(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-506208
(P2018-506208A)
(43)公表日　平成30年3月1日(2018.3.1)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104
G09C 1/00	(2006.01)	G09C	1/00	640E	5K067
H04W 4/48	(2018.01)	H04W	4/04	115	
H04W 8/00	(2009.01)	H04W	8/00	110	
H04W 84/10	(2009.01)	H04W	84/10	110	

審査請求 未請求　予備審査請求 未請求　（全 21 頁）　最終頁に続く

(21)出願番号　特願2017-533861 (P2017-533861)
(86)(22)出願日　平成27年12月22日 (2015.12.22)
(85)翻訳文提出日　平成29年8月3日 (2017.8.3)
(86)国際出願番号　PCT/FR2015/053717
(87)国際公開番号　WO2016/102887
(87)国際公開日　平成28年6月30日 (2016.6.30)
(31)優先権主張番号　1403002
(32)優先日　平成26年12月23日 (2014.12.23)
(33)優先権主張国　フランス(FR)

(71)出願人　516000549
ヴァレオ、コンフォート、アンド、ドライビング、アシスタンス
VALEO COMFORT AND DRIVING ASSISTANCE
フランス国クレテイユ、セデックス、リュ、オーギュスト、ペレ、７６－ゼッドイ、ウーロパルク
(74)代理人　100091982
弁理士　永井　浩之
(74)代理人　100091487
弁理士　中村　行孝
(74)代理人　100082991
弁理士　佐藤　泰和

最終頁に続く

(54)【発明の名称】ＢＬＥプロトコルに従って作動可能であるモバイル装置と自動車両との間の自動認識のための方法

(57)【要約】
本発明は、モバイル電子装置（ＳＰ）と電子伝達モジュール（１２０）を有する自動車両（Ｖｉ）との間の自動認識のための方法であって、前記モバイル電子装置（ＳＰ）と前記車両（Ｖｉ）の電子モジュール（１２０）はＢＬＥプロトコルに従って動作可能であり、前記モバイル電子装置（ＳＰ）は「スキャン」モードにあるとともに前記車両（Ｖｉ）は「公示」モードにあり、前記方法は、‐前記車両（Ｖｉ）の前記電子モジュール（１２０）において、前記車両（Ｖｉ）の識別データ要素（ＲＰＡｉ）を取得するステップと、
‐前記車両（Ｖｉ）の前記識別データ要素（ＲＰＡｉ）を備える少なくとも１つのデータフレーム（Ｔｄ）を、前記車両（Ｖｉ）の前記電子モジュール（１２０）から前記モバイル電子装置（ＳＰ）に発信するステップと、
‐「スキャン」モードに設定された前記モバイル電子装置（ＳＰ）において、前記車両（Ｖｉ）の前記識別データ要素（ＲＰＡｉ）を含む前記少なくとも１つのデータフレーム（Ｔｄ）を受信するステップと、‐前記モバイル電子装置（ＳＰ）において、発信された前記識別デー

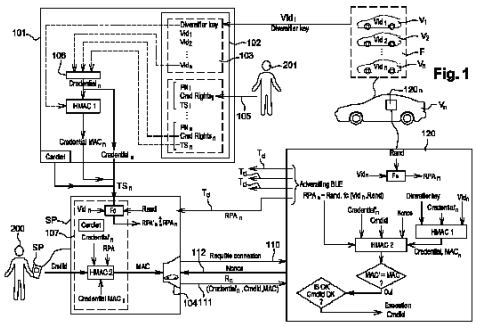
Fig.1

【特許請求の範囲】
【請求項１】
モバイル電子装置（ＳＰ）と電子伝達モジュール（１２０）を有する自動車両（Ｖｉ）との間の自動認識のための方法であって、前記モバイル電子装置（ＳＰ）と前記車両（Ｖｉ）の電子モジュール（１２０）はＢＬＥプロトコルに従って動作可能であり、前記モバイル電子装置（ＳＰ）はスキャンモードにあるとともに前記車両（Ｖｉ）はアドバタイジングモードにあり、前記方法は、
‐前記車両（Ｖｉ）の前記電子モジュール（１２０）において、前記車両（Ｖｉ）の識別データ要素（ＲＰＡｉ）を取得するステップと、
‐前記車両（Ｖｉ）の前記識別データ要素（ＲＰＡｉ）を備える少なくとも１つのデータフレーム（Ｔｄ）を、前記車両（Ｖｉ）の前記電子モジュール（１２０）から前記モバイル電子装置（ＳＰ）に送信するステップと、
‐スキャンモードにある前記モバイル電子装置（ＳＰ）において、前記車両（Ｖｉ）の前記識別データ要素（ＲＰＡｉ）を含む前記少なくとも１つのデータフレーム（Ｔｄ）を受信するステップと、
‐前記モバイル電子装置（ＳＰ）において、発信された前記識別データ要素（ＲＰＡｉ）が有効であることを検証し、次いで前記モバイル電子装置（ＳＰ）から前記車両（Ｖｉ）の前記電子モジュール（１２０）に接続リクエスト（１１０）を送信するステップと、
を備えることを特徴とする方法。
【請求項２】
前記車両（Ｖｉ）の前記識別データ要素（Ｒｐａｉ）は、式：ＰＲＡｉ＝Ｍ（ＡＳＳＯＣ）Ｒｉ　ここでＲｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ、Ｎ）、により表され、
この式において、
‐ＭとＮは、それぞれｍビットとｎビットである可変データ要素であり（ｍ及びｎは整数又はゼロ）、
‐Ｆｃは、暗号化関数であり、
‐Ｖｉｄｉは、前記車両Ｖｉのシークレットコードであり、
‐ＡＳＳＯＣは、データを互いに関連付ける関数である、
ことを特徴とする請求項１に記載の自動認識方法。
【請求項３】
‐ｍ＝ｎ＝０である、
ことを特徴とする請求項２に記載の自動認識方法。
【請求項４】
‐ｍ＝０、
‐ｎ≠０である、
ことを特徴とする請求項２に記載の自動認識方法。
【請求項５】
‐ｍ≠０、
‐ｎ＝０である、
ことを特徴とする請求項２に記載の自動認識方法。
【請求項６】
‐ｍ≠０、
‐ｎ≠０である、
ことを特徴とする請求項２に記載の自動認識方法。
【請求項７】
前記モバイル電子装置（ＳＰ）は、それ自体で、式：Ｒ’ｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ、Ｎ）に従って暗号化制御コードＲ’ｉを演算する、
ことを特徴とする請求項２及び請求項３乃至６のいずれかに記載の自動認識方法。
【請求項８】
前記モバイル電子装置（ＳＰ）において発信された前記識別データ要素（ＲＰＡｉ）が

有効であることを検証することからなるステップは、ＲｉとＲ’ｉとの等価比較からなる、
ことを特徴とする請求項７に記載の自動認識方法。
【請求項９】
前記車両（Ｖｉ）の前記電子モジュール（１２０）から前記モバイル電子装置（ＳＰ）に送信された前記データフレーム（Ｔｄ）の一部又は全部が、前記車両の動作を実施するために前記モバイル電子装置（ＳＰ）が応答すべきチャレンジとして使用される、
ことを特徴とする請求項１乃至８のいずれかに記載の自動認識方法。
【請求項１０】
前記車両（Ｖｉ）の前記電子モジュール（１２０）から前記モバイル電子装置（ＳＰ）に送信された前記データフレーム（Ｔｄ）の一部又は全部において、前記車両（Ｖｉ）の前記識別データ要素（ＲＰＡｉ）は、前記データ（Ｍ、Ｎ）に基づいて、ある発信から次の発信へと変化し得る又は変化し得ない、
ことを特徴とする請求項２乃至８のいずれかを引用する請求項９に記載の自動認識方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子モバイル通信装置と自動車の電子モジュールとの間の自動認識のための方法に係る。モバイル通信装置及び自動車の電子モジュールは、ブルートゥーススマート又はブルートゥース・ロー・エネルギ（Ｂｌｕｅｔｏｏｔｈ　Ｌｏｗ　Ｅｎｅｒｇｙ／ＢＬＥ）プロトコルにより信号を交換することが可能である。本発明の技術分野は、機械的鍵の使用以外の方法により自動車にアクセスするものである。
【０００２】
本明細書の文脈において、「電子モバイル通信装置」とは、（例えばＧＳＭ又はブルートゥース方式の）少なくとも１つの遠隔通信ネットワークを介して、人がデータや情報にアクセス可能となる電子装置を意味するために用いられる。したがって、「モバイル通信装置」には、携帯電話、より具体的にはスマートフォンタイプの携帯電話、携帯用コンピュータ、タブレット、携帯情報端末（ＰＤＡｓ）等が含まれる。本明細書において、非制限的な例として、モバイル通信装置は、記載の様々な状況におけるスマートフォンである。「自動車両」という用語は、不正確な言葉ではあるが、自動車両が有する電子モジュールを表すように使用されるであろう。「借主」という用語は、車両をレンタルする又は借りようとしている、又は現にレンタルしている又は借りている人を意味するように用いられるであろう。本発明の文脈において、ユーザは、特にスマートフォンタイプのモバイル通信装置を必ず有していなければならない。
【背景技術】
【０００３】
現在、ユーザは、スマートフォン等のモバイル通信装置を使用して、専用アプリケーション（専用アプリ）によるセキュリティが守られた信号交換プロセスに従うことで、車両の機能‐又はコマンド‐の実行を制御することができる。ここで言う機能‐又はコマンド‐とは、例えば、以下のコマンド、すなわち、車両の施錠／開錠、車両の始動、自動駐車等のうちの１つである。いくつかの適用例において、これらのコマンドのうちの１つを実行することができるように、モバイル装置に、車両の少なくとも１つのコマンドの実行を承認する識別キーを事前に格納されていなければならない。識別キーは、スマートフォンのセキュリティ要素、例えばそのＳＩＭカードや他のセキュリティ要素に格納され得る。このようにして、スマートフォンを保持することにより、ユーザは、例えば、車両の開放可能な本体部のロックを開錠することができる。この目的のために、識別キーひいてはスマートフォンに含まれるデータ、特に認証データが、当該スマートフォンと、車両の識別キーが有効であるか否かを決定する車両の電子モジュールとの間で交換される。有利な実施形態において、このようなデータ交換は、ＢＬＥプロトコルに従って実施される。

【０００４】
車両が複数のユーザによりシェアされている場合、一ユーザのスマートフォンに格納された識別キーは、ある構成において、一時的な識別キーである。すなわち、識別キーは限られた時間しか有効ではない。有効期間に関する情報は、有利には、一時識別キーを形成するコードに含まれる。レンタル用車両の場合、一時識別キーの有効期間は、車両の使用期間に一致する。一時識別キーは、ユーザが車両の使用に必要な全ての作業（予約、支払等）を実施した後に得られる。全ての場合において、識別キーは、例えば、ＢＬＥプロトコルだけでなく、ＮＦＣ、Ｗｉ‐Ｆｉ、又は、電子光学機器を介して、例えばコード（ＱＲ又はバーコード）の映像を撮影するスマートフォンのカメラにより、レンタルする車両の近傍に配置された自動端末からスマートフォンに転送され得る、或いはＧＳＭ方式のモバイル通信ネットワークを介して離れたサーバーからスマートフォンに送信され得る。

【０００５】
スマートフォンと自動車両との信号交換がＢＬＥプロトコルに従って実施されるという文脈において、自動車両は、長期間、更には永久的にアドバタイジングモードに設定されている。アドバタイジングモードとは、車両が定期的にその存在を示唆することを目的としたメッセージを発信する、また場合により何らかの情報を伝達するＢＬＥプロトコルのモードである。伝達される情報とは、例えば、専用アプリにより使用されるサービスが提供されるという表示である。

【０００６】
従来技術において、車両を事前にスマートフォンとペアリングさせることにより、車両が専用アプリを介してスマートフォンＳＰにより送信される指示を受信してこれを実行することができるようにしなくてはならない。

【０００７】
スマートフォンの方では、ＢＬＥプロトコルの「スキャン」モードに設定される。スキャンモードとは、ＢＬＥプロトコルに従って送信されるメッセージをリスニングできるようにするＢＬＥプロトコルのモードである。このため、専用アプリは、アドバタイジングモードに設定された様々な車両により送信される全ての信号を読み出すことができる。特に、この信号は、専用アプリにより送信されるコマンドをスマートフォンが受信可能であることを示す。

【０００８】
したがって、専用アプリは、スマートフォンのＢＬＥ範囲内に位置する車両であって、スマートフォンにインストールされた専用アプリからのコマンドを受信可能であるとその公示フレームにおいて示唆している車両のリストを得るために使用され得る。しかしながら、スマートフォンのユーザは、この車両リストのうちの１台又は場合により所定台数の車両しか使用する権利を有さない。ユーザが権利を有する車両のうちからどの車両を使用するかを決定するために、ユーザは当該車両を選択して、ペアリングコードと呼ばれる、該当車両に固有のコードを入力する。ペアリングコードは、ユーザが該当車両を使用する権利を授与されていることを条件として、事前にユーザに送信されている。ペアリングコードは、最も一般的には、ペアリングを目的として認証フェーズにおいてスマートフォンに入力されるコードである。別のプロセスにおいて、ペアリングコードは、ＮＦＣにより、又は（ＱＲコードやバーコードを使用して）カメラを介してスマートフォンに受信され得る。スマートフォンと車両とはこうしてペアリングされる。当然ながら、車両に用意されたのではないコードであるペアリングコードをユーザが入力した場合、ペアリングは実施されない。

【０００９】
スマートフォンと車両とがペアリングされたら、スマートフォンと車両とは、セキュリティの守られた態様において、例えばリクエスト、チャレンジ、及び／又はレスポンスの形体の信号を交換し得る。これは、有利には、ペアリング操作中に、暗号化キーが車両とスマートフォンとの間で交換されており、交換された信号が暗号化可能、及び／又は復号化可能とされているからである。別の動作モードにおいて、車両は、スマートフォンが受

信したコマンドを、これら２つの機器が事前にペアリングされている場合のみ容認する。
【００１０】
スマートフォンと車両とのペアリングのメカニズムは、これら２つの機器の間で信号交換のセキュリティを守るという点で有利である。しかしながら、このメカニズムは、スマートフォンのユーザに以下を強いるという点で制約がある。
‐ユーザの専用アプリによりユーザに提供された車両リストの中から、ユーザが権利を有する車両を識別しなければならない。車両リストは、専用アプリからのコマンドを受信可能な、スマートフォンの近傍に位置する全ての車両から構成されているため、例えば、ユーザが車両のレンタル代理店にいる場合、リストは長大になり得る。この場合、ユーザが自身に意図された車両を識別することは容易ではない。
‐ユーザが権利を有する車両に関連付けられたペアリングコードを事前に入手しなければならない。このコードは、通常、第三者によりユーザに送信されていなければならない。ユーザは、コードを記憶し又は書き留め、権利を有する車両へのアクセスを獲得するまで保持しなければならない。
‐ユーザのスマートフォンにインストールされた専用アプリにペアリングコードを入力しなくてはならない。
【００１１】
ペアリングのメカニズムは、車両の使用状態に応じて複数回繰り返される場合があるため、更に制約が重くなる。
【発明の概要】
【００１２】
本発明は、上述の従来技術の欠点のいくつか又は全てを克服することを意図し、特に、スマートフォン等のモバイル通信装置と自動車両との間の、ＢＬＥプロトコルにより交換される信号による自動認識のための方法を提案する。本認証方法は、最早ペアリングメカニズムを必要としないが、それにも拘わらず車両とモバイル機器との間の信号交換の最適なセキュリティを提供する。
【００１３】
この目的のために、本発明において、ＢＬＥプロトコルのアドバタイジングモードにある車両Ｖから発信された認証情報を備えたフレームであって、スマートフォン及びそれのみで認識されるフレームが提案される。
【００１４】
したがって、本発明は、本質的に、モバイル電子装置と電子伝達モジュールを有する自動車両との間の自動認識のための方法であって、前記モバイル電子装置と前記車両の電子モジュールはＢＬＥプロトコルに従って動作可能であり、前記モバイル電子装置はスキャンモードにあるとともに前記車両はアドバタイジングモードにあり、前記方法は、
‐前記車両の前記電子モジュールにおいて、前記車両の識別データ要素を取得するステップと、
‐前記車両の前記識別データ要素を備える少なくとも１つのデータフレームを、前記車両の前記電子モジュールから前記モバイル電子装置に送信するステップと、
‐スキャンモードにある前記モバイル電子装置において、前記車両の前記識別データ要素を含む前記少なくとも１つのデータフレームを受信するステップと、
‐前記モバイル電子装置において、発信された前記識別データ要素が有効であることを検証し、次いで前記モバイル電子装置から前記車両の前記電子モジュールに接続リクエストを送信するステップと、を備えることを特徴とする方法、に関する。
【００１５】
先行する段落で述べた主要な特徴の他に、本発明による方法は、以下に記載の単独でもよく又は技術的に可能ならば組み合わせてもよい特徴の中から１つ以上の追加の特徴を有し得る。
前記車両の前記識別データ要素は、式：ＰＲＡｉ＝Ｍ（ＡＳＳＯＣ）Ｒｉ　ここでＲｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ、Ｎ）、により記載され、

この式において、
ＭとＮは、それぞれｍビットとｎビットである可変データ要素であり（ｍ及びｎは整数又はゼロ）、
Ｆｃは、暗号化関数であり、
Ｖｉｄｉは、前記車両Ｖｉのシークレットコードであり、
ＡＳＳＯＣは、データを互いに関連付ける関数である。
ｍ＝ｎ＝０、又は、ｍ＝０且つｎ≠０、又は、ｍ≠０且つｎ＝０、又は、ｍ≠０且つｎ≠０。
前記モバイル電子装置は、それ自体で、式：Ｒ’ｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ、Ｎ）に従って暗号化制御コードＲ’ｉを演算する。
前記モバイル電子装置において発信された前記識別データ要素が有効であることを検証することからなるステップは、ＲｉとＲ’ｉとの等価比較からなる。
前記車両の前記電子モジュールから前記モバイル電子装置に送信された前記データフレームの一部又は全部が、前記車両の動作を実施するために前記モバイル電子装置が応答すべきチャレンジとして使用される。

【００１６】

本発明の他の特徴及び利点が、唯一の添付図面を参照しつつ以下の説明を熟読することにより明らかになるであろう。

【図面の簡単な説明】

【００１７】

【図１】本発明による方法の例示的な実施形態において動作している種々の要素の概略図。

【発明を実施するための形態】

【００１８】

本発明の非制限的な実施形態におけるプロセスを以下に述べる。第１フェーズにおいて、特定のサービスを提供する車両Ｖｉのセットについて（ｉは、１乃至ｎの間で変化し、ｎは車両の台数に一致する整数）、リモートサーバー１０１が、各車両Ｖｉに関する機密データセット１０３をデータベース１０２において有している。つまり、リモートサーバー１０１は、各車両Ｖｉに関して、該当する各車両Ｖｉに固有の第１シークレットコードＶｉｄｉと、複数の仮想キーを生成するために使用されるであろう第２シークレットコードＤｉｖｅｒｓｉｆｉｅｒＫｅｙと、を有する。図示しない好適な別のモードにおいて、１つ以上の異なるＤｉｖｅｒｓｉｆｉｅｒＫｅｙコードが各Ｖｉｄｉと関連付けられる。ＤｉｖｅｒｓｉｆｉｅｒＫｅｙは、Ｖｉｄｉ及び／又はインクリメントデータ要素等の他のデータ要素に基づいて得られる。

【００１９】

以下のフェーズにおいて、各車両Ｖｉに対する権利が定義されなくてはならない。各車両Ｖｉに関する権利は、スマートフォン等のモバイル通信装置ＳＰを有する各将来のユーザ２００について、以下のうちの１つ以上のデータ要素に関連付けられる。
‐各該当ユーザに関する承認使用期間ＴＳｉ。この使用期間は、例えば、１日目と２日目との間のインタバルにより、又は車両Ｖｉの使用開始日及び最大使用期間Ｄｍａｘにより定義され得る。
‐権利リストＣｍｄＲｉｇｈｔｓｉ。この権利リストＣｍｄＲｉｇｈｔｓｉは、各該当ユーザが、そのモバイル装置ＳＰの専用アプリ１０４を使用して、車両Ｖｉに対して実施する行為やコマンドを定義する。したがって、例えば、ユーザ２００は、車両Ｖｉの全部又は一部（例えば所定回数）を開放する権利、車両Ｖｉを始動させる権利、車両Ｖｉを駐車する権利、特定の条件（例えば、速度制限、走行距離又は地理的領域）下において車両を使用する権利を有することが定義される。

【００２０】

これらの権利を定義するために、通常車両の所有者である承認ユーザ２０１は、リモートサーバー１０１に、有利には、例えば承認ユーザ２０１が所有すべきパスワードを使用

して、セキュリティ通信１０５を介して接続する。こうして、所有者２０１は、各車両Ｖｉに対して、誰が承認ユーザとなり、どのような権利が各ユーザに関連付けられるかを決定する。この目的のために、所有者は、リモートサーバーに、各将来のユーザに関する前記権利を、各該当ユーザの識別子とともに通知する。有利には、ユーザの識別子は、ユーザの携帯電話番号ＰＮｉである。他の例において、識別子は、将来のユーザの携帯電話のＩＭＥＩ番号か、又はＳＩＭカードの識別番号（ＩＭＳＩ番号）でもよい。

【００２１】

所有者２０１により入力された情報及び車両Ｖｉの第１シークレットコードＶｉｄｉに基づいて、リモートサーバー１０１は、演算ユニット１０６を使用して、認定コードＣｒｅｄｅｎｔｉａｌｉを生成する。非制限的な実施形態において、認定コードＣｒｅｄｅｎｔｉａｌｉは、演算ユニット１０６により、上述のデータ（該当借主２００の権利ＣｍｄＲｉｇｈｔｓｎ、承認使用期間ＴＳｉ、及び車両Ｖｉの第１シークレットコードＶｉｄｉ）を単純に連結することにより生成され得る。別のモードにおいて、Ｖｉｄｉは連結から外される。このようにして、認定コードＣｒｅｄｅｎｔｉａｌｉは、ユーザと、任意の車両と、ユーザが該当車両Ｖｉについて有する権利について固有となる。

【００２２】

一実施形態において、次いでリモートサーバー１０１は、車両Ｖｉの認定コードＣｒｅｄｅｎｔｉａｌｉ及び第２シークレットコードＤｉｖｅｒｓｉｆｉｅｒＫｅｙに基づいて、第１暗号化モジュールにより、サイン、すなわち認証コードＣｒｅｄｅｎｔｉａｌＭＡＣｉを生成する。認証コードＣｒｅｄｅｎｔｉａｌＭＡＣｉは、認定コードＣｒｅｄｅｎｔｉａｌｉに関連付けられて、その後、当該認定コードＣｒｅｄｅｎｔｉａｌｉを認承するであろう。他の実施形態において、リモートサーバー１０１は、認証コードＣｒｅｄｅｎｔｉａｌＭＡＣｉを、第２シークレットコードＤｉｖｅｒｓｉｆｉｅｒＫｅｙ及びコードＶｉｄｉに基づいて生成する。この暗号化ＨＭＡＣ１は、例えば、英語の「Ｈａｓｈｅｄ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ」からＨＭＡＣとして知られる暗号化方式であるか、「Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ」からＡＥＳとして知られる暗号化方式であり得る。認証コードＣｒｅｄｅｎｔｉａｌＭＡＣｉは、ユーザ２００が、認定コードＣｒｅｄｅｎｔｉａｌｉによりユーザに許可された権利にその行為が限定されていることを保証するためにも使用され得る。また、認証コードＣｒｅｄｅｎｔｉａｌＭＡＣｉは、車両Ｖｉが、認定コードＣｒｅｄｅｎｔｉａｌｉに含まれる承認に関するユーザの意向を有効にすることを可能にする。

【００２３】

認定コードＣｒｅｄｅｎｔｉａｌｉ及びそのサインＣｒｅｄｅｎｔｉａｌＭＡＣｉがリモートサーバー１０１により作成されたら、それらは、コードＶｉｄｉとともに、借主２００のために特別に生成された仮想キーＣｒｅｄｅｎｔｉａｌＭＡＣｉに関連付けられた借主２００のスマートフォンＳＰのセキュリティエリア１０７に転送され格納される。スマートフォンのセキュリティエリア１０７は、例えば、スマートフォンに設けられたＳＩＭカードや他のセキュリティ要素である。他の実施形態において、セキュリティエリア１０７は、仮想セキュリティ要素により表され得る。この格納操作は、セキュリティエリアにこのような書込み操作を行うことが許可されたオペレータによってのみ実施される。このエンティティはＴＳＭ（英語で「Ｔｒｕｓｔｅｄ Ｓｅｒｖｉｃｅ Ｍａｎａｇｅｒ」）として公知である。仮想キーとそのサインの転送は、ユーザ２００の電話番号ＰＮｎを使用することにより実施される。この電話番号ＰＮｎは、承認ユーザ２０１によりリモートサーバー１０１に伝達済である。

【００２４】

同時に、ＳＩＭカードの場合カードレットと呼ばれるソフトウエア要素が、ここでも承認オペレータＴＳＭにより、セキュリティエリア１０７に格納される。カードレットソフトウエア要素は、セキュリティエリア１０７に格納された複数のコードと協働するように、特に専用アプリにより使用され得る特別なアプリである。これらのコードは、ＣｒｅｄｅｎｔｉａｌＭＡＣｉ、Ｃｒｅｄｅｎｔｉａｌｉ及びＶｉｄｉであり、Ｃｒｅｄｅｎｔｉ

ａｌＭＡＣｉ及びＶｉｄｉは特に開示されない。他のコードのうち、コードＣｒｅｄｅｎｔｉａｌｉについては、専用アプリにより車両に送信されるであろう。プロセスのセキュリティはこうして補強される。これらの種々の要素がセキュリティエリア１０７に格納されたら、スマートフォンＳＰは、コマンドを車両Ｖｉに対して専用アプリ１０４を介して発信することができる。

【００２５】

この目的のために、本発明によれば、スマートフォンＳＰが、スマートフォンＳＰの所有者であるユーザ２００が借り受けを承認された車両Ｖｉを認識するプロセスが実施される。

【００２６】

この認識プロセスの種々のステップを以下に詳述する。

‐定期的に繰り返される第１ステップにおいて、車両Ｖｉ、すなわちより正確には、ＢＬＥプロトコルに従って動作可能であるとととともにアドバタイジングモードに設定された車両Ｖｉの電子モジュール１２０は、データフレームＴｄを定期的に発信する。本発明によれば、データフレームは、第１例において、暗号化Ｆｃにより、車両Ｖｉに固有の第１シークレットコードＶｉｄｉに基づいて演算された識別データ要素ＲＰＡを備える。これは、ＲＰＡｉ＝Ｆｃ（Ｖｉｄｉ）と表される。

‐図示例に対応する第２例において、識別データ要素ＲＰＡｉは、ランダムデータ要素Ｒａｎｄと、暗号化関数を第１シークレットコードＶｉｄｉとランダムデータ要素Ｒａｎｄとに適用して得られた結果Ｆｃ（Ｖｉｄｉ、Ｒａｎｄ）とを関連付ける又は連結すること（ＡＳＳＯＣ）により得られる。これは、ＰＲＡｉ＝Ｒａｎｄ（ＡＳＳＯＣ）Ｆｃ（Ｖｉｄｉ、Ｒａｎｄ）と表される。この第２例は、ＲＡＮＤがある送信から次の送信に従って変化する、又は変化しないことにより、識別データ要素ＲＰＡの値がある送信から次の送信に従って変化し得る、又は変化し得ないため、次の識別データ要素ＲＰＡの値が何であるか推測不可能であるという点で有利である。

‐第３の例示的実施形態において、識別データ要素ＲＰＡｉは、暗号化関数Ｆｃにより、車両Ｖｉに固有の第１シークレットコードＶｉｄｉ及び可変であるデータ要素ＤＡＴＡに基づいて得られる。これは、ＰＲＡｉ＝Ｆｃ（Ｖｉｄｉ、ＤＡＴＡ）と表される。ＤＡＴＡの値は、車両Ｖｉとスマートフォンに従ってＳＰにしかわからない。ＤＡＴＡの値は、非制限的な例において、ルート値が公知である疑似乱数生成装置により、又は所定の増分カウンタにより、又はクロックにより提供され得る。この第２例は、ＤＡＴＡの値がある送信から次の送信に従って変えられる、又は変えられないという事実の結果、識別データ要素ＰＲＡの値が、ある送信から次の送信に従って変化し得る、又は変化し得ないため、次の識別データ要素ＰＲＡの値が何であるか推測不可能であるという点で有利である。

‐第４の例示的実施形態において、識別データ要素ＲＰＡｉは、データ要素ＤＡＴＡ”と、暗号化関数を第１シークレットコードＶｉｄｉとデータ要素ＤＡＴＡ’、ＤＡＴＡ”とに適用することにより得られた結果Ｆｃ（Ｖｉｄｉ、ＤＡＴＡ’、ＤＡＴＡ”）とを連結（ＡＳＳＯＣ）することにより得られる。ＤＡＴＡ’の値は、車両Ｖｉ及びスマートフォンＳＰにしかわからない。ＤＡＴＡ’の値は、非制限的な例において、ルート値が公知である疑似乱数生成装置により、又は所定の増分カウンタにより、又はクロックにより提供され得る。

【００２７】

要約すれば、全ての例示的な実施形態において、識別データ要素ＰＲＡｉは、式：ＰＲＡｉ＝Ｍ（ＡＳＳＯＣ）Ｒｉ　ここでＲｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ、Ｎ）により表される。

この式において、ＭとＮは、それぞれｍビットとｎビットである可変データ要素である（ｍ及びｎは整数）。

【００２８】

したがって、

‐第１の例示的な実施形態は、ｍ＝ｎ＝０のケースに対応する。

‐第２の例示的な実施形態は、ｎ＝０且つｍ≠０のケースに対応する。

‐第３の例示的な実施形態は、ｎ≠０且つｍ＝０のケースに対応する。
‐第４の例示的な実施形態は、ｎ≠０且つｍ≠０のケースに対応する。
‐第２ステップにおいて、スキャンモードにあるスマートフォンＳＰが、データフレームＴｄ、ひいては識別データ要素ＲＰＡｉを受信すると、スマートフォンＳＰは、それ自体で、暗号化チェックコードＲ’ｉを演算する。このチェック操作は、セキュリティエリア１０７において、車両Ｖｉに存在する暗号化関数と同一の暗号化関数Ｆｃにより実施される。後者の暗号化関数は、この暗号化関数Ｆｃを含むカードレットソフトウエア要素により、セキュリティエリア１０７に格納されている。Ｒ’ｉに対する式は以下である。

Ｒ’ｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ、Ｎ）

データ要素Ｍは、ＲＰＡｉが送信された時に受信されており、データ要素Ｎはスマートフォンによ入手されるデータ要素である。

【００２９】

スマートフォンＳＰが、使用が承認された以外の車両である車両Ｖｉ’から送信されたデータフレームＴＤ’を受信した場合、暗号化チェックコードＲ’ｉを演算するために使用される第１シークレットコードＶｉｄｉは、データフレームＴＤ’（Ｒｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ’、Ｎ’））に対する暗号化コードＲｉとは異なる結果（Ｒ’ｉ＝Ｆｃ（Ｖｉｄｉ、Ｍ’、Ｎ））を出すであろう。

【００３０】

したがって、考察した第１例（ＰＲＡｉ＝Ｆｃ（Ｖｉｄｉ））において、セキュリティエリア１０７に認定Ｃｒｅｄｅｎｔｉａｌｉにより既に伝達されている第１シークレットコードＶｉｄｉは、チェック用識別データ要素Ｒｉの演算を実施するためだけに使用される。したがって、Ｒ’ｉ＝Ｆｃ（Ｖｉｄｉ）である。セキュリティ格納エリアに格納された第１シークレットコードＶｉｄｉが、データフレームＴＤを発信した車両Ｖｉの第１シークレットコードＶｉｄｉに等しい場合に限り、データ要素Ｒｉとチェック用データ要素Ｒ’ｉとは等しいであろう。スマートフォンＳＰが、レンタルが承認された車両以外の車両Ｖｉ’により送信されたデータフレームＴＤ’を受信した場合、チェック用データ要素Ｒ’ｉ＝Ｆｃ（Ｖｉｄｉ）を演算するのに使用された第１シークレットコードＶｉｄｉは、データフレームＴＤ’の識別データ要素Ｒｉ＝Ｆｃ（Ｖｉｄｉ’）と異なる結果を出すであろう。

【００３１】

考察した第２例（ＲＰＡｉ＝Ｒａｎｄ．ＣＯＮＣＡＴ　Ｆｃ（Ｖｉｄｉ、Ｒａｎｄ））において、セキュリティエリアに認定Ｃｒｅｄｅｎｔｉａｌｉにより伝達された第１シークレットコードが使用される一方、他方において、車両ＶｉからスマートフォンＳＰに発信されたデータフレームＴｄにおけるランダムデータ要素Ｒａｎｄも使用される。チェック用識別データ要素ＲＰＡ’ｉは、以下のように演算される。ＲＰＡ’ｉ＝Ｆｃ（Ｖｉｄｉ、Ｒａｎｄ）。識別データ要素ＲＰＡｉの一部Ｆｃ（Ｖｉｄｉ、Ｒａｎｄ）がチェック用データ要素ＲＰＡ’ｉと比較される。図示例の場合のように、セキュリティ格納エリアに格納された第１シークレットコードがデータフレームＴＤを発信した車両Ｖｉの第１シークレットコードと同一の場合に限り、それらは等しいであろう。スマートフォンＳＰが、使用が承認された車両以外の車両Ｖｉ’により送信されたデータフレームＴＤ’を受信した場合、チェック用データ要素Ｒｐａ’ｉを演算するのに使用された第１シークレットコードＶｉｄｉは、データフレームＴｄｉにおいて発信された識別データ要素Ｒｐａｉの一部Ｆｃ（Ｖｉｄｉ、Ｒａｎｄ）と異なる結果を出すであろう。

【００３２】

第３及び第４の例示的な実施形態によれば、車両の識別データ要素ＲＰＡｉを得ることを目的として、スマートフォンＳＰにおける後続のプロセスは、ＰＲＡ’ｉを取得する第２の例示的な実施形態における後続のプロセスと同一である。したがって、セキュリティ格納エリアに格納された第１シークレットコードＶｉｄｉがデータフレームＴＤを発信した車両Ｖｉの第１シークレットコードＶｉｄｉと同一であり、且つスマートフォンＳＰが、（第３例において）データ要素ＤＡＴＡ又は（第４例において）ＤＡＴＡ’ を含んで

いる場合に限り、識別データ要素ＲＰＡｉのＦｃ（Ｖｉｄｉ、ＤＡＴＡ）部分又はＦｃ（Ｖｉｄｉ、ＤＡＴＡ’、ＤＡＴＡ”）部分と、チェック用識別データ要素ＲＰＡ’ｉとは等しいであろう。

【００３３】

説明しない別の実施形態において、連結形体において事前に使用された関連付けは、難読化又は混合動作に代え得る。

【００３４】

したがって、ＢＬＥプロトコルに従ってデータを交換可能な全ての車両をスキャンするようにスキャンモードに設定されることにより、スマートフォンＳＰは、ユーザ（すなわち当該スマートフォンのユーザ）が使用を承認された車両Ｖｉを認識するであろう。この認識が実施されると、スマートフォンＳＰは、接続リクエスト１１０を、有利には依然としてＢＬＥプロトコルに従って、車両Ｖｉに送信する。

【００３５】

この段階で、スマートフォンＳＰと車両Ｖｉとのデータ交換により、スマートフォンＳＰは承認を有する車両Ｖｉを識別することができるようになっており、これら２つの機器、すなわちスマートフォンＳＰと車両Ｖｉとは接続モードにある。

【００３６】

下記のステップにより、車両Ｖｉはスマートフォンから送信されたコマンドを認証できなくてはならない。

【００３７】

スマートフォンＳＰと車両Ｖｉとの接続が確立した後、所望のコマンド（施錠、開錠等）の実行ステップにおけるより強力な認証プロセスを確立することが好適である。なぜならば、スマートフォンＳＰと車両Ｖｉはペアリングされていないためである。すなわち、スマートフォンＳＰは、車両Ｖｉからのチャレンジに対するレスポンスを、そのコマンドリクエストに関連付けなければならない。

【００３８】

第１実施形態において、一度接続が確立されると、車両Ｖｉによりチャレンジが送信される。スマートフォンＳＰは、これに特定のコマンド（施錠、開錠等）を送信することにより応答する。

【００３９】

有利な実施形態において、車両により送信されるチャレンジは、ＲＰａの送信中に作成される。スマートフォンＳＰは、このチャレンジを、送信されたＲＰａの全部又は一部に基づいて解釈し、上記のケースのように特定のコマンド（施錠、開錠等）を送信することにより、これに応答する。

【００４０】

認証プロセスは以下に記載する。

‐最初に、ユーザが所望するコマンドＣｍｄｌｄ、例えば「車両を開放せよ」というコマンドが、セキュリティエリア１０７に存在する第２暗号化モジュールに送信される。ＨＭＡＣ方式の第２暗号化モジュールＨＭＡＣ２は、車両Ｖｉにより発信された識別データ要素ＲＰＡｉと、事前にセキュリティエリア１０７に格納された認定コードＣｒｅｄｅｎｔｉａｌｉに対応する単純化された認定コードＣｒｅｄｅｎｔｉａｌ’ｉとを受信する。セキュリティエリア１０７において、第１シークレットコードＶｉｄｉに関する情報は削除されているためこの情報は開示され得ない。最後に、第２暗号化モジュールは、セキュリティエリア１０７に同じく格納されている、認定コードＣｒｅｄｅｎｔｉａｌｉのサインＣｒｅｄｅｎｔｉａｌＭＡＣｉを受信する。

‐この情報に基づいて、第２暗号化モジュールは、第１検証コードＭＡＣを演算する。

‐検証コードＭＡＣが確立されたら、スマートフォンＳＰは、有利には依然としてＢＬＥプロトコルに従って、特に、単純化された認定コードＣｒｅｄｅｎｔｉａｌ’ｉと、所望のコマンドＣｍｄｌＤと、第１検証コードＭＡＣとを備えたコマンドＲｃに対するリクエスト１１１を車両Ｖｉに送信する。

‐車両Ｖｉの方では、同じ演算を実施する。すなわち、単純化された認定コードＣｒｅｄｅｎｔｉａｌ’ｉと、第１シークレットコードＶｉｄｉと、第２シークレットコードＤｉｖｅｒｓｉｆｉｅｒＫｅｙとに基づいて、車両Ｖｉは、認定コードＣｒｅｄｅｎｔｉａｌｉの認証コードＣｒｅｄｅｎｔｉａｌＭＡＣｉを、車両Ｖｉの電子モジュール１２０に同じく存在する第１暗号化モジュールＨＭＡＣ１により再演算する。サインＣｒｅｄｅｎｔｉａｌＭＡＣｉは、こうして、セキュリティエリア１０７の暗号化モジュールと同一の第２暗号化モジュールＨＭＡＣ２に供給される。第２暗号化モジュールは、チェック用識別データ要素ＲＰＡｉを、コマンドリクエストＲｃと所望のコマンドＣｍｄｌＤと単純化された認定コードＣｒｅｄｅｎｔｉａｌ’ｉとを介して受信し、これにより、第２検証コードＭＡＣ’を演算することができる。第１検証コードＭＡＣと第２検証コードＭＡＣ’とが同一である場合、所望のコマンドＣｍｌｄが権利リストＣｍｄＲｉｇｈｔｓｉに実際にあり、且つ、これらの検証が実施された時点ＲｅａｌＴｉｍｅが実際に承認された使用期間ＴＳｉに該当するということを条件として、所望のコマンドＣｍｌｄは車両Ｖｉにより実行されるであろう。他の実施形態において、検証の順序は逆であってもよい。本方法は、Ｃｒｅｄｅｎｔｉａｌ’ｉ及びＣｍｄｌＤの情報を明瞭にテストし、そして、これらが有効である場合のみ、認証コードＣｒｅｄｅｎｔｉａｌＭＡＣｉ及びＭＡＣを検証してもよい。

‐有利な実施形態において、車両Ｖｉは、補助変数ＮｏｎｃｅをスマートフォンｓＰに、発信１１２において検証コードＭＡＣの演算のために送信する。有利には、補助変数Ｎｏｎｃｅは、一度だけ使用される値を取り、車両Ｖｉによる補助変数Ｎｏｎｃｅの更なる送信は異なる値を取るであろう。補助変数Ｎｏｎｃｅは、セキュリティ格納エリア１０７の第２暗号化モジュールＨＭＡＣ２により、検証コードＭＡＣの演算において使用され、また、車両Ｖｉの第２暗号化モジュールＨＭＡＣ２により第２検証コードＭＡＣ’の演算のために使用される。このようにして、更なるセキュリティが提供される。

【００４１】

本発明において、セキュリティが守られたデータ交換が、ＢＬＥプロトコルに従ってデータを交換するスマートフォンと車両との間で、全体としてシンプルなプロセスにより提供される。ユーザがペアリングコードを入力する必要はない。

【図１】

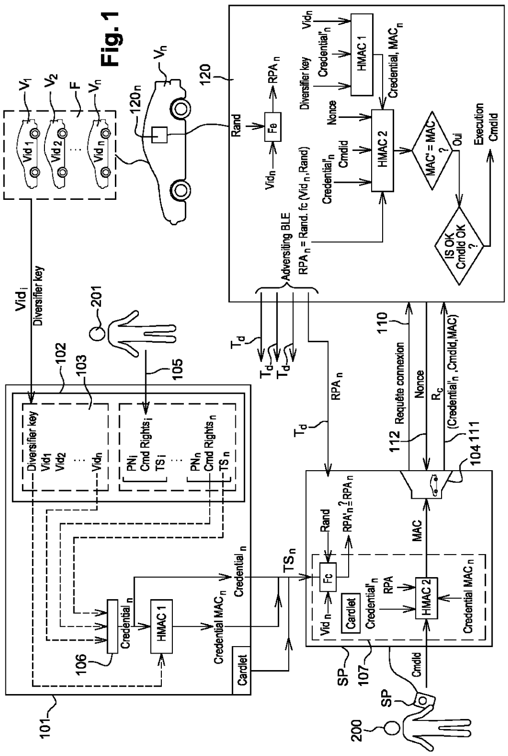
Fig. 1
101
102
103
105
106
107
104 111
112
110
120
201
200
SP
Diversifier key
Cmd Rights
Credential n
HMAC 1
HMAC 2
Cardlet
Advertising BLE
Requête connexion
Nonce
MAC
Cmdld
Execution
Cmdld
Rand
Fc
Fe
Oui

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/053717

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 H04W12/08 H04L29/06 H04W12/04 G07C9/00
H04L9/32 B60R25/24 H04W4/00 H04L29/08 H04W4/04
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L G07C B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, COMPENDEX, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/169564 A1 (GAUTAMA NEERAJ R [CA] ET AL) 19 June 2014 (2014-06-19)	1-9
Y	paragraphs [0011], [0027], [0031] paragraphs [0035], [0037], [0039] paragraphs [0047], [0059], [0062] paragraph [0066] - paragraph [0071] paragraphs [0076], [0078], [0079] paragraph [0083] - paragraph [0085] paragraphs [0087], [0089], [0091] -----	10
X	US 2014/282974 A1 (MAHER DAVID P [US] ET AL) 18 September 2014 (2014-09-18) paragraph [0097] - paragraph [0106]; figure 6 paragraph [0145] - paragraph [0151]; figure 10 paragraph [0185] - paragraph [0189]; figures 16,17 ----- -/--	1-10

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 March 2016	30/03/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Losseau, Dominique

3

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/053717

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/251279 A1 (SPANGENBERG PHILIPP PAUL [DE] ET AL) 8 October 2009 (2009-10-08)	1-9
Y	paragraph [0011] - paragraph [0016] paragraphs [0020], [0032], [0043]	10
Y	US 2014/188348 A1 (GAUTAMA NEERAJ R [CA] ET AL) 3 July 2014 (2014-07-03)	1-9
A	paragraph [0010] - paragraph [0011] paragraph [0015] - paragraph [0018] paragraphs [0029], [0030] paragraph [0041] - paragraph [0052]; figure 1A paragraph [0074] - paragraph [0085] paragraph [0107] - paragraph [0120] paragraph [0123] - paragraph [0135]; figures 4A,4B	10
Y	WO 2008/063899 A2 (TOYOTA ENG & MFG NORTH AMERICA [US]; UNIV ILLINOIS [US]; LABERTEAUX KE) 29 May 2008 (2008-05-29) paragraph [0012] - paragraph [0016] paragraph [0028] - paragraph [0037]	1-8,10
Y	FR 2 774 833 A1 (FRANCE TELECOM [FR]) 13 August 1999 (1999-08-13) page 3, line 22 - page 4, line 8 page 7, line 25 - page 8, line 13 page 12, line 1 - page 17, line 17; figure 1a page 17, line 23 - page 18, line 6; figure 1b page 18, line 20 - page 19, line 2 page 23, line 6 - page 24, line 17 page 24, line 23 - line 29; figure 1e page 25, line 27 - page 27, line 12 page 27, line 30 - page 29, line 6 page 30, line 9 - page 31, line 22; figure 1g page 32, line 25 - line 30; figure 2a page 33, line 20 - page 34, line 4; figure 2b	1-10
Y	Alfred Menezes ET AL: "Handbook of Applied Cryptography, Chap 10: Identification and Entity Authentication" In: "Handbook of Applied Cryptography; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS]", 1 January 1997 (1997-01-01), CRC Press, XP055141231, pages 385-424,	10
A	Chapitre 10.3; page 397 - page 405	2-9

-/--

3

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/053717

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7 366 677 B1 (LIU TE-KAI [US] ET AL) 29 April 2008 (2008-04-29) column 1, line 55 - column 2, line 3 column 3, line 60 - column 4, line 12 -----	1-10
A	EP 0 492 692 A2 (DELCO ELECTRONICS CORP [US]) 1 July 1992 (1992-07-01) column 2, lines 10-26, 51-56 column 3, line 11 - column 4, line 12 column 5, line 6 - line 18 column 5, line 30 - column 6, line 39 -----	1-10

3

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2015/053717

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014169564 A1	19-06-2014	CN 103874061 A	18-06-2014
		DE 102013225742 A1	18-06-2014
		US 2014169564 A1	19-06-2014
US 2014282974 A1	18-09-2014	CN 105378774 A	02-03-2016
		EP 2973285 A1	20-01-2016
		US 2014282974 A1	18-09-2014
		WO 2014165284 A1	09-10-2014
US 2009251279 A1	08-10-2009	EP 1910134 A2	16-04-2008
		ES 2423679 T3	23-09-2013
		US 2009251279 A1	08-10-2009
		WO 2007009453 A2	25-01-2007
US 2014188348 A1	03-07-2014	CN 103905127 A	02-07-2014
		DE 102013224330 A1	03-07-2014
		US 2014188348 A1	03-07-2014
WO 2008063899 A2	29-05-2008	US 2008235509 A1	25-09-2008
		WO 2008063899 A2	29-05-2008
FR 2774833 A1	13-08-1999	AT 273541 T	15-08-2004
		DE 69919331 D1	16-09-2004
		EP 1055203 A1	29-11-2000
		FR 2774833 A1	13-08-1999
		JP 2002502925 A	29-01-2002
		WO 9940546 A1	12-08-1999
US 7366677 B1	29-04-2008	NONE	
EP 0492692 A2	01-07-1992	AU 632721 B2	07-01-1993
		AU 8966491 A	25-06-1992
		DE 69112191 D1	21-09-1995
		DE 69112191 T2	04-01-1996
		EP 0492692 A2	01-07-1992
		JP H086520 B2	24-01-1996
		JP H04302682 A	26-10-1992
		US 5144667 A	01-09-1992

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/053717

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04W12/06 H04W12/08 H04L29/06 H04W12/04 G07C9/00
H04L9/32 B60R25/24 H04W4/00 H04L29/08 H04W4/04
ADD.
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04W H04L G07C B60R

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, COMPENDEX, INSPEC, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2014/169564 A1 (GAUTAMA NEERAJ R [CA] ET AL) 19 juin 2014 (2014-06-19)	1-9
Y	alinéas [0011], [0027], [0031] alinéas [0035], [0037], [0039] alinéas [0047], [0059], [0062] alinéa [0066] - alinéa [0071] alinéas [0076], [0078], [0079] alinéa [0083] - alinéa [0085] alinéas [0087], [0089], [0091]	10
X	US 2014/282974 A1 (MAHER DAVID P [US] ET AL) 18 septembre 2014 (2014-09-18) alinéa [0097] - alinéa [0106]; figure 6 alinéa [0145] - alinéa [0151]; figure 10 alinéa [0185] - alinéa [0189]; figures 16,17	1-10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
17 mars 2016	30/03/2016

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Losseau, Dominique

3

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/053717

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2009/251279 A1 (SPANGENBERG PHILIPP PAUL [DE] ET AL) 8 octobre 2009 (2009-10-08)	1-9
Y	alinéa [0011] - alinéa [0016] alinéas [0020], [0032], [0043]	10

Y	US 2014/188348 A1 (GAUTAMA NEERAJ R [CA] ET AL) 3 juillet 2014 (2014-07-03)	1-9
A	alinéa [0010] - alinéa [0011] alinéa [0015] - alinéa [0018] alinéas [0029], [0030] alinéa [0041] - alinéa [0052]; figure 1A alinéa [0074] - alinéa [0085] alinéa [0107] - alinéa [0120] alinéa [0123] - alinéa [0135]; figures 4A,4B	10

Y	WO 2008/063899 A2 (TOYOTA ENG & MFG NORTH AMERICA [US]; UNIV ILLINOIS [US]; LABERTEAUX KE) 29 mai 2008 (2008-05-29) alinéa [0012] - alinéa [0016] alinéa [0028] - alinéa [0037]	1-8,10

Y	FR 2 774 833 A1 (FRANCE TELECOM [FR]) 13 août 1999 (1999-08-13) page 3, ligne 22 - page 4, ligne 8 page 7, ligne 25 - page 8, ligne 13 page 12, ligne 1 - page 17, ligne 17; figure 1a page 17, ligne 23 - page 18, ligne 6; figure 1b page 18, ligne 20 - page 19, ligne 2 page 23, ligne 6 - page 24, ligne 17 page 24, ligne 23 - ligne 29; figure 1e page 25, ligne 27 - page 27, ligne 12 page 27, ligne 30 - page 29, ligne 6 page 30, ligne 9 - page 31, ligne 22; figure 1g page 32, ligne 25 - ligne 30; figure 2a page 33, ligne 20 - page 34, ligne 4; figure 2b	1-10

Y	Alfred Menezes ET AL: "Handbook of Applied Cryptography, Chap 10: Identification and Entity Authentication" In: "Handbook of Applied Cryptography; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS]", 1 janvier 1997 (1997-01-01), CRC Press, XP055141231, pages 385-424,	10
A	Chapitre 10.3; page 397 - page 405	2-9

	-/--	

3

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/053717

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 7 366 677 B1 (LIU TE-KAI [US] ET AL) 29 avril 2008 (2008-04-29) colonne 1, ligne 55 - colonne 2, ligne 3 colonne 3, ligne 60 - colonne 4, ligne 12 -----	1-10
A	EP 0 492 692 A2 (DELCO ELECTRONICS CORP [US]) 1 juillet 1992 (1992-07-01) colonne 2, lignes 10-26, 51-56 colonne 3, ligne 11 - colonne 4, ligne 12 colonne 5, ligne 6 - ligne 18 colonne 5, ligne 30 - colonne 6, ligne 39 -----	1-10

3

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2015/053717

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2014169564 A1	19-06-2014	CN 103874061 A	18-06-2014
		DE 102013225742 A1	18-06-2014
		US 2014169564 A1	19-06-2014
US 2014282974 A1	18-09-2014	CN 105378774 A	02-03-2016
		EP 2973285 A1	20-01-2016
		US 2014282974 A1	18-09-2014
		WO 2014165284 A1	09-10-2014
US 2009251279 A1	08-10-2009	EP 1910134 A2	16-04-2008
		ES 2423679 T3	23-09-2013
		US 2009251279 A1	08-10-2009
		WO 2007009453 A2	25-01-2007
US 2014188348 A1	03-07-2014	CN 103905127 A	02-07-2014
		DE 102013224330 A1	03-07-2014
		US 2014188348 A1	03-07-2014
WO 2008063899 A2	29-05-2008	US 2008235509 A1	25-09-2008
		WO 2008063899 A2	29-05-2008
FR 2774833 A1	13-08-1999	AT 273541 T	15-08-2004
		DE 69919331 D1	16-09-2004
		EP 1055203 A1	29-11-2000
		FR 2774833 A1	13-08-1999
		JP 2002502925 A	29-01-2002
		WO 9940546 A1	12-08-1999
US 7366677 B1	29-04-2008	AUCUN	
EP 0492692 A2	01-07-1992	AU 632721 B2	07-01-1993
		AU 8966491 A	25-06-1992
		DE 69112191 D1	21-09-1995
		DE 69112191 T2	04-01-1996
		EP 0492692 A2	01-07-1992
		JP H086520 B2	24-01-1996
		JP H04302682 A	26-10-1992
		US 5144667 A	01-09-1992

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
Ｈ０４Ｗ 12/06 (2009.01)	Ｈ０４Ｗ 12/06	

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

（特許庁注：以下のものは登録商標）
１．ＱＲコード
２．ブルートゥース
３．ＢＬＵＥＴＯＯＴＨ

(74)代理人 100105153
弁理士 朝倉 悟
(74)代理人 100127465
弁理士 堀田 幸裕
(74)代理人 100208188
弁理士 榎並 薫
(72)発明者 ローラン、ペーテル
フランス国クレテイユ、セデックス、リュ、オーギュスト、ペレ、７６－ゼッドイ、ウーロパルク、ケアオブ、ヴァレオ、コンフォート、アンド、ドライビング、アシスタンス

Ｆターム(参考) 5J104 AA08 KA03 NA02 NA11 NA38
5K067 AA15 AA34 BB03 DD17 DD23 EE02 EE25 EE35 HH22 HH36

【要約の続き】
タ要素（ＲＰＡｉ）が有効であることを検証し、次いで前記モバイル電子装置（ＳＰ）から前記車両（Ｖｉ）の前記電子モジュール（１２０）に接続リクエスト（１１０）を発信するステップと、
を備えることを特徴とする方法、に関する。