(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-18804
(P2006-18804A)
(43)公開日　平成18年1月19日(2006.1.19)

(51)Int.Cl.		F I			テーマコード（参考）
G07B 15/00	(2006.01)	G07B	15/00	510	3E027
G06Q 50/00	(2006.01)	G07B	15/00	L	5H180
G06Q 10/00	(2006.01)	G06F	17/60	112Z	5J104
G08G 1/017	(2006.01)	G06F	17/60	512	
G08G 1/09	(2006.01)	G08G	1/017		

審査請求 有　請求項の数 5　OL　外国語出願　（全 8 頁）　最終頁に続く

(21)出願番号　特願2005-141673 (P2005-141673)
(22)出願日　平成17年5月13日 (2005.5.13)
(31)優先権主張番号　102004024421.9
(32)優先日　平成16年5月14日 (2004.5.14)
(33)優先権主張国　ドイツ(DE)
(31)優先権主張番号　102004037447.3
(32)優先日　平成16年8月2日 (2004.8.2)
(33)優先権主張国　ドイツ(DE)

(71)出願人　598051819
ダイムラークライスラー・アクチェンゲゼルシャフト
ドイツ連邦共和国　７０５６７　シュトットガルト，エップルシュトラッセ　２２５
(74)代理人　100123342
弁理士　中村　承平
(74)代理人　100111143
弁理士　安達　枝里
(72)発明者　ヴォルフガンク・ベイヤー
ドイツ連邦共和国　７１２６３　ヴァイルデア　シュタット、アルテ　レーニンガーシュトラーセ　１２３

Fターム(参考)　3E027 EA01 EC06 EC07
5H180 AA01 BB04 BB05 EE10
5J104 KA05 PA01 PA07 PA16

(54)【発明の名称】通行料金登録用通信システム

(57)【要約】
【課題】　通行料金登録用通信システムを提供する
【解決手段】　本発明は、車両と、車両に割り当てられ、対応する通信装置を備えた通行料金オペレータとの間の、無線通信用の通信装置を備えた車両についての、通行料金登録用通信システムに関する。この場合、車両は、通行料金オペレータに割り当てられた通行料金登録エリア内の、通行料金オペレータに関連する通行料金情報を送信し、通行料金オペレータは、これから、課金されるべき通行料金を決定又は請求する。車両が、その通信装置により、車両に割り当てられた通行料金オペレータの通行料金登録エリア外の他の通行料金オペレータと通信する場合は、割り当てられた通行料金オペレータの証明書が正常に送信され、かつ公開キー又は秘密キーに基づく場合にのみ、通行料金を登録するために、通行料金関連情報の交換が行われる。
【選択図】　図１

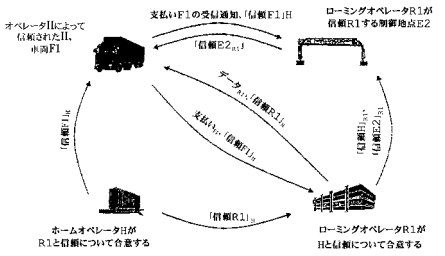

図１

【特許請求の範囲】
【請求項１】
車両と、該車両に割り当てられ、対応する通信装置を備えた通行料金オペレータとの間の無線通信用の通信装置を備えた車両についての、通行料金登録用通信システムであって、車両が、通行料金オペレータに割り当てられた通行料金登録エリア内の前記通行料金オペレータに関連する通行料金情報を送信し、前記通行料金オペレータが、前記車両から課金されるべき通行料金を決定又は請求する通行料金登録用通信システムであって、
通信装置により、車両（Ｆ１）が、通行料金を登録するために、該車両に割り当てられた通行料金オペレータ（Ｈ）の通行料金登録エリア外の他の通行料金オペレータ（Ｒ１）と通信し、前記割り当てられた通行料金オペレータ（Ｈ）の証明書が正常に送信されかつ公開キー又は秘密キーに基づく場合にのみ、通行料金関連情報を交換するための正常な通信が行われることを特徴とする通行料金登録用通信システム。
【請求項２】
前記証明書が、車両（Ｆ１）に割り当てられた通行料金オペレータ（Ｈ）と、他の通行料金オペレータ（Ｒ１）又は前記車両又は通行料金登録用通信システムの別の地点の通行料金制御地点（Ｅ２）との間で、双方により定義されることを特徴とする請求項１に記載の通行料金登録用通信システム。
【請求項３】
前記証明書が、中央認証地点なしで定義されることを特徴とする請求項２に記載の通行料金登録用通信システム。
【請求項４】
証明書の送信が、該送信された証明書が正常であると認証された通信当事者のものである場合に、正常であると評価されることを特徴とする請求項１～３のいずれか一項に記載の通行料金登録用通信システム。
【請求項５】
前記証明書及び前記公開キー又は秘密キーが、共に送信されることを特徴とする請求項１～４のいずれか一項に記載の通行料金登録用通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通行料金登録用通信システムに関する。
【背景技術】
【０００２】
従来、通行料金オペレータに、１つの通行料金登録領域がそれぞれ割り当てられ、前記通行料金オペレータが、このエリアに入ってくる交通量に従って通行料金を直接請求する通行料金に関する概念が知られている。この概念には、請求項１の前文による、通行料金登録用通信システムが必要である。
【０００３】
通行料金システムの複数のオペレータが、オペレータ自身の各領域内で通行料金を請求するために、互いの車両又は車両装置を受け入れる場合には、不正行為からシステム全体を保護するための手段にかかる要求及びすべての関係者にかかる要求が複雑なものになる。
【０００４】
銀行業務の分野において、ヨーロッパでは、階層的なキー管理システムを選択することにより、このような複雑な構造及び要求が取り扱われてきた。欧州中央銀行が主要なキーを有し、その公開部分は全員に知られており、その下のそれぞれの階層層には欧州中央銀行によって承認されたキーがあり、したがって、この下の層において取り扱いが行われる。この結果、ある銀行が、最初はその階層母体のキーのみを信頼しているが、その後、承認チェーンにより階層構造の上まで上がり、再び対応する銀行へと下がってくると、どのような銀行であれ、他の任意の銀行の公開キーをチェックすることができる。この解決方

法の欠点は、通行料金の分野においては不可能な、明確に定義された階層構造がなければならないことである。このような中央キー管理機能は、このような装置が強力であることにより、許容できるものではない。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

本発明は、そのホームエリア内ではない通行料金登録エリア内にある車両のために、無理なくかつ信頼できる方法で、通行料金を登録できるようにする通行料金登録用通信システムを提供する目的に関するものである。

【課題を解決するための手段】

【０００６】

この目的は、請求項１の特徴を有する、通行料金登録用通信システムによって達成される。

【０００７】

本発明の利点が、従属項の主題として記載されている。

【０００８】

本発明による通信システムにより、たとえば、その通行料金オペレータの登録エリアとは異なる通行料金登録エリア内にある車両が、ローミング通行料金オペレータ又はローミング当事者とも呼ぶ、他の通行料金オペレータに、直接又は間接的に交信することができる。この場合、充分に安全な情報を確実なものにするために、公開キー又は秘密キーに基づいて、さらに、通常は２人の通行料金オペレータの間で協議されたものであり、かつ証明書の送信者が証明書の生成者と同様に信頼できるものであるということを示した証明書に基づいて、通信が使用される。このことにより、たとえば、通行料金オペレータ（車両自身の通行料金オペレータと別の通行料金オペレータ／ローミング当事者）の間の合意により、証明書の送信者が信頼の置けるものであると考えられ、この結果、証明書及び使用される公開キー及び／又は秘密キー、及び／又はこれから導き出された対称キーの両方に基づいて、安全な送信、したがって送信内容についての信頼が得られることが確実となり、双方が、情報の安全な送信について直接合意する必要がない。

【０００９】

通行料金オペレータだけでなく、通行料金システムの様々な個々の地点においても、双方が、これに対応する方法で、中央認証地点を必要とせずに、このような証明書又はこれに相当する証明書について合意することができ、したがって、無線通信用の通信装置による、通行料金システムの様々な加入者の間の安全な通信が可能となる。この安全かつ信頼の置ける通信に基づいて、車両と、他の通行料金システムの他の地点、たとえば制御ブリッジ、請求地点などとの間で、通行料金関連情報を実施することができる。

【００１０】

通行料金システムのすべての当事者又は地点に等しい優先度が与えられるキー管理システムを備えた、通行料金を登録する、決定する、又は請求するための通信システムを提案することが特に適切であることが実証されている。どの当事者も、自分の秘密キーを自身で定義し、必要な場合には、契約当事者（たとえば近隣の通行料金オペレータ）との相互信頼について合意することができ、当事者は、これに対応する証明書を相互に発行することができる。これらの証明書は、特に各端末、たとえばあるオペレータの車両装置及び他のオペレータの制御システムに、特にオフラインで送信される。この場合、証明書だけでなく、通信している当事者間の通信をさらに確実にする秘密キー及び公開キーも使用される。適宜、発行地点への受信通知なしで機能する、このような証明書が交換される場合には、許容できる程度の経費で、信頼できる安全なプロセスが、未知のユニットの間で行われ得る。

【００１１】

この場合、中央認証地点としての中央「トラストセンター」は必要ない。ヨーロッパでは、それぞれの通行料金オペレータが、オペレータの双方が他の当事者と合意した付属の

証明書と共に、自身のキーを生成することにより、自身の車両ユニットを設定する。ローミングの場合には、つまり、あるオペレータの車両が別のオペレータの登録エリアに入ってくるような状況においては、車両及び通行料金システムの制御装置も、不正行為を防止しながら、これらの外部装置／車両を取り扱うことができる。

【００１２】

新しいオペレータがいる場合には、すべての車両装置は、既に設定されている場合でも、オペレータの間で、これに対応する証明書についての合意がなされ、通信中に証明書が交換されると、不正行為を防止しながら、新しい通行料金エリア内を継続して操作することができる。

【００１３】

送信された証明書が正常に認証された通信当事者のものである場合には、その証明書の送信が正常であると評価されることが、特に適切であることが実証されている。この結果、通信システムに対する信頼を伝播する又は浸透させることができ、このことにより、キー管理を組織化するための経費が著しく削減される。証明書及び公開キー又は秘密キーが、特に統合された形で共に送信される場合に、組織化又は送信に要する経費がさらに減少し得る。このことは、セキュリティに著しい悪影響を及ぼすことなく実施され得る。

【００１４】

通行料金オペレータは、基本的に、自身の通行料金システムを操作するのではないが、通行料金支払い用プロセッサとしての機能を果たしている会社でもあり得る。このような会社は、たとえば、通行料金システムを操作するのではないが、ローミング当事者との契約に基づいて、通行料金支払いの処理を行う銀行であり得る。

【００１５】

以下、例示的実施形態により、本発明についてより詳細に説明する。本発明は、この実施形態に限定されるものではない。さらに好ましい詳細が、この例示において見出され得る。

【発明を実施するための最良の形態】

【００１６】

図１は、通行料金システムの様々な構成要素又は地点の相互作用の関係の図式的な説明図である。通行料金システムのこれらの構成要素又は地点は、本発明による通信システムを用いて、相互に交信する。

【００１７】

以下の例示的シーケンスが発生する。即ち、

【００１８】

通行料金オペレータＨは、車両装置Ｆ１を設定し、（安全な方法で格納されている）そのホームオペレータＨの公開キー、及びオペレータＨを信頼するそれぞれの受取人にもＦ１の公開キーを信頼するよう要請する証明書を、この車両装置に与える。この証明書は、オペレータＨの秘密キーで署名されている。

【００１９】

ホームオペレータＨはまた、契約当事者との相互信頼について合意するが、この場合、また、そのローミング当事者である別の通行料金オペレータＲ１に、ホームオペレータＨを信頼するすべての受信者にもＲ１を信頼するよう要請する証明書を転送する。

【００２０】

次いで、車両は、ローミング当事者Ｒ１の領域に入ると、そこで、通行料金関連データの後で、たとえば、道路通行料金を支払うための決定に必要な道路データの後で問い合わせを行う。

【００２１】

ローミング当事者Ｒ１は、その秘密キーで署名されたデータレコードで応答し、同時に（又はこの前のサインオンプロセス中に）、ホームオペレータＨによって発行された、Ｈを信頼するそれぞれの受信者にもそれ（Ｒ１）を信頼するよう要請する証明書を送信する。

【００２２】
無線通信用の通信装置を含む車両装置は、（保証された）Ｈの公開キーを認識しているので、証明書の署名を検査することができ、したがって、ローミング当事者Ｒ１のデータを信頼する。
【００２３】
車両装置が、ローミング当事者Ｒ１のデータから、支払うべき区間を検出すると、支払い伝票が生成され、自身の秘密キーで署名される。（秘匿性を保護するために、この情報及び恐らく他の情報、さらに受信者の公開キーを有するデータレコードが暗号化され得る。）この署名された支払レコードが、すべての当事者にＦ１を信頼するよう要請するホームオペレータの証明書と共に、オペレータＲ１に送られる。したがって、前記オペレータＲ１は、証明書の署名及び車両ユニットＦ１の署名を信頼し、支払いを受け入れる。
【００２４】
オペレータＲ１はまた、証明書ＨによりＦ１に対する信頼を表明した結果として、この支払いも信頼しなければならず、これをその当事者Ｈに提出することができる。したがって、ＨからＲ１への、これに対応する支払いの流れが保証される。
【００２５】
車両Ｆ１が、ローミング当事者Ｒ１の通行料金エリア内の制御地点Ｅ２に到着すると、制御地点Ｅ２から、Ｒ１を信頼するすべての受信者にもＥ２を信頼するよう要請する、そのローミング当事者Ｒ１から受信された証明書が送られる。車両装置は、データが送信された時には既に取得されている証明書により、既にＲ１を信頼しており、したがって、有効な制御地点としてＥ２も信頼する。
【００２６】
したがって、車両装置は、この制御地点に、Ｆ１自身が署名した支払いの受信通知を送信し、同時に、前記車両装置は、Ｈが発行した自身の証明書も送るが、この証明書では、Ｈを信頼するすべての受信者にもＦ１を信頼するよう要請している。
【００２７】
この場合、Ｅ２は、自身のローミング当事者Ｒ１の自身のコントロールセンタにより、ホームオペレータＨを信頼するよう既に要請されており、このことは、ホームオペレータＨとローミング当事者Ｒ１との間の契約によって合意されている。この結果、制御地点Ｅ２は、車両装置のホームオペレータＨを既に信頼しており、その証明書の評価により、Ｅ２はまた、車両装置Ｆ１を、したがって支払いの受信通知を信頼する。
【００２８】
このことにより、提供されたセキュリティに基づいて、ホームオペレータＨにより、別の通行料金登録領域からの、たとえばローミング当事者Ｒ１の領域からの、通行料金総額を請求することが確実に可能となる。この場合、複数の通行料金登録領域が重なっていることもある。
【００２９】
この実施形態は、非常に安全かつ構造上簡単な通信方法、したがって、中央認証地点が不要となる通行料金の登録を提供するものである。
【００３０】
通行料金オペレータＨは、基本的に、自身の通行料金システムを操作するのではないが、この場合、通行料金支払い用プロセッサとしての機能を果たしている会社でもあり得る。このような会社は、たとえば、通行料金システムを操作するのではないが、ローミング当事者との契約に基づいて、通行料金支払い処理を行う銀行であり得る。
【図面の簡単な説明】
【００３１】
【図１】本発明による通信システムを備えた通行料金システムの概略的な構造を表す。
【符号の説明】
【００３２】
Ｈ　通行料金オペレータ

Ｆ１　車両（装置）
Ｒ１　通行料金オペレータ（ローミング当事者）
Ｅ２　制御地点

【図１】

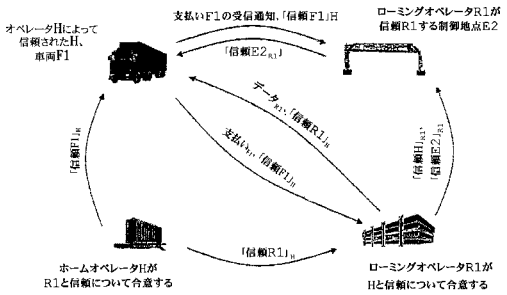

図１

フロントページの続き

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	***(2006.01)***	G08G	1/09	F	
		H04L	9/00	675B	

【外国語明細書】
2006018804000001.pdf
2006018804000002.pdf
2006018804000003.pdf
2006018804000004.pdf