1のデバイスに送信してもよい。

【0101】

先に説明したように、第1のデバイスによって返されるアクセス応答は、肯定的な応答又は否定的な応答であってもよく、可能な実装では、応答が肯定的であるときに、第2のデバイスは、第1のプロビジョニング・メッセージを第1のデバイスに直接送信してもよく、応答が否定的であるときに、第2のデバイスは、サーバ（例えば、図2bに示すKM

10

20

30

40

50

Sサーバ)と対話して、第1のデバイスにアクセスする際の権限を更新してもよい。例えば、第2のデバイスは、そのトークンを更新してもよく、更新されたトークンにより、第2のデバイスは、第1のデバイスにアクセスしてもよい。

【0102】

S505：第1のデバイスは、プロビジョニング・データに従って、グループ鍵を生成する。

【0103】

第1のプロビジョニング・メッセージは、グループ鍵を生成するためのプロビジョニング・データを含み、第1のデバイスが、第2のデバイスから第1のプロビジョニング・メッセージを受信すると、それは、第1のプロビジョニング・メッセージに含まれるプロビジョニング・データに従って、グループ鍵（例えば、図2aに示すVSK）を生成してもよい。

10

【0104】

ここでは、1つの第1のデバイスの動作のみを示しているが、実際のアプリケーションでは、車両内のすべてのECUデバイスが、同じ動作を実行して、グループ鍵を生成してもよいと留意されたい。

【0105】

また、以下の部分で詳細に述べるように、実際のアプリケーションでは、ECUデバイスが、車両内のゲートウェイに接続されることがあり、その場合に、外部のソースから第1のデバイスに伝送されるデータ又は情報が、最初にゲートウェイに遭遇することがあるため、従って、第1の車両がECUデバイスであることにより、ステップS501におけるアクセス要求の受信、及びステップS504における第1のプロビジョニング・メッセージの受信は、間接受信、すなわち、ゲートウェイからの転送によってこのような種のデータを受信するものと解釈すべきである。

20

【0106】

本開示によれば、第2のデバイスは、車両内の第1のデバイスにアクセスし、車両内のすべての第1のデバイスに対してグループ鍵を1つのプロビジョニング・メッセージで設定することが可能であり、それによってたとえそれが多くのデバイス及び多くの車両に対して展開されたとしても、トラフィック・オーバーヘッド及びネットワーク伝送及び動作遅延を低減する。

30

【0107】

以下、ECUデバイスの自己鍵生成の詳細な実装を、添付図面を参照して述べてもよい。

【0108】

実際のアプリケーションでは、ECUデバイスは、ゲートウェイ（GW）に接続されることがある。ゲートウェイは、オンボードECUデバイスに接続されたデバイスを表すと共に、診断などの外部デバイスと通信するためのインターフェースを有する。したがって、第2のデバイスは、ECUデバイスにアクセスするときに、最初にゲートウェイに遭遇してもよい。

【0109】

したがって、図2a及び図2bに示す第3のステップは、ECUデバイスがどこで行うかに応じて2つの方法で実装されてもよい。図6a及び図6bは、第3のステップがGWでどのように行われるかを示し、図6cは、通常のECUデバイスに対するフローを示す。プロビジョニング・ツールが車両にアクセスしようとするときに、最初にGWに遭遇し、車両内のECUデバイスへのアクセスを入手するためにGWを通過する必要がある。したがって、GWは、車両生産における最初のプロビジョニング・ターゲットとすべきである。

40

【0110】

図6a～図6cは、本開示の一実施形態による、鍵プロビジョニング方法における自己鍵生成の概略フローチャートを示す。図5a及び図5bと比較して、図6a～図6cにはより特定の詳細が追加されている。図6a～図6cに示す処理の前に、ECUデバイスは

50

、図 3 a に示す方法で設定されており、第 2 のデバイスも図 4 a に示す方法で構成されていると留意されたい。

【0111】

方法は、以下を含んでもよい。

【0112】

S 6 0 1：プロビジョニング・ツールは、ゲートウェイに、ゲートウェイへのアクセスを要求するためのアクセス要求を送信し、ゲートウェイは、プロビジョニング・ツールからアクセス要求を受信する。

【0113】

アクセス要求がトリガされると、アクセス要求は、第 1 のデバイスにデータの書き込むための要求だけであってもよい。

【0114】

S 6 0 2：ゲートウェイは、プロビジョニング・ツールがゲートウェイへのアクセスを許可されているかどうかを判定する。

【0115】

ゲートウェイは、アクセス要求を受信すると、セキュリティのためにプロビジョニング・ツールが第 1 のデバイスにアクセスすることを許可されているかどうかを判定してもよい。判定は、ゲートウェイとプロビジョニング・ツールとの間のトークンベース認証であってもよい。特定の権限については、図 8 a 及び図 8 b を参照して後で説明される。

【0116】

S 6 0 3：ゲートウェイは、判定に基づいて、プロビジョニング・ツールにアクセス応答を送信し、プロビジョニング・ツールは、ゲートウェイからアクセス応答を受信する。

【0117】

アクセス応答は、肯定的なアクセス応答又は否定的なアクセス応答であってもよい。

【0118】

受信したアクセス・トークンが有効であると判定すると、ゲートウェイは、肯定的なアクセス応答をプロビジョニング・ツールに送信し、受信したアクセス・トークンが無効であると判定すると、ゲートウェイは、否定的なアクセス応答をプロビジョニング・ツールに送信し、これは、プロビジョニング・ツールによって送信されたアクセス・トークンが期限切れになったときに可能性としてであってもよい。

【0119】

プロビジョニング・ツール側では、肯定的なアクセス応答の受信は、プロビジョニング・ツールがゲートウェイをプロビジョニングするための正しいアクセス・トークンを有することを示し得るが、否定的なアクセス応答の受信は、プロビジョニング・ツールがゲートウェイをプロビジョニングするための正しいアクセス・トークンを有していないことを示し得るので、従って、プロビジョニング・ツールは、ゲートウェイから否定的なアクセス応答を受信すると、ゲートウェイに対するアクセス・トークンを更新するためのトークン更新要求をサーバに送信し、グループ鍵に対応するアクセス・トークンとして、更新されたアクセス・トークンをサーバから受信してもよい。いずれの場合も、プロビジョニング・ツールは、最終的にゲートウェイにアクセスすることが可能となる。

【0120】

サーバ側では、第 2 のデバイスからゲートウェイに対するアクセス・トークンを更新するためのトークン更新要求を受信すると、サーバは、トークン更新要求に従って、更新されたアクセス・トークンをプロビジョニング・ツールに送信する。

【0121】

S 6 0 4：プロビジョニング・ツールは、第 1 のプロビジョニング・メッセージをゲートウェイに送信し、ゲートウェイは、プロビジョニング・ツールから第 1 のプロビジョニング・メッセージを受信する。

【0122】

第 1 のデバイスからアクセス応答を受信すると、プロビジョニング・ツールは、第 1 の

10

20

30

40

50

プロビジョニング・メッセージを第1のデバイスに送信してもよい。

【0123】

第1のプロビジョニング・メッセージは、ゲートウェイによってグループ鍵を生成するためのプロビジョニング・データを含んでもよい。

【0124】

S605：ゲートウェイは、プロビジョニング・データに従って、グループ鍵を生成する。

【0125】

プロビジョニング・データは、プロビジョニング鍵によって暗号化されたランダム・ストリング、プロビジョニング鍵によって暗号化されたプロビジョニング・タイムスタンプ、及び検証署名を含んでもよい。

10

【0126】

グループ鍵は、以下のように生成されてもよい。すなわち、ゲートウェイが、プロビジョニング鍵を使用して、プロビジョニング・データを復号して、ランダム・ストリング及びプロビジョニング・タイムスタンプを取得し、次いで、ランダム・ストリング及びプロビジョニング・タイムスタンプに基づいて、グループ鍵を生成し、グループ鍵を生成した後、ゲートウェイは、プロビジョニング・データにおける検証署名に従って、生成されたプロビジョニング鍵の有効性を検証する。

【0127】

先に説明したように、グループ鍵（VSK）以外に、ECUデバイスはまた、FSKを任意選択として所有してもよい。以下のステップは、任意選択であり、実際のニーズに応じて行われてもよい。

20

【0128】

S606：ゲートウェイは、プロビジョニング・ツールに第1のプロビジョニング応答を送信し、プロビジョニング・ツールは、第1のプロビジョニング応答を受信する。

【0129】

グループ鍵を生成した後、ゲートウェイは、プロビジョニング・ツールに応答を送信して、プロビジョニング・ツールが、グループ鍵が正常に生成されたかどうかを知ることになるようにする。

【0130】

S607：第1のプロビジョニング応答が、グループ鍵が第1のデバイスによって正常に生成されたことを示すときに、プロビジョニング・ツールは、ゲートウェイに対して機能秘密鍵をプロビジョニングするためのプロビジョニング要求を送信し、ゲートウェイは、第2のデバイスからプロビジョニング要求を受信する。

30

【0131】

S608：ゲートウェイは、グループ鍵及び事前記憶されたデータに基づいて、機能秘密鍵を生成する。

【0132】

FSKの生成は、生成されたグループ鍵と何らかの事前記憶されたデータに基づいて行われてもよい。

40

【0133】

ゲートウェイ（FKSがゲートウェイによって生成される場合）又はECUデバイス（FKSがECUデバイス自体によって生成される場合）は、VSK及び事前定義ストリングを使用して、ECU専用機能キー及びいくつかのグループ専用機能鍵を取得することができる。{ECU部品番号、一意ID、シリアル番号、及び追加ストリング（「e2e」など）}は、（KMSサーバとECUデバイス間のエンドツーエンド秘密鍵として）ECU専用鍵のための事前定義ストリングの一例とすることができる。

【0134】

FSK生成の可能な実装が、図7aに示されている。FSKsの例が、図7bに示されている。図7aに示すように、事前定義ストリングは、ECUデバイスに事前に書き込ま

50

れた何らかのデータであってもよく、F S Kの生成はまた、車両のアイデンティティ（V I N）に基づいてもよい。鍵導出機能（K D F）の出力は、E C Uデバイス内の署名を用いて検証されてもよい。

【0135】

V S Kの例は、H M A C - S H A 2 5 6などの擬似ランダム関数（P R F）を用いたK D F（P V K，V I N || 事前定義ストリング || R S || T S）であってもよい。また、機能鍵の一例は、K D F（V S K，V I N || 事前定義ストリング）であってもよい。

【0136】

また、P B K D F 2（R F C 8 0 1 8、P K C S # 5 : P a s s w o r d - B a s e d C r y p t o g r a p h y S p e c i f i c a t i o n V e r s i o n 2 . 1）及び s c r y p t（R F C 7 9 1 4、T h e s c r y p t P a s s w o r d - B a s e d K e y D e r i v a t i o n F u n c t i o n）などのK D Fの例において、P w（p a s s w o r d、p a s s p h r a s e）、ソルト、反復／コスト・ファクタなどの図7 bに示すパラメータが適用され得る。

10

【0137】

S 6 0 9：ゲートウェイは、第2のプロビジョニング応答を第2のデバイスに送信し、プロビジョニング・ツールは、第1のデバイスから第2のプロビジョニング応答を受信する。

【0138】

第2のプロビジョニング応答は、F S Kがゲートウェイによって正常に生成されたかどうかをプロビジョニング・ツールに知らせるように機能する。

20

【0139】

S 6 1 0：ゲートウェイは、生成された鍵をE C Uデバイスにルーティングする。

【0140】

V S K及びF S Kの生成後、ゲートウェイは、生成された鍵をE C Uデバイスにルーティングしてもよい。

【0141】

可能な実装では、V S K及びF S Kの生成後、ゲートウェイは、次いで、公開鍵及び鍵を生成するためのストリングなど、鍵プロビジョニングに関連する秘密情報を消去してもよい。

30

【0142】

上記のプロセスをよりよく理解するために、図6 bを参照のこと。それは、プロビジョニング・ツールからデバイスへのV S Kプロビジョニング要求（ステップS 6 0 1におけるアクセス要求）から開始される。例えば、このプロビジョニング要求は、診断メッセージ（U D S、U n i f i e d D i a g n o s t i c S e r v i c e）上の一種の「データ書き込み」要求とすることができる。続いて、トークンベース認証が行われた後、プロビジョニング・ツールは、K M Sから受信したプロビジョニング・データを送信する（ステップS 6 0 4と同様）。G Wがこのデータを受信すると、それは、1）暗号テキストを復号して、メッセージからランダム・ストリング及びタイムスタンプを入手し、2）復号されたデータを用いてV S Kを生成し、3）生成されたデータが正しいかどうかを検証する。これらのプロセスが正常に行われる場合、プロビジョニング・ツールは、F S Kプロビジョニングし、E C Uデバイスに他の機能秘密鍵を生成するように要求する。デバイスがすべての鍵生成を終了するときに、それは、この自己生成に関連するプロビジョニング・データ及び秘密情報を削除する。G Wは、これらの受信データを車両内の対応するE C Uデバイスにルーティングする担当を有する。

40

【0143】

図6 cは、プロビジョニングがE C Uデバイスで行われる別の可能な場合を示しており、この場合に、ゲートウェイは、一般にプロビジョニング・ツールから受信したすべてをE C Uデバイスにルーティングする。トークンベース認証、グループ鍵の生成、及びF S Kは、図6 a及び図6 bと同じであるが、これは、簡略化のため詳細には説明されない。

50

【0144】

追加的に、VSKの生成に関して、図2bを参照して、各ECUにおいて、KDF（鍵導出機能）、秘密鍵、事前定義ストリング及びパラメータからなる「自己鍵生成器」（ECUデバイスにおいてソフトウェア機能として実装され得る）を使用して鍵生成が実行される。HKDF、PBKDF2、Scryptなど多くのKDFがある。それらのうちのいずれか1つを選択することができる。これとは別に、KDFは、外部のソースから受信した追加の入力ストリングを取って、車両に対して一意の結果を生成する。例示的なストリングのいくつかは、図8に示されている。

【0145】

さらに、典型的なECUデバイスのプロセスは、GW内で行われるものと同様であるが、「鍵確認」というもう1つのステップを除き、GWは、典型的なチャレンジ応答認証の一種として、ECUデバイスがFSKを正しく生成することを確認する。例えば、ECUデバイスは、ゲートウェイから鍵確認チャレンジを受信してもよく、ここで、プロビジョニング・ツールから機能秘密鍵が正しく生成されたかどうかを確認するための鍵確認要求を受信すると、鍵確認チャレンジがゲートウェイによって送信され、次いで、ECUデバイスは、鍵確認チャレンジ、機能秘密鍵、及び第2の事前定義されたアルゴリズムに従って、鍵確認応答を生成し、鍵確認応答をゲートウェイに送信する。

【0146】

図6cと組み合わせて、前述の鍵確認プロセスは、以下のようにチャレンジ応答であってもよい。

【0147】

- 1) GWは、チャレンジとして「ランダム数」を対応するECUに送信する。
- 2) ECUは、生成された鍵（生成されたFSK）とMAC_{VSK}（FSK | ランダム）の形態のような暗号関数を使用して応答を行い、それを、GWに返信し、ここで、MACは、メッセージ認証コードアルゴリズムを指し、これは、実際の必要に応じて他の好適なアルゴリズムに変更されてもよく、本明細書において限定されない。
- 3) GWは、それを自分自身の世代と比較し、失敗又は成功を判定する。

【0148】

可能な実装では、GWは、プロビジョニング・ツールが車両にアクセスしようとする度にアクセス・トークンを完全に検証する必要はない。クッキー又はキャッシュと同様の方法を用いて最新の認証ログを保持して使用することで、遅延を低減することができる。例えば、GWは、署名を検証する時間を無駄にすることなく（それを以前に検証された署名と比較することによって）、アクセス・トークン内の認可値を単にチェックすることができる。認証プロセスの詳細については、後の部分で説明されてもよい。

【0149】

図6cに示すように、ECU1及びECU2は、最初に順次プロビジョニングされ、別の可能な場合では、プロビジョニング・ツールは、ネットワーク及びGWがそれを行う余裕がある場合、同時に複数のデバイスにアクセスすることができる。最も時間を消費するプロセスのうちの1つは、署名検証である。伝送、復号、鍵生成は、いくらか速い。デバイスの検証処理中に、プロビジョニング・ツールは、他のデバイスにアクセスして、全体の時間を低減することができる。隔離された異なるネットワーク上の他のデバイスへのアクセスは、中断の可能性を低減することによって、プロセス全体を最適化するのに役立つ。

【0150】

図9a及び図9bは、本開示の一実施形態による、鍵プロビジョニング方法におけるトークンベース認証の概略フローチャートを示す。これらの図は、実際には前述のステップS602を特定している。上述したように、プロビジョニングは、ECUデバイス（図6c）で直接行われてもよいし、ゲートウェイ（図6b）で行われてもよく、従って、特定の状況に応じて、トークンベース認証は、ECUデバイスとプロビジョニング・ツールを備えた第2のデバイスとの間、又はゲートウェイと第2のデバイスとの間で実行されてもよい。以下、認可がゲートウェイとプロビジョニング・ツールとの間で行われる一例を取

ることによって、説明が行われる。認可が、ECUデバイスとプロビジョニング・ツールを備えた第2のデバイスとの間にある場合では、ECUデバイスの動作については、ゲートウェイの動作を参照してもよい。

【0151】

図9aは、トークンベース認証の例示的なフローチャートを示す。認証プロセス全体は、UDS (Unified Diagnostic Services) 認証の自動車標準プロトコルに基づき、これは、UDSセキュリティ・アクセス、シード鍵認証、又はチャレンジ応答認証として知られている。従来のランダム・チャレンジを使用する方法とは異なり、ECUデバイスは、図9bに示すように、「カウンタ」を用いて固定チャレンジ番号を使用する。このカウンタは、プロビジョニングの何らかの特定のステータスを表し、例えば、カウンタ番号「1」は、デバイスが現在PVKを有し、VSKを生成するための次のステップに進むことができることを意味する。デバイスはプロビジョニングを完了するたびに、それは、カウンタ番号を1ずつ増加させる。このカウンタは決して減分することができず、より小さい番号に戻ることができないことに留意する。ECUデバイス又はゲートウェイからチャレンジとしてカウンタを受信するときに、プロビジョニング・ツールは、このカウンタ・チャレンジ番号と一致するアクセス・トークンに応答すべきである。プロビジョニングが正常に完了した後にカウンタが増加するため、プロビジョニング・ツールは、トークンを再使用することができない。したがって、以前に使用されたトークンを用いてリレー攻撃を誰かが試みる場合、それは、すでに増加しているカウンタ番号と一致しないため、拒否されなくてはならない。

【0152】

処理は、図9bと組み合わせてさらに説明される。

【0153】

S901:ゲートウェイは、プロビジョニング・ツールに、プロビジョニング・ツールの権限を検証するための認証要求を送信し、プロビジョニング・ツールは、ゲートウェイから認証要求を受信する。

【0154】

トークンベース認証は、チャレンジ応答認証であってもよい。従来のランダム・チャレンジを使用する方法とは異なり、ECUデバイスは、図9bに示すように、「カウンタ」を用いて固定チャレンジ番号を使用する。

【0155】

可能な実装では、認証要求は、ローカル・カウンタ(図2bに示すようなカウンタ)を含んでもよく、ローカル・カウンタは、ゲートウェイのプロビジョニング状態を反映するように構成されてもよく、カウンタの値は、ゲートウェイのプロビジョニング状態が変更されると、ゲートウェイによりプリセットされた規則に基づいて変更される。

【0156】

ここで、悪意のあるアクセスをブロックするためにローカル・カウンタの値に特定の意味を定義してもよい。例えば、図9aの表に示すように、0であるローカル・カウンタは、プロビジョニングされていない状態を表してもよく、1であるローカル・カウンタは、PVKがプロビジョニングされた状態を表してもよく、2であるローカル・カウンタは、VSKがプロビジョニングされた状態を表してもよく、3であるローカル・カウンタは、FSKがプロビジョニングされた状態を表してもよく、3よりも大きいローカル・カウンタは、いくつかの鍵が更新された状態を表してもよい。以下、このような想定に基づいて説明がなされるが、ローカル・カウンタの特定の値は説明のためだけのものであり、本開示に対する制限として解釈されるべきではないと理解されるべきである。ECUデバイスの異なるプロビジョニング状態を示す限り、他の値も可能である。

【0157】

S902:プロビジョニング・ツールは、認証要求と一致するアクセス・トークンを判定する。

【0158】

プロビジョニング・ツールは、認証要求に従って、ゲートウェイのプロビジョニング状態を判定し、ゲートウェイのグループ鍵（VSK）がゲートウェイによって生成されていないと判定すると、プロビジョニング・ツールは、グループ鍵に対応するアクセス・トークンを、認証要求に合致するアクセス・トークンとして使用する。ここで、アクセス・トークンは、図4aに示すフローに従って、プロビジョニング・ツールによってサーバから受信されてもよい。プロビジョニング・ツールが正しいアクセス・トークンを持っていない場合、それは、そのアクセス・トークンを更新するようサーバに要求してもよい。更新プロセスは、後で詳細に説明される。

【0159】

S903：プロビジョニング・ツールは、認証要求と一致したアクセス・トークンをゲートウェイに送信し、ゲートウェイは、認証要求と一致したアクセス・トークンを受信する。

10

【0160】

S904：ゲートウェイは、受信したアクセス・トークンが有効であるかどうかを判定する。

【0161】

アクセス・トークンの有効性の判定は、アクセス・トークンの特定の構造に基づいて行われてもよい。

【0162】

アクセス・トークンの例示的な構造を図10に示す。図10に示すように、アクセス・トークンは、第1の事前定義されたアルゴリズムに基づいて生成された検証対象クレデンシャル、検証対象カウンタ、検証対象タイムスタンプ、検証対象車両アイデンティティ、及び検証対象署名を含んでもよい。

20

【0163】

この構成によれば、アクセス・トークンを受信すると、ゲートウェイは、受信したアクセス・トークンが有効であるかどうかを判定してもよく、具体的には、ゲートウェイは、アクセス・トークン内の各フィールドを図2bのECUデバイスに示すそのローカルデータと比較してもよく、ゲートウェイは、条件が満たされる場合、受信したアクセス・トークンが無効であると判定してもよく、条件は、以下のいずれか1つ以上を含んでもよい。

【0164】

30

1) ローカル・カウンタ（図2bのECUデバイスに示すカウンタ）及び第1の事前定義されたアルゴリズムに基づいて生成されたローカル・クレデンシャルが、検証対象のクレデンシャルと不整合である。

【0165】

受信したアクセス・トークン内のクレデンシャルは、事前定義されたアルゴリズムに従って、サーバによって生成され、ゲートウェイは、検証を完了するために同じアルゴリズムに従って、クレデンシャルを生成してもよい。

【0166】

可能な実装では、クレデンシャルは両方の側（ゲートウェイとサーバ）で以下のように生成されてもよい。すなわち、 $Cred\text{ential} = MAC_{Key}$ （追加ストリング | カウンタ | パディング）、ここで、 $Cred\text{ential}$ は、カウンタ及び事前共有秘密鍵に基づくMAC（メッセージ認証コード）アルゴリズムを使用して生成されたタグであり、事前共有秘密鍵は、PVK又は機能鍵の1つ、例えば、認証鍵（AUK）であってもよく、鍵は、 $Counter = 1$ 又は2の場合、PVKと等しく、 $Counter > 2$ の場合、AUKであり、上記のアルゴリズムにおける追加ストリングは、任意選択であり、例えば、OEM ID、車両タイプ、又は何らかの事前定義ランダム・ストリングであってもよく、パディングは、32バイト及び64バイト長を長さ又はゼロに合わせるなど、クレデンシャルを生成するためのアルゴリズムに依存する。

40

【0167】

2) ローカル・カウンタ（図2bのECUデバイスに示すカウンタ）が、検証対象カウ

50

ンタと不整合である。

【0168】

ゲートウェイは、ローカル・カウンタを、受信したアクセス・トークン内の検証対象カウンタと比較し、これら2つの値が不整合である場合、アクセス・トークンが無効であると判定する。

【0169】

さらに、図9aを参照して先に説明したように、通常の場合（プロビジョニング・ツールに対して）、すなわち、P V Kが設定され、V S Kの生成の準備ができていない状態では、カウンタは1に等しくなければならない。

【0170】

3) ローカル・タイムスタンプが、検証対象タイムスタンプよりも後である。

【0171】

ゲートウェイは、ローカル・タイムスタンプ（図2bのECUデバイスに示すタイムスタンプ）を、受信したアクセス・トークン内の検証対象タイムスタンプと比較し、これら2つの値が不整合である場合、アクセス・トークンが無効であると判定してもよい。

【0172】

実際、検証対象タイムスタンプは、アクセス・トークンが生成されたときの値を表し、ローカル・タイムスタンプは、製造（工場）で注入された値、すなわちECU生産時間を表す。したがって、トークン生成時間は、ECU生産時間よりも最新であるべきであるため、ローカル・タイムスタンプは、プロビジョニング・ツールが古い（期限切れ／廃止された）トークンを再使用しようとする「リプレイ攻撃」の場合を保護するために使用され得る。

【0173】

4) 第1のデバイスが属する車両のアイデンティティが、検証対象車両のアイデンティティと不整合である。

【0174】

前述したように、プロビジョニング・ツールの設定段階において、サーバは、一定の車両にアクセスするためのアクセス・トークンをプロビジョニング・ツールに返してもよく、従って、アクセス・トークンは、第1のデバイスが属する車両のアイデンティティを含んでもよいし、少なくとも1つのアクセス・トークン内にすくなくとも1つの検証対象車両アイデンティティがあってもよく、これは、プロビジョニング・ツールによってサーバに送信されるトークン要求（図4aのステップS402）が車両のアイデンティティのリストを含むときの場合であり、結果的に、アクセス・トークンは、プロビジョニング・ツールがアクセスすることを認可された車両の複数のアイデンティティを含んでもよい。

【0175】

言い換えれば、タイムスタンプは、KMSサーバによってトークンが生成された時間に依存し、受信したアクセス・トークンの有効期限（トークンの鮮度）をチェックするために使用される。

【0176】

5) 公開鍵を用いた検証対象署名のチェックの失敗。

【0177】

検証対象署名は、KMSのプライベート鍵（ターゲット・デバイスが保持する公開鍵と対になっている）と、R S A S S A - P S S、E C D S A、E d D S Aなどの何らかの署名アルゴリズムを用いて、上記にリストされた先行するデータ {クレデンシャル、カウンタ、アクセス可能ターゲット、タイムスタンプ} に対して生成される。

【0178】

可能な実装では、アクセス・トークンは、車両グループ／タイプ、デバイス・タイプ及びデバイス・アイデンティティのリストなど、アクセス可能な車両及びECUをさらに識別するために使用されるフィールドを含んでもよい。

【0179】

10

20

30

40

50

受信したアクセス・トークンが有効であると判定すると、ゲートウェイは、肯定的なアクセス応答をプロビジョニング・ツールに送信し、受信したアクセス・トークンが無効であると判定すると、ゲートウェイは、否定的なアクセス応答をプロビジョニング・ツールに送信する。

【0180】

図11は、ECUデバイスのための認証ロジックを示す。ゲートウェイにおける認証ロジックは、ECUデバイスにおけるものと同様であり、簡潔にするために省略される。デバイスはアクセス・トークンを受信するときに、それは、最初にクレデンシャルとカウンタが有効であることを検証し、次いで、アクセス可能なターゲット、タイムスタンプ、及び署名が有効であることを順次確認する。検証に失敗するたびに試行回数が増加し、その数が3回を超えた場合（実際のニーズに従って定義可能であってもよい）、アクセスは、一定時間（10秒）制限されてもよい。試行回数と遅延タイマーに関してこれらの閾値を特定したとしても、それらは、車製造業者の方針に応じて調整可能とすることができる。鍵プロビジョニング・プロセス全体が正常に完了する場合、デバイスは、KDFと鍵メタデータを消去する。

【0181】

上記の処理は、グループ鍵、すなわちVSKを生成するためのトークンベース認証である。

【0182】

ステップ902で説明したように、通常、ECUデバイスはまだプロビジョニングされていないため、ECUデバイスでのローカル・カウンタは1に等しく、これは、PVK、すなわち図2bに示すプロビジョニング鍵がECUデバイスに対して既に設定されていること、言い換えれば、例えば図3aに示すフローに基づいて、ECUデバイスの設定が行われていることを意味し、この時点で、ECUデバイスは、グループ鍵（VSK）を生成する準備が整っている。したがって、プロビジョニング・ツールは、ゲートウェイがプロビジョニングの準備ができていると判定し、従って、認証要求と一致するアクセス・トークンとしてVSKを生成するためにKMSサーバから受信したアクセス・トークンを判定することができる。

【0183】

別の場合では、チャレンジが2に等しいときに、プロビジョニング・ツールは、認証要求に基づいて、ゲートウェイがVSKでプロビジョニングされたと判定し、この場合、ゲートウェイが依然としてゲートウェイ上でプロビジョニングを実行したい場合、それは、FSKに対応するアクセス・トークンを用いてゲートウェイにアクセスしなければならず、図10に示すアクセス・トークンの構造と組み合わせて、トークンベース認証中にゲートウェイ又はECUデバイスで有効性チェックを確実にするために、アクセス・トークン内の検証対象カウンタは2に等しいべきである。

【0184】

別の場合では、チャレンジが3に等しいときに、プロビジョニング・ツールは、認証要求に基づいて、ゲートウェイがVSKでプロビジョニングされたと判定し、この場合、ゲートウェイが依然としてゲートウェイ上でプロビジョニングを実行したい場合、それは、鍵更新に対応するアクセス・トークンを用いてゲートウェイにアクセスしなければならず、図10に示すアクセス・トークンの構造と組み合わせて、トークンベース認証中にゲートウェイ又はECUデバイスで有効性チェックを確実にするために、検証対象カウンタは3に等しいべきである。

【0185】

図9bでは、ゲートウェイがVSKを用いてプロビジョニングされておらず、そのため、プロビジョニング・ツールがグループ鍵に対応するアクセス・トークンを用いてチャレンジに応答する場合を単に説明する。可能な実装では、プロビジョニング・ツールが、認証要求と一致するアクセス・トークンを用いてゲートウェイ又はECUデバイスにアクセスするときであっても、ゲートウェイ又はECUデバイスによって拒否される可能性は依

10

20

30

40

50

然としてあり、これは、プロビジョニング・ツールのセキュリティを実際に考慮している。例えば、何らかの攻撃は、以前に使用されたトークン、期限切れのトークン、又は未認可のトークンを再使用する可能性がある。

【0186】

いずれにしても、プロビジョニング・ツールが認証要求と一致する正しいアクセス・トークンを有していない場合、それは、そのアクセス・トークンを更新する必要があることがある。プロビジョニング・ツールによる認証及び許可の検証のための可能なプロセスが図12に示されており、プロビジョニング・ツールは、ゲートウェイから否定的な応答を受信したときにアクセス・トークンを検証し、アクセス・トークンを更新してもよい。

【0187】

具体的には、図12に示すように、プロビジョニング・ツールがアクセス・トークンを受信すると、それは、ゲートウェイにUDS認証要求を送信してもよく、カウンタを含むチャレンジを受信し、次いで、プロビジョニング・ツールは、カウンタと一致するアクセス・トークンを判定し得る。

【0188】

カウンタと一致するアクセス・トークンがない場合、プロビジョニング・ツールは、更新されたアクセス・トークンを要求するためにKMSサーバにトークン更新要求を送信してもよく、KMSサーバは、プロビジョニング・ツールが自身のポリシーに従って、ゲートウェイをプロビジョニングすることを認可されているかどうかを判定し、そうである場合、KMSサーバは、プロビジョニング・ツールに更新されたトークンを送信してもよい。

【0189】

カウンタと一致するアクセス・トークンがある場合、プロビジョニング・ツールは、判定されたアクセス・トークンをゲートウェイに送信してもよく、アクセス・トークンがゲートウェイにおいて有効性チェックに失敗した場合、すなわち、アクセス・トークンがゲートウェイによって拒否された場合、プロビジョニング・ツールは、ゲートウェイから否定的な応答を受信すると、アクセス・ターゲット・チェック、タイムスタンプ・チェック、又は署名チェックのうちの1つが失敗したかをチェックしてもよい。アクセス・ターゲット・チェックの失敗は、ターゲット車両とのアクセス・トークンのアクセス要求のチェックにつながる可能性があり、タイムスタンプ・チェックの失敗は、先に説明されたようにトークン更新要求の送信につながる可能性があり、署名の失敗は検証鍵ID要求の送信につながる可能性があり、ゲートウェイは、検証鍵IDをチェックのためにプロビジョニング・ツールに送信する可能性があり、これは、結果的に、KMSサーバへのトークン更新要求で使用される。

【0190】

サプライヤからのプロビジョニング鍵の潜在的な漏洩に関する懸念があり得る。攻撃者がVSKを取得する場合、異なる部分や段階で管理されている少なくとも3種の情報を収集するべきである。

【0191】

1) プロビジョニング鍵： サプライヤ生産時にサプライヤ製造／プロビジョニング・ツールに配布される。

【0192】

2) 事前定義ストリング（例えば、図7bに示すソルトであってもよく、これは、他の後続秘密鍵の鍵導出に使用される）： サプライヤ生産の前にサプライヤ・セキュリティ管理者に配布される。

【0193】

3) 暗号化されたRS及びTS： 車両生産時にOEM製造／プロビジョニング・ツールに配布される。

【0194】

したがって、VSKが攻撃者にさらされた場合、情報がサプライヤ製造システム、サプライヤ・セキュリティ管理者、及びOEM製造システムのすべてから漏洩したことを意味

10

20

30

40

50

する。又は、ECUデバイスの保護メモリ（例えば、HSM）が危急化されている。

【0195】

本開示のセキュリティは、以下の理由により保証される。すなわち、各コンポーネントのセキュリティ管理及びシステムとプロビジョニング・ツールとの間のセキュア・チャネルの想定の下で、ディーラーシップ・プロビジョニング・ツールは、OEMの許可の下で出荷又は販売される特定の車両の一定のデバイスにのみアクセスすることができる（車両製造段階では使用されない）。このようなアフターマーケット・プロビジョニング・ツールのユース・ケースについては、次の部分で説明される。

【0196】

本開示の技術的解決策は、いくつかの技術的利点を提供してもよい。

10

【0197】

まず、それは、管理がしやすく、拡張が容易である。例えば、プロビジョニング・ツールは、各ECUに対するアクセス認可を取得する必要はなく、それらは、アクセス可能なターゲットを特定する1つのアクセス・トークンをサーバから取得するだけであり、さらに、プロビジョニング・ツール及びKMSサーバは、車両上のすべてのECUに対して単に1つのメッセージ（すなわち、プロビジョニング・ツールからECUデバイスへの第1のプロビジョニング・メッセージと、KMSサーバからプロビジョニング・ツールへの第2のプロビジョニング・メッセージであり、いずれのプロビジョニング・メッセージもプロビジョニング・データを含む）を管理する。さらに、技術的解決策は、（UDSのような）標準自動車プロトコルにわたって展開可能である。

20

【0198】

第2に、提案した解決策に基づいて、低トラフィックで高速動作を用いた大量生産に対して効率的になる。サプライヤは、ECUタイプの秘密を保持する必要があるだけであり（すべてのECUを異なって管理する必要はない）、OEM製造業者は、車両タイプに対するプロビジョニング・メッセージを単に1つ保持する。ECUデバイス又はゲートウェイにおいて鍵を自己生成することにより、情報が限定されたデータサイズの縮小が達成され、複数のデバイスに対して同時に鍵をセッティングすることも可能である。

【0199】

第3に、提案された解決策は、セキュリティ問題にも関係している。実際、いかなる秘密も他の外部システム及びツールと共有されず、従って、提案された解決策は、車両デバイスとKMSサーバとの間のエンドツーエンド・セキュリティを提供するだけでなく、各車両に対する鍵独立性及びKMSの署名からの鍵認証を提供する。さらに、それは、PKの利用と露出が非常に限られているため、暗号分析攻撃に対してロバストである。

30

【0200】

前述の解決策とは別に、本開示は、ディーラーシップ・プロビジョニング・ツールのための解決策も提供する。図13及び図14に示すように、それらは、ディーラーシップ・プロビジョニング・ツール（アフターマーケット・ツール、ここでのプロビジョニング・ツールは、ソフトウェア又はハードウェアとして実装されてもよい）のいくつかのユース・ケースを示す。図13に示す第1のケースは、部品交換（例えばECU交換）のためのものであり、図14に示す第2のケースは、FCKの更新のためのものである。ほとんどのプロセスは、上述と同じである。

40

【0201】

図13では、これらのテスターが新しい交換デバイスにアクセスするために、それらは、OEMから所望のデバイスに対するアクセス・トークンを取得しなければならない。プロビジョニング・ツールは、VIN（車両のアイデンティティ）及び新たなECU交換品（第1のデバイスの交換デバイス）のECUアイデンティティに従って、アクセス・トークン及びプロビジョニング・データの要求をサーバに送信し、対象車両（VINで識別）及び対象ECUデバイス（ECUアイデンティティで識別）にアクセスするために特定されたアクセス・トークン及びプロビジョニング・データを受信すると、プロビジョニング・ツールは、受信したアクセス・トークン及びプロビジョニング・データを用いてECU

50

交換をプロビジョニングしてもよく、特定の動作は、図 5 に示す第 1 のデバイスのプロビジョニングと同じであってもよい。E C U デバイスの交換は、E C U デバイスが損傷又は古いシナリオに適用されてもよく、テスターは、提案された方法を使用して、新しい E C U デバイスをプロビジョニングし、損傷又は古い E C U デバイスを新しいものと交換してもよい。

【0202】

同様に、テスターがいくつかの特定のキーを更新したい場合、それは、O E M の許可を用いて更新認可のための特別なアクセス・トークンを取得すべきである。これは、デバイスがより大きいカウンタ番号（例えば 2 より大きい）を提示するためである。具体的には、第 2 のデバイスは、第 1 のデバイスの機能秘密鍵を更新するための機能秘密アクセス・トークンを要求する要求をサーバに送信してもよく、要求を受信すると、サーバは、機能秘密アクセス・トークン及び対応する更新データを第 2 のデバイスに返してもよく、サーバから機能秘密アクセス・トークン及び対応する更新データを受信すると、第 2 のデバイスは、図 9 の機能秘密鍵のプロビジョニングと同様に第 1 のデバイスをプロビジョニングしてもよい。例えば、車両内の E C U デバイスの鍵を更新するプロセスを示す図 1 4 に示すように、特定のキー更新に対して、プロビジョニング・ツールは、E C U デバイスとのチャレンジ応答認可を実行し、チャレンジ内のカウンタ番号に対応するアクセス・トークンをサーバに要求し、サーバから返されたアクセス・トークン及び更新データを用いて、プロビジョニング・ツールが E C U デバイス内の鍵を更新することが可能となる。トークン更新の詳細については、図 1 2 及び関連する説明を参照されたい。

【0203】

図 1 5 は、本開示の一実施形態による、第 1 のデバイスの概略構造図を示す。第 1 のデバイスは、車両に搭載されてもよい。第 1 のデバイス 1 5 0 0 は、受信モジュール 1 5 0 1 と、判定モジュール 1 5 0 2 と、送信モジュール 1 5 0 3 と、生成モジュール 1 5 0 4 と、を含む。

【0204】

受信モジュール 1 5 0 1 は、第 1 のデバイスへのアクセスを要求するアクセス要求を第 2 のデバイスから受信するように構成されており、判定モジュール 1 5 0 2 は、アクセス要求に基づいて、第 2 のデバイスが第 1 のデバイスへのアクセスを許可されているかどうかを判定するように構成されており、送信モジュール 1 5 0 3 は、判定に基づいて、第 2 のデバイスにアクセス応答を送信するように構成されており、受信モジュール 1 5 0 1 は、第 2 のデバイスから第 1 のプロビジョニング・メッセージを受信するようにさらに構成されており、第 1 のプロビジョニング・メッセージは、グループ鍵を生成するためのプロビジョニング・データを含み、グループ鍵は、車両内の第 1 のデバイス間で共有され、生成モジュール 1 5 0 4 は、プロビジョニング・データに従って、グループ鍵を生成するように構成されている。

【0205】

可能な実装では、判定モジュール 1 5 0 2 は、具体的には、アクセス要求がトリガされると、第 2 のデバイスの権限を検証するための認証要求を第 2 のデバイスに送信することと、認証要求と一致するアクセス・トークンを第 2 のデバイスから受信することと、受信したアクセス・トークンが有効であるかどうかを判定することと、を行うように構成されている。

【0206】

送信モジュール 1 5 0 3 は、受信したアクセス・トークンが有効であると判定すると、肯定的なアクセス応答を第 2 のデバイスに送信することと、受信したアクセス・トークンが無効であると判定すると、否定的なアクセス応答を第 2 のデバイスに送信することと、を行うように構成されている。

【0207】

可能な実装では、第 1 のデバイスは、サーバからローカル・プロビジョニング・データを取得するように構成されている取得モジュールをさらに含み、ローカル・プロビジョニ

ング・データは、プロビジョニング鍵、公開鍵、及びローカル・タイムスタンプを含み、プロビジョニング鍵は、グループ鍵を生成するように構成されており、公開鍵は、第2のデバイスの権限を検証するように構成されており、ローカル・タイムスタンプは、生成されたプロビジョニング鍵の有効性を検証するように構成されている。

【0208】

可能な実装では、プロビジョニング・データは、プロビジョニング鍵によって暗号化されたランダム・ストリング、プロビジョニング鍵によって暗号化されたプロビジョニング・タイムスタンプ、及び検証署名を含む。

【0209】

生成モジュール1504は、プロビジョニング鍵を使用して、プロビジョニング・データを復号し、ランダム・ストリング及びプロビジョニング・タイムスタンプを取得することと、ランダム・ストリング及びプロビジョニング・タイムスタンプに従って、グループ鍵を生成することと、検証署名に従って、生成されたプロビジョニング鍵の有効性を検証することと、を行うように構成されている。

【0210】

可能な実装では、アクセス・トークンは、第1の事前定義されたアルゴリズムに基づいて生成された検証対象クレデンシャル、検証対象カウンタ、検証対象タイムスタンプ、少なくとも1つの検証対象車両アイデンティティ、及び検証対象署名を含む。

【0211】

判定モジュール1502は、具体的には、条件が満たされる場合、受信したアクセス・トークンが無効であると判定するように構成されており、条件は、ローカル・カウンタ及び第1の事前定義されたアルゴリズムに基づいて生成されたローカル・クレデンシャル及び第1の所定のアルゴリズムが検証対象クレデンシャルと不整合であること、ローカル・カウンタが検証対象カウンタと不整合であること、ローカル・タイムスタンプが検証対象タイムスタンプよりも遅いこと、第1のデバイスが属する車両のアイデンティティが少なくとも1つの検証対象車両アイデンティティと不整合であること、及び検証対象署名を公開鍵でチェックすることに失敗することのうちのいずれか1つ以上を含む。

【0212】

可能な実装では、アクセス・トークンは、車両タイプ、デバイス・タイプ及びデバイス識別子のリストのうちのいずれか1つ以上を含む。

【0213】

可能な実装では、認証要求は、ローカル・カウンタを含み、ローカル・カウンタは、第1のデバイスのプロビジョニング状態を反映するように構成されており、カウンタの値は、第1のデバイスのプロビジョニング状態が変更されると、第1のデバイスによりプリセットされた規則に基づいて変更される。

【0214】

可能な実装では、送信モジュール1503は、第1のプロビジョニング応答を第2のデバイスに送信するようにさらに構成されている。

【0215】

可能な実装では、受信モジュール1501は、第2のデバイスから、第1のデバイスに対する機能秘密鍵をプロビジョニングするためのプロビジョニング要求を受信するようにさらに構成されており、生成モジュール1504は、グループ鍵及び事前記憶されたデータに基づいて、機能秘密鍵を生成するようにさらに構成されており、送信モジュール1503は、第2のプロビジョニング応答を第2のデバイスに送信するようにさらに構成されている。

【0216】

可能な実装では、受信モジュール1501は、第3のデバイスから鍵確認チャレンジを受信するようにさらに構成されており、第2のデバイスから機能秘密鍵が正しく生成されたかを確認するための鍵確認要求を受信すると、鍵確認チャレンジが第3のデバイスによ

10

20

30

40

50

って送信され、生成モジュール1504は、鍵確認チャレンジ、機能秘密鍵、及び第2の事前定義されたアルゴリズムに従って、鍵確認応答を生成するようにさらに構成されており、送信モジュール1503は、鍵確認応答を第3のデバイスに送信するようにさらに構成されている。

【0217】

本開示によって提供される解決策によれば、車両内のすべてのECUデバイスに、プロビジョニング・データを含む1つのプロビジョニング・メッセージによってグループ鍵をプロビジョニングすることができる。このようにして、鍵プロビジョニングの効率が改善され、プロビジョニング・コストが低減される。生成されたグループ鍵を使用して、ECUデバイスに関連付けられたデータ通信のセキュリティが確保される。さらに、ECUデバイスにおける鍵を自己生成することにより、情報が限定されたデータサイズの縮小が達成され、複数のデバイスに対して同時に鍵をセッティングすることも可能である。

【0218】

第1のデバイスは、上述の方法の実施形態のいずれか1つにおける技術的解決策を実装するように適用されてもよい。実装原理及びその技術的效果は同様であり、本明細書では説明されない。

【0219】

図16は、本開示の一実施形態による、第2のデバイスの概略構造図を示す。第2のデバイス1600は、送信モジュール1601及び受信モジュール1602を含む。

【0220】

送信モジュール1601は、第1のデバイスに第1のデバイスへのアクセスを要求するためのアクセス要求を送信するように構成されており、第1のデバイスは、車両に搭載され、受信モジュール1602は、第1のデバイスからアクセス応答を受信するように構成されており、アクセス応答は、アクセス要求に基づいて、第1のデバイスによって返され、送信モジュール1601は、第1のプロビジョニング・メッセージを第1のデバイスに送信するようにさらに構成されており、第1のプロビジョニング・メッセージは、第1のデバイスによって、グループ鍵を生成するためのプロビジョニング・データを含み、グループ鍵は、車両内の第1のデバイス間で共有される。

【0221】

可能な実装では、送信モジュール1601は、グループ鍵に対応するアクセス・トークンを要求するためのトークン要求をサーバに送信するようにさらに構成されており、トークン要求は、第2のデバイスがプロビジョニングしようとしている複数の車両の1つ以上のアイデンティティを含み、第1のデバイスが属する車両は、複数の車両に含まれ、受信モジュール1602は、サーバから、グループ鍵に対応するアクセス・トークン及びアクセス・トークンに対応する第2のプロビジョニング・メッセージを受信するようにさらに構成されている。

【0222】

可能な実装では、受信モジュール1602は、第1のデバイスから、第2のデバイスの権限を検証するための認証要求を受信するようにさらに構成されている。

【0223】

第2のデバイスは、判定モジュールをさらに含み、判定モジュールは、認証要求と一致するアクセス・トークンを判定するようにさらに構成されており、送信モジュール1601は、認証要求と一致するアクセス・トークンを第1のデバイスに送信するようにさらに構成されている。

【0224】

可能な実装では、判定モジュールは、認証要求に従って、第1のデバイスのプロビジョニング状態を判定することと、第1のデバイスのグループ鍵が第1のデバイスによって生成されないと判定すると、グループ鍵に対応するアクセス・トークンを、認証要求に一致するアクセス・トークンとして使用することと、を行うようにさらに構成されている。

【0225】

可能な実装では、受信モジュール1602は、第1のデバイスから否定的なアクセス応答を受信するように構成されており、アクセス応答は、アクセス要求に基づいて第1のデバイスによって返され、送信モジュール1601は、第1のデバイスに対するアクセス・トークンを更新するためのトークン更新要求をサーバに送信することと、グループ鍵に対応するアクセス・トークンとして、更新されたアクセス・トークンをサーバから受信することと、を行うようにさらに構成されている。

【0226】

可能な実装では、受信モジュール1602は、第1のデバイスから第1のプロビジョニング応答を受信するようにさらに構成されている。

【0227】

送信モジュール1601は、第1のプロビジョニング応答が、グループ鍵が第1のデバイスによって正常に生成されたことを示すときに、第1のデバイスに対して機能秘密鍵をプロビジョニングするためのプロビジョニング要求を送信するようにさらに構成されている。

【0228】

受信モジュール1602は、第1のデバイスから第2のプロビジョニング応答を受信するようにさらに構成されている。

【0229】

可能な実装では、送信モジュール1601は、第1のデバイスの交換デバイスに対するアクセス・トークンを要求するための要求をサーバに送信するようにさらに構成されており、受信モジュール1602は、サーバから、グループ鍵に対応するアクセス・トークンを受信することと、受信したアクセス・トークンを使用して、交換デバイスをプロビジョニングすることと、を行うようにさらに構成されている。

【0230】

本開示によれば、第2のデバイスは、車両内の第1のデバイスにアクセスし、車両内のすべての第1のデバイスに対してグループ鍵を1つのプロビジョニング・メッセージで設定することが可能であり、それによってたとえそれが多くのデバイス及び多くの車両に対して展開されたとしても、トラフィック・オーバーヘッド及びネットワーク伝送及び動作遅延を低減する。

【0231】

第2のデバイスは、上述の方法の実施形態のいずれか1つにおける技術的解決策を実装するように適用されてもよい。実装原理及びその技術的効果は同様であり、本明細書では説明されない。

【0232】

図17は、本開示の一実施形態による、サーバの概略構造図である。サーバ1700は、受信モジュール1701及び送信モジュール1702を含む。

【0233】

受信モジュール1701は、第4のデバイスから第1のデバイスを設定するための設定要求を受信するように構成されており、設定要求は、第1のデバイスが属する車両のアイデンティティを含み、第1のデバイスは、車両に搭載され、送信モジュール1702は、第4のデバイスにローカル・プロビジョニング・データを送信するように構成されており、ローカル・プロビジョニング・データは、第1のデバイスのグループ鍵を生成するように構成されており、グループ鍵は、車両内の第1のデバイス間で共有される。

【0234】

可能な実装では、受信モジュール1701は、第2のデバイスからトークン要求を受信するようにさらに構成されており、トークン要求は、第2のデバイスがプロビジョニングしようとして計画している1つ以上の車両のアイデンティティを含み、第1のデバイスが属する車両は、複数の車両に含まれ、送信モジュール1702は、トークン要求に対応するアクセス・トークン及びアクセス・トークンに対応する第2のプロビジョニング・メッセージを第2のデバイスに送信するようにさらに構成されている。

【0235】

可能な実装では、受信モジュール1701は、第2のデバイスから、第1のデバイスに対するアクセス・トークンを更新するためのトークン更新要求を受信し、トークン更新要求に従って、更新されたアクセス・トークンを第2のデバイスに送信するようにさらに構成されている。

【0236】

サーバは、上述の方法の実施形態のいずれか1つにおける技術的解決策を実装するように適用されてもよい。実装原理及びその技術的効果は同様であり、本明細書では説明されない。

【0237】

図18は、本開示の一実施形態による第1のデバイスの概略ブロック図である。

【0238】

図18に示すように、本開示の一実施形態は、第1のデバイス1800をさらに提供する。デバイス1800は、図15のデバイス1500であってもよく、これは、方法の実施形態における方法に対応する第1のデバイスに関するコンテンツを実装するように構成され得る。デバイス1800は、入力インターフェース1810、出力インターフェース1820、プロセッサ1830、及びメモリ1840を含む。入力インターフェース1810、出力インターフェース1820、プロセッサ1830、及びメモリ1840は、バス・システムにより接続され得る。メモリ1840は、プログラム、命令又はコードを記憶するように構成されている。プロセッサ1830は、メモリ1840内のプログラム、命令又はコードを実行して、入力インターフェース1810を制御して、信号を受信し、出力インターフェース1820を制御して、信号を送信し、前述の方法の実施形態における動作を完了するように構成されている。

【0239】

具体的な実装では、図15に示すデバイス1500内の送信モジュール1503は、図18の出力インターフェース1820を用いて実装されてもよく、また、受信モジュール1501は、図18の入力インターフェース1810を用いて実装されてもよく、図15に示すデバイス1500内の判定モジュール1502及び生成モジュール1504は、図18のプロセッサ1830を用いて実装されてもよい。

【0240】

図19は、本開示の一実施形態による、第2のデバイスの概略ブロック図である。

【0241】

図19に示すように、本開示の一実施形態は、第1のユーザ・デバイス1900をさらに提供する。デバイス1900は、図16のデバイス1600であってもよく、これは、方法の実施形態における方法に対応する第1のデバイスに関するコンテンツを実装するように構成され得る。デバイス1900は、入力インターフェース1910、出力インターフェース1920、プロセッサ1930、及びメモリ1940を含む。入力インターフェース1910、出力インターフェース1920、プロセッサ1930、及びメモリ1940は、バス・システムにより接続され得る。メモリ1940は、プログラム、命令又はコードを記憶するように構成されている。プロセッサ1930は、メモリ1940内のプログラム、命令又はコードを実行して、入力インターフェース1910を制御して、信号を受信し、出力インターフェース1920を制御して、信号を送信し、前述の方法の実施形態における動作を完了するように構成されている。

【0242】

特定の実装では、図16に示すデバイス1600内の送信モジュール1601は、図19の出力インターフェース1920を用いて実装されてもよく、また、受信モジュール1602は、図19の入力インターフェース1910を用いて実装されてもよい。

【0243】

図20は、本開示の一実施形態による、サーバの概略ブロック図である。

【0244】

図 20 に示すように、本開示の一実施形態は、第 1 のユーザ・デバイス 2000 をさらに提供する。デバイス 2000 は、図 17 のデバイス 1700 であってもよく、これは、方法の実施形態における方法に対応する第 1 のデバイスに関するコンテンツを実装するように構成され得る。デバイス 2000 は、入力インターフェース 2010、出力インターフェース 2020、プロセッサ 2030、及びメモリ 2040 を含む。入力インターフェース 810、出力インターフェース 2020、プロセッサ 2030、及びメモリ 2040 は、バス・システムにより接続され得る。メモリ 2040 は、プログラム、命令又はコードを記憶するように構成されている。プロセッサ 2030 は、メモリ 2040 内のプログラム、命令又はコードを実行して、入力インターフェース 2010 を制御して、信号を受信し、出力インターフェース 2020 を制御して、信号を伝送し、前述の方法の実施形態における動作を完了するように構成されている。

10

【0245】

特定の実装では、図 17 に示すデバイス 1700 内の送信モジュール 1702 は、図 20 の出力インターフェース 2020 を用いて実装されてもよく、また、受信モジュール 1701 は、図 20 の入力インターフェース 2010 を用いて実装されてもよい。

【0246】

本開示はまた、コンピュータ実行可能な命令を記憶するコンピュータ記憶媒体を提供し、このコンピュータ実行可能な命令は、実行されるときに、本開示の実施形態による方法を実装する。

【0247】

本開示はまた、命令を含むコンピュータ・プログラム製品に関連し、この命令は、コンピュータ上で実行されるときに、コンピュータに上述の実施形態における方法を実行させる。

20

【0248】

例えば、説明された方法に関連する開示は、当該方法を行うように構成された対応するデバイス又はシステムについても真であり、その逆もまた真であり得ることが理解される。例えば、1 つ又は複数の特定の方法ステップが説明される場合、対応するデバイスは、説明された 1 つ又は複数の方法ステップを行う（例えば、1 つのユニットが 1 つ又は複数のステップを行うか、又は複数のユニットの各々が複数のステップのうちの 1 つ以上を行う）ために、1 つ又は複数のユニット、例えば、機能ユニットを、たとえそのような 1 つ以上のユニットが明示的に説明されるか、図に示されていなくても、含んでもよい。

30

一方、例えば、1 つ又は複数のユニット、例えば、機能ユニットに基づいて特定の装置が説明される場合、対応する方法は、1 つ又は複数のユニットの機能性を行う（例えば、1 つのステップが 1 つ又は複数のユニットの機能性を行うか、又は複数のユニットのうちの各々が複数のユニットのうちの 1 つ以上の機能性を行う複数のステップ）ために、1 つのステップを、たとえそのような 1 つ又は複数のステップが明示的に説明されるか、図に示されていなくても、含んでもよい。

さらに、本明細書で説明された種々の例示的な実施形態及び／又は態様の特徴は、特に断らない限り、互いに組み合わせてもよいことが理解される。

【0249】

本開示の明細書及び請求項並びに上記の図面における「第 1」、「第 2」などの用語は、異なる対象を区別することを意図しているが、特定の順序を定義することを意図していない。

40

【0250】

本開示の実施形態における「及び／又は」などの用語は、関連付けられたオブジェクト間の関連付けを説明するために使用されるにすぎず、これは、3 つの関係があり得ることを示し、例えば、A 及び／又は B は、A のみの存在、A と B の両方の存在、及び B のみの存在を示してもよい。

【0251】

本開示の実施形態では、「例示的」、「例えば」などの表現は、例又は具体例の例示を

50

示すために使用される。本開示の実施形態では、「例示的」又は「例えば」として説明された任意の実施形態又は設計スキームは、他の実施形態又は設計スキームよりも好ましい又は有利であると解釈されるべきではない。特に、「例示的」又は「例えば」の使用は、特定の方式に関連概念を提示することを目的としている。

【0252】

1つ以上の例では、説明された機能は、ハードウェア、ソフトウェア、ファームウェア、又はそれらの任意の組み合わせで実装されてもよい。ソフトウェアで実装される場合、機能は、コンピュータ可読媒体上の1つ以上の命令又はコードとして記憶又は伝送され、ハードウェアベース処理ユニットによって実行されてもよい。コンピュータ可読媒体は、データ記憶媒体のような有形媒体に対応するコンピュータ可読記憶媒体、又は、例えば通信プロトコルに従って、ある場所から他の場所へのコンピュータ・プログラムの転送を容易にする任意の媒体を含む通信媒体を含んでもよい。このようにして、コンピュータ可読媒体は、一般に、(1) 非一時的である有形のコンピュータ可読記憶媒体、又は(2) 信号又は搬送波などの通信媒体に対応し得る。データ記憶媒体は、本開示で説明される技術の実装のための命令、コード及び／又はデータ構造を検索するために、1つ以上のコンピュータ又は1つ以上のプロセッサによってアクセス可能な任意の利用可能な媒体であり得る。コンピュータ・プログラム製品は、コンピュータ可読記憶媒体を含んでもよい。

【0253】

一例として、限定するものではないが、このようなコンピュータ可読記憶媒体は、RAM、ROM、EEPROM、CD-ROM又は他の光ディスク記憶デバイス、磁気ディスクストレージ、又は他の磁気記憶デバイス、フラッシュメモリ、又は命令又はデータ構造の形式で所望のプログラム・コードを記憶するために使用することができ、コンピュータによってアクセスすることができる他の任意の媒体を含むことができる。また、任意の接続は、適切にコンピュータ可読媒体と呼ばれる。例えば、同軸ケーブル、光ファイバケーブル、ツイスト・ペア、デジタル加入者線(DSL)、又は赤外線、無線、及びマイクロ波などの無線技術を用いて、ウェブサイト、サーバ、又は他のリモート・ソースから命令が伝送される場合、同軸ケーブル、光ファイバケーブル、ツイスト・ペア、DSL、又は赤外線、無線、及びマイクロ波のような無線技術は、媒体の定義に含まれる。しかしながら、コンピュータ可読記憶媒体及びデータ記憶媒体は、接続、搬送波、信号、又は他の一時的な媒体を含まず、代わりに非一時的で有形の記憶媒体に向けられると理解されたい。ディスクは、本明細書で使用する場合、コンパクトディスク(CD)、レーザディスク、光ディスク、デジタル多用途ディスク(DVD)、フロッピー・ディスク及びブルーレイ・ディスクを含み、ディスクは、通常、磁氣的にデータを再生し、ディスクは光学的にレーザでデータを再生する。上記の組み合わせはまた、コンピュータ可読媒体の範囲に含まれるべきである。

【0254】

命令は、1つ以上のデジタル信号プロセッサ(DSP)、汎用マイクロプロセッサ、特定用途向け集積回路(ASIC)、フィールド・プログラマブル論理アレイ(FPGA)、又は他の同等の集積又は個別論理回路などの1つ以上のプロセッサによって実行されてもよい。したがって、本明細書で使用する用語「プロセッサ」は、前述の構造のいずれか、又は本明細書で説明される技術の実装に好適な他の構造を指してもよい。追加的に、いくつかの態様において、本明細書で説明される機能は、符号化及び復号のために構成される専用ハードウェア及び／又はソフトウェア・モジュール内に提供されてもよく、又は組み合わされたコーデックに組み込まれてもよい。また、この技術は、1つ以上の回路又は論理素子で完全に実装することができる。

【0255】

この開示の技法は、無線ハンドセット、集積回路(IC)又はICのセット(例えば、チップセット)を含む、多種多様なデバイス又は装置で実装されてもよい。様々なコンポーネント、モジュール、又はユニットが、開示された技法を実行するように構成されたデバイスの機能的態様を強調するために本開示において説明されているが、必ずしも異なる

ハードウェア・ユニットによる実現を必要としない。むしろ、上述のように、様々なユニットが、コーデック・ハードウェア・ユニット内で組み合わせられてもよく、又は、適切なソフトウェア及び／又はファームウェアと共に、上述の1つ以上のプロセッサを含む、相互動作可能なハードウェア・ユニットの集合によって提供されてもよい。

【0256】

コンピュータ可読非一時的媒体は、磁気記憶媒体、光学記憶媒体、及び固体記憶媒体を含むすべてのタイプのコンピュータ可読媒体を含み、特に信号を除く。ソフトウェアは、ルータ、クライアント、又は他のネットワークデバイスにインストールして販売することができる。代替的には、ディスク媒体を介して、又は例えば、ソフトウェア作成者によって所有されるサーバから、若しくはソフトウェア作成者によって所有されていないが使用されているサーバからなどを含む任意の方式のネットワーク又は配布システムからソフトウェアを取得することを含めて、ソフトウェアを取得してデバイスにロードすることができる。ソフトウェアは、例えば、インターネットを介して配布するためにサーバ上に記憶され得る。

【0257】

請求項では、語句「comprising」は、他の要素又はステップを排除せず、不定冠詞「a」又は「an」は、複数を排除しない。単一プロセッサ又は他のユニットは、請求項に規定された複数の項目の機能を満たしてもよい。一定の措置が相互に異なる従属請求項に規定されているという事実だけでは、これらの措置の組み合わせが有利に使用できないことを示さない、排除しない、又は示唆しない。コンピュータ・プログラムは、他のハードウェアと共に、又はその一部として供給される光学記憶媒体、固体媒体などの好適な媒体上に記憶又は配布されてもよいが、インターネット、他の有線又は無線電気通信システムなどの他の形態でも配布されてもよい。

【0258】

前述の詳細な説明は、例示及び説明の目的で提示されている。網羅的であることも、本明細書で請求項に記載される主題を開示された正確な形態に限定することも意図されていない。上記の教示に照らして、多くの修正及び変形が可能である。説明された実施形態は、開示された技術の原理及びその実際的な適用を最もよく説明するために選択されており、それによって、当業者は、様々な実施形態において、及び企図された特定の使用に好適な様々な修正を用いて、その技術を最もよく利用することが可能となる。開示の範囲は、本明細書に添付された請求項によって定義されることが意図される。

10

20

30

40

50

【図面】

【図 1】

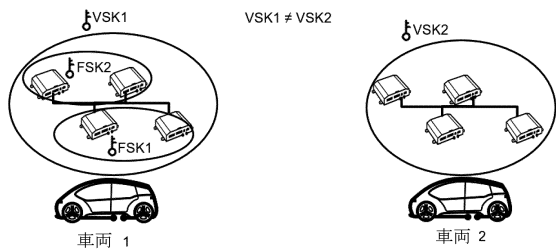


FIG. 1

【図 2 a】

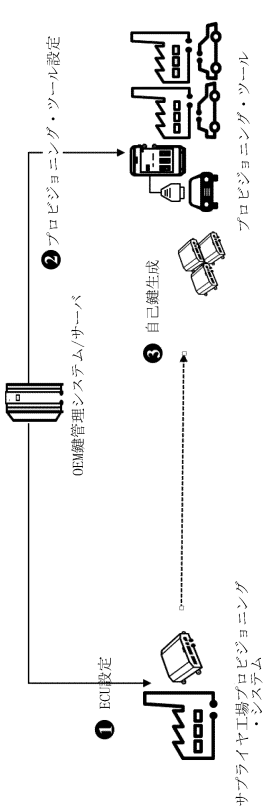


FIG. 2a

10

20

30

40

50

【図 3 a】



FIG. 3a

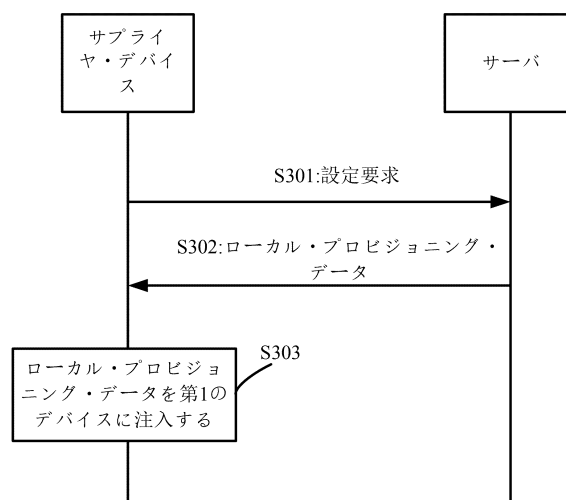


FIG. 3a

【図 4 a】

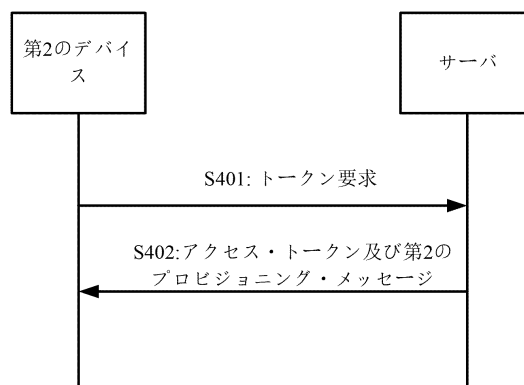


FIG. 4a

【図 5】

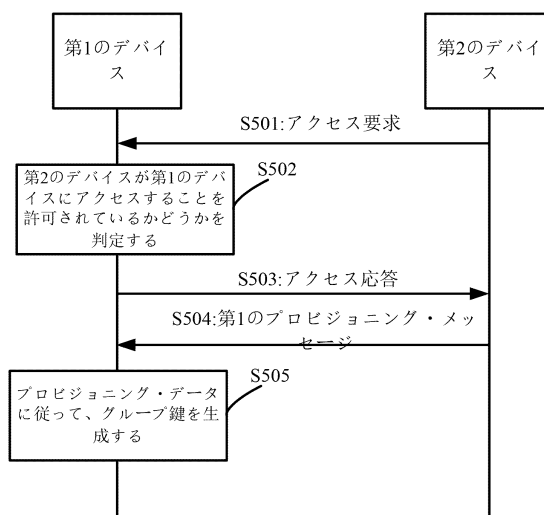


FIG. 5

FIG. 4b

【図 6 b】

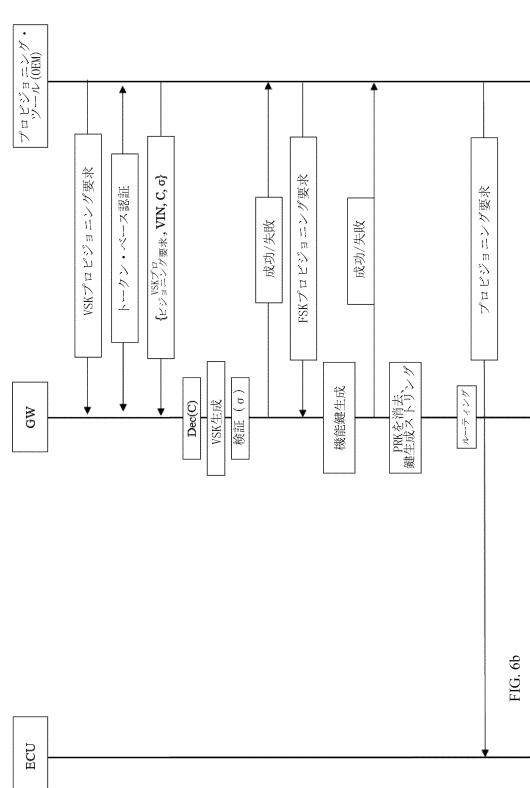
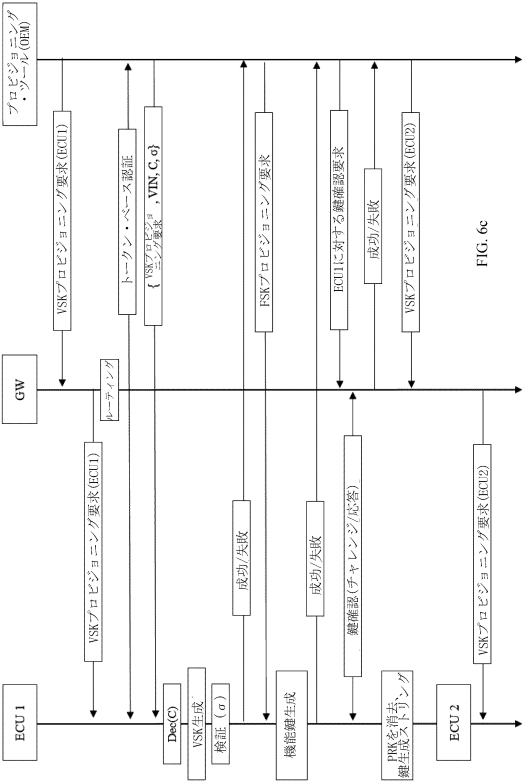


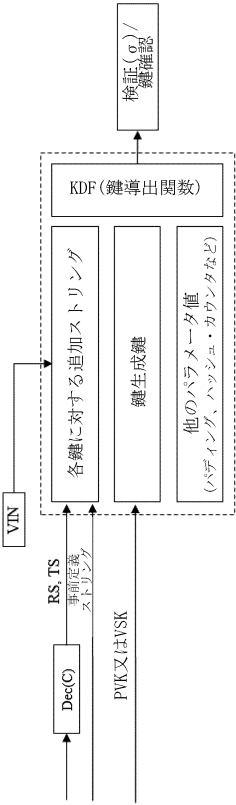
FIG. 6a

FIG. 6b

【図 6 c】



【図 7 a】



【図 7 b】

FSKの例	ユース・ケース	鍵/ パスワード	ソルト (事前定義 ストリング)	乱数/ コスト・ フラクタ
E2E鍵	ECUとRMSとの間のエンドツーエンド	VSK	Part# UID "e2e"	1024
SecOC鍵	セキュア・オンボード通信	VSK	"secoc-app-key"	1024
TLS PSK	PSKベースTLS	VSK	"tls-aes-gcm-key"	1024
認証鍵 (AUK)	車両内のECU間の認証又はUDS認証	VSK	"uds-seed-key"	1024
鍵更新鍵	鍵暗号化鍵	VSK	Vin番号	1024

FIG. 7b

【図 8】

```
Self Key Generator := {  
  KDF,  
  Secret key in secure storage,  
  Key Meta := {  
    additional input strings,  
    pre-defined strings,  
    iterations,  
    paddings  
  }  
}
```

FIG. 8

10

20

30

40

50

【図 9 a】

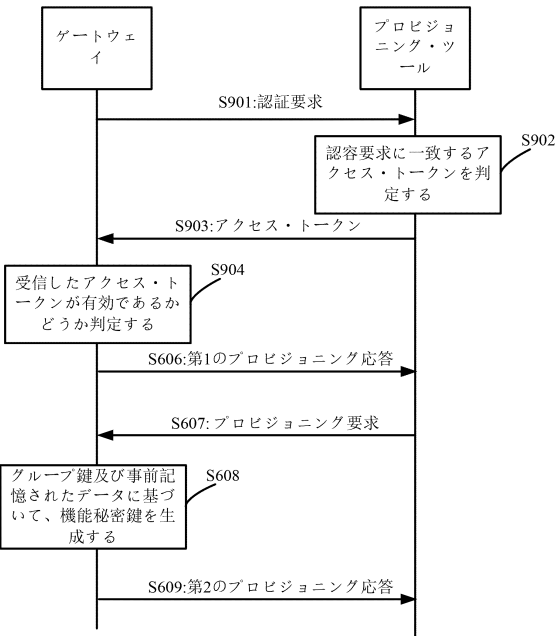


FIG. 9a

【図 9 b】

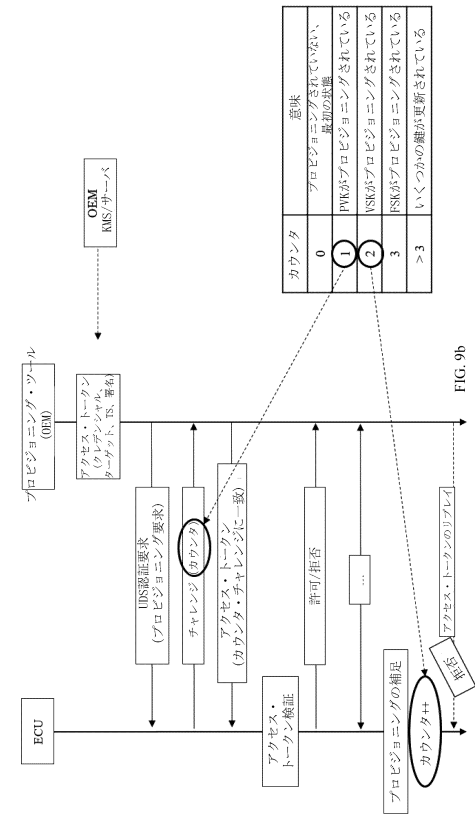


FIG. 9b

【図 10】

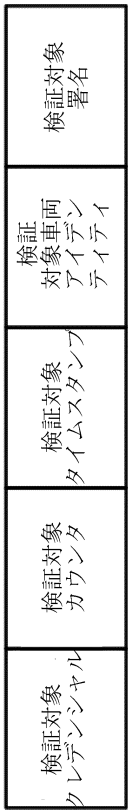


FIG. 10

【図 11】

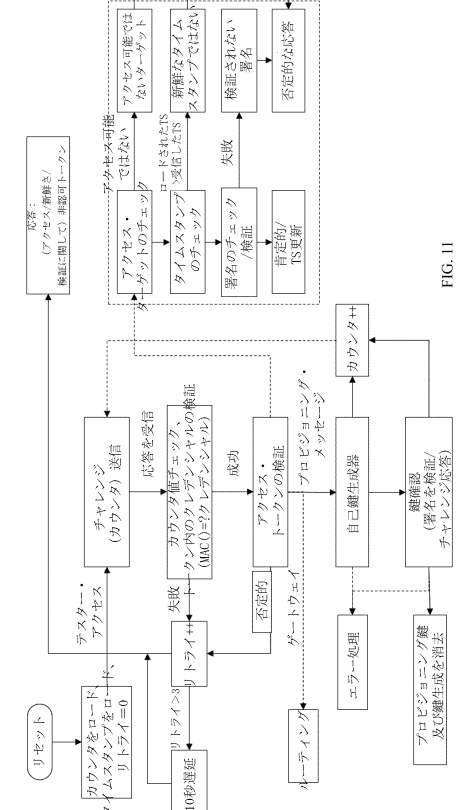
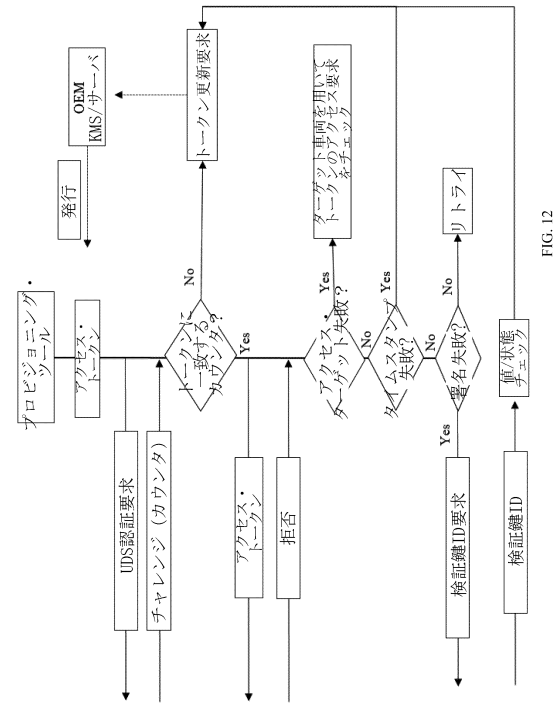


FIG. 11

【図 1 2】



【図 1 3】

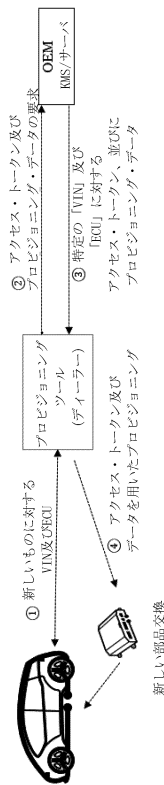


FIG. 13

【図 1 4】

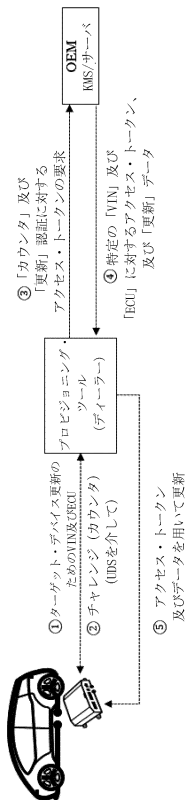


FIG. 14

【図 1 5】

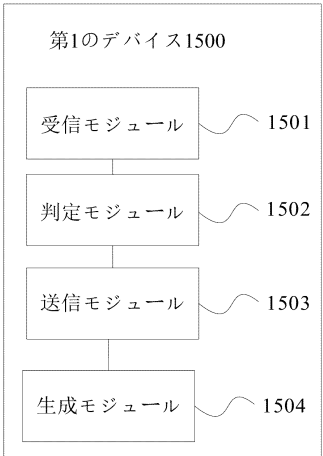


FIG. 15

【図 1 6】

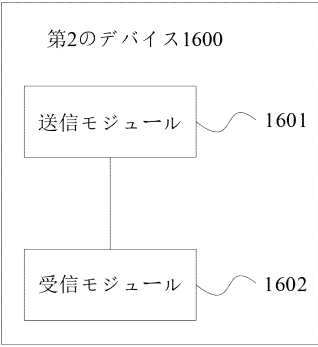


FIG. 16

【図 1 7】

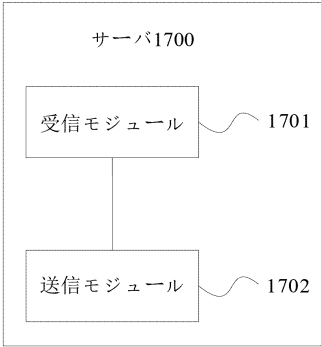


FIG. 17

10

【図 1 8】

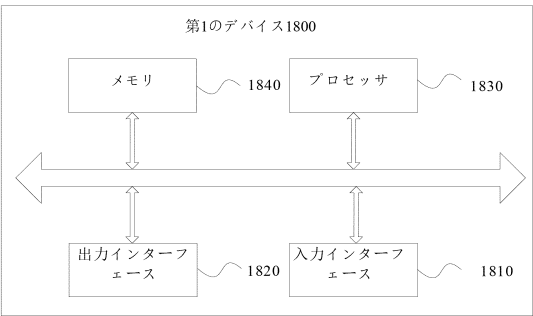


FIG. 18

【図 1 9】

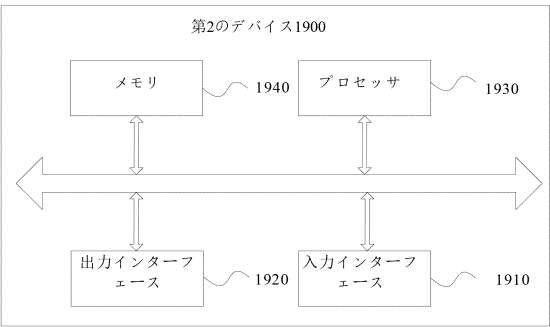


FIG. 19

20

【図 2 0】

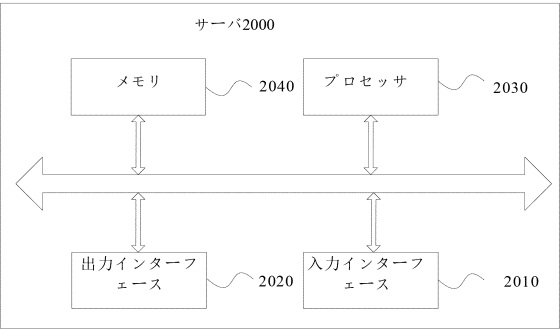


FIG. 20

30

40

50

フロントページの続き

- イ インターナショナル プライベート リミテッド
- (72)発明者 ウエイ, ジュオ
シンガポール共和国, シンガポール 138589 ザ・メトロポリス・タワー・2, #17-08
, 11 ノース・ブオナ・ヴィスタ・ドライブ, ファーウェイ インターナショナル プライベート
リミテッド
- (72)発明者 ジョオン, スティーブン イン
シンガポール共和国, シンガポール 138589 ザ・メトロポリス・タワー・2, #17-08
, 11 ノース・ブオナ・ヴィスタ・ドライブ, ファーウェイ インターナショナル プライベート
リミテッド
- 審査官 中里 裕正
- (56)参考文献 特開2020-048203 (JP, A)
特開2017-225186 (JP, A)
特開2013-142963 (JP, A)
特開2020-036234 (JP, A)
菅島健司 他, セキュアかつ効率的な車載鍵管理の提案, 2016年暗号と情報セキュリティシ
ンポジウム, 2016年01月22日, pp.1-6
- (58)調査した分野 (Int.Cl., DB名)
H04L 9/08
H04L 9/32
G06F 21/44