(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5189073号
(P5189073)

(45)発行日　平成25年4月24日(2013.4.24)　(24)登録日　平成25年2月1日(2013.2.1)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
G09C	1/00	(2006.01)	G09C	1/00	640E
B60R	25/04	(2013.01)	B60R	25/04	608

請求項の数 9　(全 18 頁)

(21)出願番号	特願2009-502010 (P2009-502010)
(86)(22)出願日	平成19年3月15日 (2007.3.15)
(65)公表番号	特表2009-531893 (P2009-531893A)
(43)公表日	平成21年9月3日 (2009.9.3)
(86)国際出願番号	PCT/EP2007/052459
(87)国際公開番号	WO2007/113093
(87)国際公開日	平成19年10月11日 (2007.10.11)
審査請求日	平成22年3月4日 (2010.3.4)
(31)優先権主張番号	102006015212.3
(32)優先日	平成18年3月30日 (2006.3.30)
(33)優先権主張国	ドイツ(DE)

(73)特許権者　599147447
ブンデスドルケライ　ゲーエムベーハー
ＢＵＮＤＥＳＤＲＵＫＥＲＥＩ　ＧＭＢＨ
ドイツ連邦共和国，１０９５８　ベルリン，オラニーンシュトラーセ　９１
(74)代理人　100104156
弁理士　龍華　明裕
(74)代理人　100118005
弁理士　飯山　和俊
(74)代理人　100143502
弁理士　明石　英也
(74)代理人　100138128
弁理士　東山　忠義
(74)代理人　100112520
弁理士　林　茂則

最終頁に続く

(54)【発明の名称】動産、特に自動車を未許可の使用から保護する方法、コンピュータプログラム、および動産

(57)【特許請求の範囲】

【請求項１】

航空機、車両、特に乗用車、または、建設作業機械、モバイル機器、ポータブルコンピュータ、特にラップトップコンピュータ、または、携帯電話である動産を未認可の使用から保護する方法であって、

前記動産の暗号化認証をコンピュータシステムにより実行することであって、前記暗号化認証は、前記動産に帰属する非対称の対のキーを用いて実行され、前記非対称の対のキーは秘密キーと公開キーを含み、コードは前記動産の電子部品群の一つ以上の識別子から生成され、前記コードは前記秘密キーを用いてサインされ、前記コードは前記動産の識別のために使用されることと、

前記動産を識別する識別子又はコードと、前記公開キーとを含む証明書、およびサイン入りコードを前記動産から前記コンピュータシステムに送信することと、

前記動産からの前記サイン入りコードと前記証明書を前記コンピュータシステムにより受信することと、

前記サイン入りコードの有効性を前記コンピュータシステムにより前記公開キーを用いて確認することであって、前記証明書がコードを含む場合に、前記サイン入りコードは前記証明書内のコードと比較され、前記サイン入りコードが前記証明書のコードに一致すれば、前記サイン入りコードは有効であると確認し、または、前記証明書が前記動産を識別する識別子を含む場合に、前記サイン入りコードは、前記コンピュータシステムに格納された属性テーブル内において、前記証明書に含まれる前記識別子に関連付けられたコード

と比較され、前記サイン入りコードが当該コードに一致すれば、前記サイン入りコードは有効であると確認することと、
前記動産に関するブロッキングが格納されているかを前記コンピュータシステムにより確認することと、
前記動産に関するブロッキングが格納されておらず、前記サイン入りコードが有効な場合に、前記動産を使用できるようにすべく使用信号を前記コンピュータシステムから前記動産に送信することと、
前記動産に関するブロッキングが格納されている、または前記サイン入りコードが有効でない場合に、ブロッキング信号を前記コンピュータシステムから前記動産に送信することと
を含む方法。
【請求項２】
前記コンピュータシステムは、前記ブロッキングを格納するデータベースを含み、前記コンピュータシステムは、前記動産に関するブロッキングが前記データベースに格納されているかどうかを確認すべく、前記動産の前記暗号化認証が完了した後に、前記データベースにアクセスする請求項１に記載の方法。
【請求項３】
前記コンピュータシステムにより補助コードを受信することと、
前記補助コードの補助証明書を生成することと、
前記補助証明書を、安全な接続を介して前記動産に送信することにより、そこに格納されている前記証明書を交換することとを含む請求項１または２に記載の方法。
【請求項４】
前記動産の地理的位置を定義する位置信号は、前記動産が前記ブロッキング信号を受信した後に前記動産により送信される請求項１に記載の方法。
【請求項５】
請求項１から４のいずれか１項に記載の方法を実行するための複数の命令を含むコンピュータプログラム。
【請求項６】
航空機、車両、特に乗用車、または、建設作業機械、モバイル機器、ポータブルコンピュータ、特にラップトップコンピュータ、または、携帯電話である動産であって、
電子デバイスを含み、前記電子デバイスは、
前記動産に帰属する、秘密キーと公開キーを含む非対称の対のキーを用いた暗号によって当該動産を認証する手段と、
前記電子デバイスおよび／または前記電子デバイスとネットワーク接続されうる前記動産の電子部品群の一つ以上の識別子から、前記動産の識別に使用されるコードを得る手段と、
前記秘密キーを用いて前記コードにサインする手段と、
サイン入りコードと証明書をコンピュータシステムに送信する手段と
使用信号またはブロッキング信号を前記コンピュータシステムから受信する手段と
を含み、
前記証明書は公開キーを含み、前記証明書はコードまたは前記動産を識別する識別子を含み、前記コードまたは前記識別子は、前記サイン入りコードの有効性を確認するために前記コンピュータシステムによって使用される
動産。
【請求項７】
前記電子部品群の電子部品のそれぞれは、内部の不揮発性メモリに格納されている前記識別子を有し、前記コードを得る手段は、予め定められたアルゴリズムを実行し、前記アルゴリズムを使って前記識別子に基づいてコードを生成するために、前記電子部品のそれぞれから前記識別子を要求するよう構成されている請求項６に記載の動産。
【請求項８】

前記電子部品の暗号化認証を実行するための手段を含み、
前記電子部品のそれぞれは、非対称の対のキーを含み、
前記電子デバイスは、擬似乱数を生成し、前記擬似乱数を前記電子部品群のうちの一の電子部品の前記非対称の対のキーの公開キーを用いて暗号化し、暗号化された前記擬似乱数を当該一の電子部品に送信し、
前記電子部品の暗号化認証を実行するための手段は、前記暗号化された擬似乱数を当該一の電子部品における前記非対称の対のキーの秘密キーを用いて復号し、復号された擬似乱数を、前記電子デバイスに返信する請求項６または７に記載の動産。
【請求項９】
前記電子デバイスは、自動車の電子デバイス、特に制御ユニットである請求項６から８のいずれか１項に記載の動産。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、動産を未許可の使用から保護する方法、それに対応するコンピュータプログラム製品、コンピュータシステム、および、自動車の電子デバイスに関する。
【背景技術】
【０００２】
ＵＳ　２００２／０１３５４６６　Ａ１では、サーバコンピュータを有する自動車に接続されることができるＰＤＡの認証について記載されている。この場合、ＰＤＡは、車両を発進させるキーの機能を果たす。これには不都合な点があり、ＰＤＡを手に入れた泥棒は、車両を使用することができてしまう。さらに、自動車電子装置を不正に操作して車両の身元を変えられてしまう。
【０００３】
ＤＥ　４４４０９７５　Ｃ２には、車両が第三者によって使用されることを防ぐ装置が記載されている。この装置は、電磁波に基づく送信ラインを介し自動車外の場所との間で使用信号を周期的かつ逐次的に送受信し、車両の動作に必要な１つ以上の車両のパーツを、使用制御装置によって動作状態に維持するよう設計される。使用信号は、２つの連続する使用信号間の時間差より長い予め決められた期間に使用制御装置によって受信される。一方で、この確定した期間内にさらなる使用信号が受信されなければ、各パーツのさらなる動作および自動車の次なる動作は完全に阻止される。したがって、自動車を使用するためには、許可を与える信号を受信することが必要となる。
【０００４】
自動車が盗まれると、認可されている持ち主は直ちにその場所に盗難を通知し、許可されていた使用信号の送信は、止められる。それによって使用制御装置が車両のさらなる動作を阻止する。これは、使用信号が送信されなくなった直後、あるいは、新たな時間間隔の期限が切れた直後のいずれでも起きうる。例えば、認可されたパーツの動作時間内に新たな使用信号が受信されない場合、対応する車両のパーツは、予め定められた期間は使用制御信号による動作を維持するであろうし、その結果、車両は危険な状態にさらされるか、または、使用できる状態になってしまう。時間間隔の期限が切れ次第、対応する車両のパーツは、次回エンジン始動スイッチを切った後に使用制御装置によって動作を止められるので、動作状態には戻れない。
【０００５】
無線ネットワークによって使用信号を送信することは、不正な操作に対しては大いに効力があるものと想定される。それは、システムの裏をかく目的で、どこか他の場所で使用信号を生成することができるようにすべく、異なる車両向けに発信された多数の信号から適切な車両に宛てた信号を検出することは、認可された人物にとっても、とりわけ未認可の人物にとっても不可能なはずだからである。必要に応じて、コードベースの使用信号の送信が導入されるが、一般的には、例えば、電子キーの暗号化によるアクセス認可システムにおける使用コードの送信として導入される。

【０００６】
しかしながら、その車両が自動車に帰属するコードにより識別される間のこのようなコードベースの使用信号の送信は、例えば、自動車電子装置を不正に操作することにより検出され、回避されうる。
【発明の開示】
【０００７】
一方、本発明は、動産、特に車両を未認可の使用から保護するための改良された方法を生成することを課題とし、また、それに対応するコンピュータプログラム製品、コンピュータシステム、さらに、動産を未認可の使用から保護するための改良された電子デバイスを課題とする。
【０００８】
これらの課題は、請求項に記載された特徴によりそれぞれ解決される。本発明の好適な実施形態は、独立請求項に示されている。
【０００９】
本発明によれば、動産を未認可の使用から保護するための方法は、動産を外部コンピュータシステムによって暗号化身元確認および／または暗号化認証することと、動産に対するブロッキングが格納されたか確認することと、動産に対するブロッキングが存在しない場合、動産の使用を可能にすべく、コンピュータシステムから動産に信号を送信することと、を含む。
【００１０】
本発明によれば、動産は、例えば、航空機、車両、特に自動車、建設作業機械、モバイル機器、ポータブルコンピュータ、特にラップトップコンピュータ、携帯電話、スマートフォンなどの移動可能な固定資産であり、特に、１つ以上の電子部品を含む移動可能な固定資産であると考えられている。
【００１１】
最先端の技術とは異なり、動産自体、例えば自動車の暗号化身元確認および／または暗号化認証は、本発明では、外部コンピュータシステムにより行われる。これによって、コンピュータシステムから送信された使用信号またはブロッキング信号が、自動車電子装置を不正に操作することによって身元が変えられてしまっている盗まれた自動車でなく、認可された自動車に届くことを確実にする。
【００１２】
本願明細書中、「認可」とは、自動車の身元を照明することであると理解される。身元は、例えば、対応する証明書だけでなく、車両またはその自動車電子装置に帰属する非対称の対のキーに基づいて照明される。証明書は、自動車および／またはその自動車電子装置を識別する識別子を含む。
【００１３】
本願明細書中、「身元確認」とは、自動車および／またはその自動車電子装置のすでに知られた身元を確認することであると理解される。したがって、認可は、例えば、その後、身元を保証するのであれば、暗号法なしで行える、すなわち、身元の確認は、暗号法によってもよらなくても行うことができる。また、身元の確認は、非対称の対のキーと、自動車またはその自動車電子装置に帰属する対応する証明書に基づいてもよい。
【００１４】
本発明の一実施形態によれば、暗号化身元確認および／または暗号化認証は、したがって、自動車に帰属する非対称の対のキーを用いて実行される。
【００１５】
暗号化身元確認および／または暗号化認証の実行にあたり、コンピュータシステムは、例えば、乱数、特に擬似乱数を生成する。擬似乱数は、暗号化せずにコンピュータシステムから動産、例えば、自動車に送信される。擬似乱数は、自動車に帰属する秘密キーを用いて自動車電子装置により暗号化される。暗号化された擬似乱数は、自動車の証明書と共に、自動車からコンピュータシステムへと返送される。

【００１６】
その後、コンピュータシステムは、暗号化された状態で受け取られた擬似乱数を、受け取られた証明書の公開キーを用いて解読する。両方の擬似乱数が一致するということは、秘密キーおよび公開キーと、対応する証明書とからなる自動車に帰属する非対称の対のキーが有効であることを意味する。したがって、非対称の対のキーに帰属する証明書によって、自動車の身元は、明白に確認される。
【００１７】
本発明の一実施形態によれば、外部コンピュータシステムは、ブロッキングを格納するデータベースを有する。例えば、自動車が盗まれたことが知らされた場合、対応するブロッキングがデータベースに入力される。暗号化認証実行の後、コンピュータシステムは、暗号化身元確認および／または暗号化認証がなされている自動車がブロックの対象としてデータベースに入力されているかどうかを決定すべく、データベースにアクセスする。その場合は、コンピュータシステムは、対応するブロッキング信号を自動車に送信することにより、例えば、エンジン始動スイッチをオフにした後はエンジンがかからなくされる。
【００１８】
本発明の一実施形態によれば、コンピュータシステムは、自動車からサイン入りコードを受信する。コンピュータシステムは、サイン入りコードの有効性を確認する。サイン入りコードが有効である場合、さらに、自動車のブロッキングがデータベースに格納されていない場合のみ、コンピュータシステムは、自動車を使用できるようにすべく、自動車に使用信号を送信する。
【００１９】
コードは、例えば、通し番号、型番、製造番号、および／または、そのような一連の数字、または、そのような数字の１つ以上による他のアルゴリズムにより生成されるコードでありうる。例えば、自動車電子装置の１つ以上の構成要素の通し番号が入力されてコードとなる。コードは、例えば、通し番号を順序付けすることにより生成される。あるいはまた、通し番号、または、順序付けされた通し番号、型番、および／または、製造番号からハッシュ値が形成され、コードとして機能する。
【００２０】
コードは、自動車電子装置によりサインされ、外部コンピュータシステムに送信される。ここで、サイン入りコードは有効であることが確認される。自動車電子装置の不正操作が試みられている間に、例えば、コードを生成するためのその通し番号に関与する自動車電子装置の１つの構成要素が交換されることによってコードが変更され、その結果、外部コンピュータシステムにより受信されるサイン入りコードは無効にされる。外部コンピュータシステムがコードの無効を決定すると、ブロッキング信号が送信される。
【００２１】
本発明の一実施形態によれば、使用信号およびブロッキング信号はどちらもコンピュータシステムの秘密キーによってサインされる。サインは、どちらの場合も、使用信号またはブロッキング信号が有効になる前に、自動車電子装置により確認される。これによって、送信を認可されていない場所から使用信号またはブロッキング信号が送信できないようにすることを保証する。
【００２２】
本発明の一実施形態によれば、自動車電子装置に帰属する対のキーの証明書は、例えば、自動車電子装置の構成要素が修理のために交換される必要がある場合などには、補助証明書と置き換えられる。このような場合、コードは、構成要素を交換することによりに変更できる。補助証明書のリクエストは、好ましくは、認可された自動車修理場が行う。
【００２３】
本発明の一実施形態によれば、外部コンピュータシステムは、いわゆる公開鍵基盤（ＰＫＩ）のトラストセンターに所属している。
【００２４】
さらなる側面では、本発明は、本発明における方法を、例えば、トラストセンターのコ

ンピュータシステムで実行するためのコンピュータプログラム製品に関する。
【００２５】
さらなる側面では、本発明は、車両の暗号化身元確認および／または暗号化認証のための手段と、車両の使用状態を決定するための手段と、使用状態の関数としての信号を車両に送信する手段とを有するコンピュータシステムに関する。
【００２６】
さらなる側面では、本発明は、自動車電子装置により実行される、自動車を保護する方法に関する。方法は、自動車の暗号化身元確認および／または暗号化認証を外部コンピュータシステムにより実行することと、コンピュータシステムから使用信号およびブロッキング信号を受信することと、を含む。
【００２７】
本発明の一実施形態によれば、車両に帰属するコードが自動車電子装置によってサインされ、そのサイン入りコードが外部コンピュータシステムに送信されることにより、サイン入りコードの有効性がそこで確認される。自動車に帰属するコードは、自動車電子装置の構成要素内に格納されている、例えば、通し番号、型番、および／または、製造業者の識別子など、自動車電子装置の構成要素の１つ以上の識別子から生成されうる。したがって、自動車に帰属するコードは、その構成要素の実際の組成により定義される当該自動車の特性であり、いわば、当該自動車の「指紋」のようなものであるといえよう。
【００２８】
本発明の一実施形態によれば、ブロッキング信号が受信された後に自動車の実際の地理的位置を定義する位置信号が生成される。これによって、盗難されたことが届けられている自動車の発見が容易になる。
【００２９】
さらなる側面では、本発明は、本発明における方法を実行する、自動車電子装置により実行される命令を有するコンピュータプログラム製品に関する。
【００３０】
さらなる側面では、本発明は、例えば電子制御装置（ＥＣＵ）などの自動車電子装置に関する。自動車電子装置は、コンピュータシステムにより自動車の暗号化身元確認および／または暗号化認証を実行する手段と、コンピュータシステムから使用信号およびブロッキング信号を受信する手段とを有する。
【００３１】
自動車のコード特性を生成するにあたり、暗号化身元確認および／または暗号化認証のための自動車電子装置の個別の構成要素は、不正に操作されることを防止すべく、制御デバイスおよび／または互いによって形成されうる。
【図面の簡単な説明】
【００３２】
以下、本発明の実施形態が図面を参照しながらより詳細に記載される。
【００３３】
【図１】本発明におけるコンピュータシステム、および、本発明における自動車電子装置の一実施形態を示すブロック図である。
【００３４】
【図２】本発明における方法の一実施形態を示すフローチャートである。
【００３５】
【図３】本発明におけるコンピュータシステム、および、本発明における自動車電子装置のさらなる実施形態を示すブロック図である。
【００３６】
【図４】本発明におけるコンピュータシステム、および、本発明における自動車電子装置のさらなる実施形態を示すブロック図である。
【００３７】
【図５】本発明における方法の一実施形態を示すフローチャートである。

【００３８】
【図６】本発明におけるトラストセンターのコンピュータシステムおよびブロッキングサービス、および、本発明における自動車電子装置のさらなる実施形態を示すブロック図である。
【００３９】
【図７】本発明における方法のさらなる実施形態を示すフローチャートである。
【００４０】
【図８】本発明における方法のさらなる実施形態を示すフローチャートである。
【００４１】
【図９】本発明におけるトラストセンターのためのコンピュータシステム、本発明における自動車修理場のコンピュータ、および、本発明における自動車電子装置の一実施形態を示すブロック図である。
【００４２】
【図１０】本発明における方法のさらなる実施形態を示すフローチャートである。
【発明を実施するための最良の形態】
【００４３】
以下の実施形態において、対応する要素には同じ参照符号が付される。
【００４４】
図１は、例えば乗用車または営業車でありうる自動車１００を概略的に示す。自動車１００は、盗難に対する防御が特に必要な高級車である。
【００４５】
自動車１００は、１つ以上の自動車電子デバイスを含む自動車電子装置１０２を有する。自動車電子装置は、例えば、ＣＡＮおよび／またはＬＩＮバスを介し互いに通信しうるいわゆる電子制御装置（ＥＣＵ）であってよい。
【００４６】
暗号化プロトコルを実装すべく、命令１０４が自動車電子装置１０２により実行されうる。あるいはまた、自動車電子装置１０２は、加入者識別モジュール（ＳＩＭ）のフォーマットのチップカード用のチップカードリーダを含みうる。チップカードリーダは、命令１０４を実行するためのｍｉｃｒｏｍｅｔｈｏｄｏｒを含む。
【００４７】
自動車１００は、ネットワーク１０６を介し、コンピュータシステム１０８に接続される。ネットワーク１０６は、例えば、セルラー無線通信網、および／または、コンピュータネットワークなどの公衆通信網、特にインターネットでありうる。自動車電子装置１０２とコンピュータシステム１０８との間の通信は、例えば、グローバル・システム・フォー・モバイル・コミュニケーションズ（ＧＳＭ）、ユニバーサル・モバイル・テレコミュニケーション・システム（ＵＭＴＳ）、または、符号分割多重アクセス（ＣＤＭＡ）などのセルラー無線接続を介し、あるいは、アナログＦＭを介した、もしくはＴＭＣの一部としての他の無線接続の助けを借りて実装されうる。さらに、異なるメッセージ送信チャネルがアップリンク、すなわち、自動車電子装置１０２からコンピュータシステム１０８、および、ダウンリンク、すなわち、コンピュータシステム１０８から自動車電子装置１０２までの通信接続のために用いられうる。これは、同様に、コンピュータシステム１０８と１１４との間の通信を要求する。
【００４８】
コンピュータシステム１０８は、例えば、いわゆるトラストセンターなど高度なセキュリティ環境に好ましくは配置される。コンピュータシステム１０８は、暗号化プロトコルを実装するためのコンピュータプログラムの命令１１０を実行する。
【００４９】
暗号化プロトコルを用い、自動車１００の身元が決定されるおよび／または確認される。自動車１００は、例えば、自動車特有のコード、または、自動車の公式登録ＩＤなどの他の識別子により明白に識別される。このような自動車識別コード、または、このような

識別子あるいは車両ＩＤは、以下、自動車識別子（自動車ＩＤ）と称する。

【００５０】

自動車ＩＤをキーとして用いることにより、コンピュータシステム１０８は、紛失メッセージが作成される間に、ブロックされた自動車の自動車ＩＤが格納される記憶装置１１２にアクセスしうる。ブロックされた自動車の対応するブロッキングリストは、データベース形式の記憶装置１１２に格納されうる。

【００５１】

ブロッキングは、コンピュータシステム１０８を介し記憶装置１１２に直接入力されることができる。また、このようなブロッキングは、ネットワーク１０６または他の通信接続を介しコンピュータシステム１０８とデータを交換しうる他のコンピュータシステム１１４からも入力されることができる。

【００５２】

本実施形態では、コンピュータシステム１１４は、暗号化プロトコルを実装するためのコンピュータプログラムの命令１１６を実行する役割も果たす。暗号化プロトコルを用い、自動車のブロッキングを記憶装置１１２に入力するためのコンピュータシステム１１４の身元、および、その認証が決定および／または確認されうる。さらに、コンピュータシステム１１４は、自動車の紛失メッセージを記録するためのアプリケーションプログラム１１８を有する。

【００５３】

認可されたユーザにより自動車１００が使用される場合、記憶装置１１２には自動車１００に対するブロッキングは格納されていない。自動車１００の始動と同時に、例えば、自動車電子装置１０２またはチップカードにより、命令１０４の実行が開始される。自動車電子装置１０２は、ネットワーク１０６を介しコンピュータシステム１０８との接続を確立するので、命令１１０の実行はそこで開始される。自動車電子装置１０２によって命令１０４が実行されることにより、また、コンピュータシステム１０８によって命令１１０が実行される。例えば、自動車の自動車ＩＤの信ぴょう性が確認されることに基づいて暗号化プロトコルは実現する。自動車電子装置１０２とコンピュータシステム１０８との間の通信は、例えば、ｈｔｔｐなどのいわゆるリクエスト／レスポンスプロトコルに従い、ネットワーク１０６を介して実行される。

【００５４】

自動車１００の身元が暗号化プロトコルの方法により確認および／または認証された後、コンピュータシステム１０８は、自動車１００のブロッキングが記憶装置１１２に格納されているかどうかを確認する。この場合は格納されていないので、コンピュータシステム１０８は、ネットワーク１０６を介し、使用信号を自動車１００に送信する。使用信号が受信されたことによってのみ、自動車１００は使用されうる。使用信号の受信後、自動車１００のエンジンが始動されるだけでもよいし、または、エンジン始動ロック装置システムが停止されてもよく、あるいは、自動車１００の１つのおよび／または複数の手動ブレーキが、使用信号が受信された後にのみ解除されうる。

【００５５】

使用信号は、一定の有効期間を有しうるので、この方法は、有効期間が失効するまでは自動車１００が動作するたびに繰り返される。

【００５６】

自動車１００が盗まれてしまった場合、自動車１００の持ち主は、コンピュータシステム１１４を操作するブロッキングサービスとコンタクトを取ることができる。このようなブロッキングサービスは、例えば、サービス会社、公式機関または警察によって利用可能にされうる。

【００５７】

持ち主が自動車１００の紛失を通知すると、そのことがアプリケーションプログラム１１８により登録される。コンピュータシステム１１４は、コンピュータシステム１０８との接続を確立し、コンピュータシステム１１４の暗号化身元確認および／または暗号化認

証がコンピュータシステム１０８により実行される。その結果、ブロッキングリクエストがその目的のために認可されるコンピュータシステムによってのみ記録されることを確実にする。コンピュータシステム１０８によるコンピュータシステム１１４の暗号化身元確認および／または暗号化認証が成功した後、ブロッキングリクエストは、記憶装置１１２に格納されるよう、例えば、自動車ＩＤと共に、ネットワーク１０６を介しコンピュータシステム１１４からコンピュータシステム１０８へと送信される。

【００５８】

自動車１００が盗まれた後、また、ブロッキングが記憶装置１１２に格納された後に自動車１００のエンジン始動スイッチがかかると、自動車電子装置１０２により再び命令１０４の実行が開始される。自動車１００の身元確認および／または認証を実行した後、コンピュータシステム１０８は、自動車１００に対するブロッキングが記憶装置１１２に登録されていることを実際に決定する。したがって、コンピュータシステム１０８は、使用信号を自動車１００に送信しないので、自動車は使用できない。あるいは、この場合、コンピュータシステム１０８は、ブロッキング信号を自動車１００に送信して自動車を動けなくすることもできる。

【００５９】

自動車電子装置１０２に対する不正操作が試みられた場合、この安全機構を回避する目的で自動車電子装置１０２の１つ以上の構成要素を交換した場合、自動車ＩＤが変更されるので暗号化身元確認および／または暗号化認証は、確実に失敗する。この場合も、使用信号は送信されない。

【００６０】

命令１０４および１１０または１１６および１１０により実行される暗号化プロトコルは、例えば、以下のように進行しうる。

【００６１】

自動車電子装置１０２は、コンピュータシステム１０８にリクエストを送信する。そしてコンピュータシステム１０８は、乱数、特に擬似乱数を生成する。乱数は、ネットワーク１０６を介し、コンピュータシステム１０８から自動車１００へと返送される。自動車電子装置１０２は、例えば、チップカードに格納される秘密キーを用いて受信した乱数をエンコードするので、自動車電子装置は、暗号化された数を受け取る。

【００６２】

この暗号化された数も自動車電子装置１０２の証明書と同様に自動車電子装置１０２からコンピュータシステム１０８へと応答として返送される。コンピュータシステムは、証明書の公開キーを用いて暗号化された数を解読する。コンピュータシステム１０８に生成された乱数が自動車電子装置１０２からの応答として受信した乱数と一致すれば、自動車１００の身元確認および／または認証はうまくいったことになる。

【００６３】

例えば、自動車電子装置１０２は、暗号化プロトコルを開始する初期リクエストと共に、その対のキーに属する証明書をコンピュータシステム１０８に送信する。証明書は、自動車１００の自動車ＩＤを含みうるので、コンピュータシステム１０８は、記憶装置１１２へのアクセスのためのアクセスキーを自動車ＩＤの形式で受け取ることにより、当該車両に関するブロッキングが格納されているかどうかを確認する。

【００６４】

同じ原理に従い、コンピュータシステム１１４の暗号化身元確認および／または暗号化認証も、コンピュータシステム１０８を用いて進められることができる。コンピュータシステム１１４も、コンピュータシステム１０８からコンピュータシステム１１４の公開キーを用いてエンコードされた擬似乱数を受信し、受信した擬似乱数を、その秘密キーを用いて解読し、それをコンピュータシステム１０８に返送する。コンピュータシステム１０８によりエンコードされた乱数とコンピュータシステム１１４からの応答として返送された乱数とが一致すれば、暗号化身元確認および／または暗号化認証は、今回もうまくいったということである。

【００６５】
異なるコンピュータシステム１１４のそれぞれは、ネットワーク１０６を介しコンピュータシステム１０８と通信することができ、紛失メッセージを記録するために分散して配置されうる。例えば、このようなコンピュータシステム１１４は、警察署、認可された自動車売買業者または自動車修理場、および／または、自動車の紛失が電話、または、電子メールなどの他の手段によって連絡されうるコールセンターに配置されることができる。
【００６６】
これは、自動車の未認可の使用に対する効果的な防御となり、窃盗をしづらくする。本発明では、例えばバイオメトリック安全装置またはアラームなどのドライバーによって直接コントロールされうる安全装置は存在しないので、自動車の認可されたユーザをおびやかす潜在性はさらに減少する。
【００６７】
図２は、対応するフローチャートを示す。ステップ２００では、自動車の動作要素が起動される。例えば、自動車を開くための中心ロックの起動、エンジンをスタートさせるためのスタータの起動、または、それらを解除するための手動または足ブレーキの操作などである。
【００６８】
ステップ２００におけるような動作により、続いて、使用またはブロッキング信号を受信するための暗号化身元確認および／または暗号化認証の方法が開始する。例えば、自動車を開けるための遠隔制御の起動によりシーケンスがすでに始まっている場合、ドライバーが自動車に近づいて中に入る間に方法はすでに始まっており、ドライバーが自動車に到達しているときにはすでに決断が下されていて、その結果、中に入った後にはドライバーはわずかな遅れがあろうとなかろうと自動車を動かすことができるという利点を有する。
【００６９】
この方法は、例えば、いわゆるキーレスゴー・ロッキングシステムがすでに起動した後に自動的に開始されうる。したがって、ロッキングシステムが自動車の近傍でＲＦＩＤ（無線ＩＣタグ）キーカードを感知した場合、当該方法は開始される。
【００７０】
ステップ２０２では、対応するトラストセンターのコンピュータによる自動車の身元確認および／または認証は、暗号化プロトコルによる方法によってなされる（図１の命令１０４および１１０も参照のこと）。
【００７１】
自動車の暗号化身元確認および／または認証が無事終わると、トラストセンターは、当該自動車がブロッキングリストに載っているかどうかを確認する。載っていなければ、ステップ２０６において、その自動車に特有の自動車使用信号が生成されて当該自動車に送信される。
【００７２】
使用信号は、好ましくはトラストセンターによってサインされる。使用信号のサインは、トラストセンターの公開キーの助けを借りて自動車電子装置により確認される。使用信号のサインは、それが有効だったときのみ自動車が使用できるよう、自動車電子装置により受け入れられる。使用信号は、好ましくは、対応する自動車の自動車ＩＤも含む。
【００７３】
逆のケース、すなわち、自動車がブロッキングリストに載っていた場合、ブロッキング信号が生成され、自動車に送信される（ステップ２０８）。これによって、自動車は、直ちに、あるいは、例えば、次にスタートしようとしたときに動けなくなる。
【００７４】
自動車電子装置は、自動車の実際の地理的位置を含んだメッセージ付きのブロッキング信号に応答しうる。これによって自動車の発見が簡単になる。
【００７５】
図３は、トラストセンターおよび自動車電子装置１０２のコンピュータシステム１０８

の追加の実施形態である。コンピュータシステム１０８において、トラストセンター１０８の公開キー１３２および秘密キー１３４は、使用信号およびブロッキング信号にサインし、また、暗号化プロトコルを実行するために格納される。

【００７６】

本実施形態では、自動車電子装置１０２は、例えば構成要素Ａ、Ｂ、Ｃなど異なる構成要素１２０を有し、それらの構成要素は車両ネットワーク１２２を介し互いに接続される。自動車ネットワーク１２２は、例えば、ＣＡＮおよび／またはＬＩＮバスでありうる。

【００７７】

識別子は、構成要素１２０のそれぞれに帰属し、対応する構成要素の不揮発性または簡単に操作されない記憶装置に格納されうる。このようなコードは、例えば、対応する構成要素１２０の記憶装置１２４に格納される対応する通し番号でありうる。

【００７８】

構成要素１２０の少なくとも１つは、自動車１００に帰属する公開キー１２６および秘密キー１２８からなる対のキーへのアクセスを有する。対の公開キー１２６および秘密キー１２８は、証明書１３０に帰属する。

【００７９】

証明書１３０には、例えば、自動車１００を識別する役割を果たすコードが格納されている。このコードは、予め定められたアルゴリズムを実装する命令１０４を実行することによって生成される。命令１０４は、予め定められたアルゴリズムを実装する。それによって、異なる構成要素１２０の通し番号Ａ、Ｂ、Ｃは、当該予め定められたアルゴリズムの助けを借りてこれらの通し番号Ａ、Ｂ、Ｃに基づくコードを生成すべくクエリされる。

【００８０】

暗号化プロトコルの実行にあたり、命令１０４は、異なる構成要素１２０からの通し番号Ａ、Ｂ、Ｃをクエリすることによりコードを決定する。このようにして生成されたコードは、秘密キー１２８によってサインされ、証明書１３０と共にコンピュータシステム１０８に送信される。コンピュータシステム１０８は、公開キー１２６を用いてサインされたコードの有効性を確認する。サインされたコードが正しい場合、すなわち、証明書１３０に格納されたコードに対応する場合のみ、暗号化身元確認および／または認証は成功する。

【００８１】

暗号化身元確認の目的で通し番号から当該コードを生成することは、自動車電子装置１０２の構成要素１２０の１つを交換する場合、結果として生じるコードも必然的に変わるというメリットがある。このような場合、通し番号をクエリすることにより得られたコードと証明書１３０に格納されたコードとはもはや一致しないので、暗号化身元確認は必ず失敗する。したがって、当該構成要素１２０の１つ以上を交換して自動車電子装置１０２を不正に操作することは防止される。

【００８２】

対のキー１２６および１２８と、証明書１３０とは、命令１０４の少なくとも一部も実行するチップカードに格納されうる。この場合、構成要素Ａは、対応する暗号化機能にアクセスできるようにすべくチップカードが挿入されるチップカードリーダを有する。

【００８３】

図４は、証明書が通し番号から得られたコードは含まないが他の明確な自動車ＩＤを含む他の実施形態を示す。このような自動車ＩＤは、例えば、自動車自身の通し番号、シャーシ番号、公式登録番号、または、他の明確なコードでありうる。

【００８４】

したがって、暗号化プロトコルの実行にあたり、自動車電子装置は、構成要素１２０の異なる通し番号から車両に特有のコードを決定する。このコードは、秘密キー１２８を用いてサインされ、ネットワーク１０６を介し証明書１３０と共にコンピュータシステム１０８に送信される。コンピュータシステム１０８は、自動車ＩＤをキーとして用いて属性テーブル１３６にアクセスすることにより、そこから自動車ＩＤに帰属する自動車に特有

のコードを読み出す。このコードは、コンピュータ１０８が自動車電子装置１０２から証明書１３０と共に受け取ったサイン入りコードと一致するはずなので、暗号化身元確認および／または認証を実行することができる。

【００８５】

図５は、対応するフローチャートを示す。自動車の暗号化身元確認および／または認証は、図２の実施形態におけるステップ２０２と同様に、図５の実施形態におけるステップ２０２'において実行される。あるいはまた、コードのクエリ、すなわち、通し番号は、この方法のために形成される制御デバイスにより自動車電子装置の構成要素の１つ以上によってステップ３００において実行される。例えば、ステップ３０２において、この制御デバイスは、通し番号から自動車に特有のコードを生成する。この自動車に特有のコードは、ステップ３０４において自動車の秘密キーの助けを借りてサインされ、ステップ３０６において対応する証明書と共にトラストセンターのコンピュータシステムに送信される。このコードが無効かどうかがここで確認される（ステップ３０８）。もし無効であれば、ステップ２０８が実行される。有効であれば、ステップ２０４が実行される。

【００８６】

制御デバイス１２０とサーバ１４０との間の通信は、好ましくは、安全なメッセージ送信手続きを介して実行される。

【００８７】

図６は、携帯電話ネットワーク１０６を介しコンピュータシステム１０８と通信する役割を果たす移動無線アンテナ１３８を有する自動車１００の一実施形態を示す。コンピュータシステム１０８は、命令１１０を実行させるサーバ１４０を有する。

【００８８】

コンピュータシステム１４０の対のキーは、公開キー１３２および秘密キー１３４からなり、本実施形態では、チップカード読み取りデバイスを介しサーバ１４０にアクセスできるチップカード１４２に格納される。本実施形態では、ブロッキングリストまたはブロッキング情報を格納するための記憶装置１１２は、サーバ１４０に接続される独立したデータベースとして形成される。

【００８９】

この場合、自動車電子装置の構成要素Ａ（図３および４参照）は、制御ユニットとして形成される。制御ユニットでは、自動車１００に帰属する非対称の対のキー１２６および１２８がチップカード１４４に格納され、チップカード１４４は、対応するチップカード読み取りデバイスを介して制御ユニット１２０によりアクセスされることができる。

【００９０】

この場合、自動車電子装置の追加の構成要素１２０は、エンジン電子部品、２つの電子部品、シャーシ電子部品であり、それらは、独立したＥＣＵとしてそれぞれ形成されうる。それぞれのＥＣＵには、個別の非対称の対のキー１４６、１４６'、１４６''、１４６'''が格納される。

【００９１】

例えば、構成要素１２０の通し番号などのコードのクエリの前に、まずそれらの身元が、暗号によって確認および／または認証されなければならず、それは、制御ユニット１２０により対応する対のキーの助けを借りて行われる。

【００９２】

それによって、制御ユニット１２０が擬似乱数を生成し、それを例えば対のキー１４６などの対応する対のキーの公開キーによりエンコードし、ネットワーク１２２を介して対応する構成要素１２０、考えられる例ではエンジン電子部品１２０に送信するといった段取りで進めることが再び可能になるだろう。

【００９３】

エンジン電子部品１２０は、制御デバイス１２０が受信した暗号化された数をその対のキー１４６の秘密キーの助けを借りて解読し、解読された数を制御デバイスに返送する。受信されてエンジン制御部品によって解読された数が最初に送信された乱数と一致したと

きのみ、通し番号はクエリされることができ、エンジン電子部品１２０の身元は、制御デバイス１２０により確認および／または認証される。

【００９４】

制御ユニットによる構成要素１２０の１つの暗号化身元確認および／または認証が失敗すると、制御ユニットは、コードを生成することができず、対応するエラーメッセージをコンピュータシステム１０８に送信することにより、自動車１００のブロッキングを始めることができる。

【００９５】

図７は、本発明に従う方法の別の実施形態を示す。ステップ４００において、車両は、例えば、スタータボタンを押すことにより起動される（図２および５のステップ２００を参照）。この後、ステップ４０２において、車両とトラストセンターとの間に通信接続が確立される。ステップ４０４において、データ接続を用い、第１の暗号化認証ステップが例えば上記のような擬似乱数を交換することにより実行される。

【００９６】

ステップ４０４において暗号化認証のこの第１のステップが成功に終った後、ステップ４０６において、トラストセンターは自動車のサイン入り自動車ＩＤをリクエストする。ステップ４０８において、自動車は、自動車ＩＤのサインを生成し、ステップ４１０においてそのサインをトラストセンターに送信する。ステップ４１２においてサインが確認される。このサインが有効であれば、暗号化認証の第２のステップも成功に終る。

【００９７】

次に、ステップ４１４において、当該自動車に関するブロッキングがブロッキングリストに入力されているかどうかが確認される。入力されていなければ、ステップ４１６において、リリースコード形式の使用信号が自動車に送信されてステップ４１８において受信される。その結果、自動車の使用が可能になる。

【００９８】

しかしながら、ステップ４１４において、自動車のブロッキングリストにブロッキングが載っていた場合、ステップ４１９においてブロッキングコード形式のブロッキング信号が自動車に送信され、ステップ４２０で受信される。続いて、ステップ４２２において、自動車は、例えば、ＧＰＳレシーバのリクエストによって現在の地理的位置を決定し、ステップ４２２において、その実際の位置をトラストセンターに送信する。ステップ４２４において、トラストセンターは、その位置情報を例えば警察に転送する。

【００９９】

図８は、本発明における、ブロッキングリストをアップデートする方法の一実施形態を示す。ステップ５００において、自動車のユーザまたは持ち主が自分の自動車が盗難にあったことを通知することにより、紛失メッセージがブロッキングサービスに届く。次に、ステップ５０２において、ブロッキングサービスとトラストセンターとの間にデータ接続が確立される。

【０１００】

ステップ５０４において、ブロッキングサービスは、トラストセンターによって認証される。認証が成功した後、ステップ５０６において、トラストセンターは、盗まれたことが通知された自動車に帰属する証明書のブロッキングがブロッキングサービス（ステップ５０８）によって入力されうるブロッキングマスクを生成する。ステップ５１０において、ブロッキングサービスの秘密キーを用いて証明書をブロッキングするリクエストがサインされ、トラストセンターに送信される。ステップ５１２において、トラストセンターは、ブロッキングサービスのサインを確認し、サインが有効であれば、ステップ５１４において、ブロッキングリストをしかるべくアップデートする。

【０１０１】

自動車の値段が高くても、自動車電子装置１０２の構成要素１２０のそれぞれは、時々故障する可能性があり、新しいものと交換しなければならない（図３および４参照）。構成要素１２０の１つを交換することにより、その識別子、例えば、通し番号も変更され、

したがって、結果として生じるコードも変わる。このような場合、証明書１３０は、リクエストされたような、アップデートされたコードを含む新しい証明書と交換されなくてはならない。これは、不正操作されるのを防止すべく、図９に示されるような、この目的のために認可された自動車修理場で行われなければならない。

【０１０２】

認可された自動車修理場は、例えば、自動車電子装置１０２用の異なる診断機能を有する特別なパソコンなどの自動車修理場のコンピュータ１４８を有する。自動車修理場のコンピュータ１４８は、例えば、１つ以上のケーブル１５０を介して自動車電子装置１０２と直接接続されうる。

【０１０３】

自動車修理場のコンピュータは、対応する認可された自動車修理場に帰属する証明書１５６に加えて、公開キー１５２および秘密キー１５４からなる非対称の対のキーを含む。認可された自動車修理場は、証明書１５６に示されている。

【０１０４】

自動車修理場のコンピュータ１５６は、例えば、ネットワーク１０６を介し、トラストセンターのコンピュータシステム１０８と通信しうる。コンピュータシステム１０８は、証明書を生成するための証明書生成機１５８を有する。

【０１０５】

自動車電子装置１０２の構成要素１２０に１つ以上が対応する交換パーツと交換された後、自動車修理場のコンピュータ１４８は、結果として生じたコードを自動車電子装置１０２から読み取る。自動車修理場のコンピュータ１４８は、コンピュータシステム１０８との接続を確立し、コンピュータ１０８によってそれ自身（コンピュータ１４８）を認証する。認証が成功した後、自動車修理場のコンピュータ１４８は、新しいコード付きの新しい証明書のリクエストをコンピュータシステム１０８に送信する。次に、証明書生成機１５８がそこで動作を開始し、自動車修理場のコンピュータ１４８を介してあるいは直接自動車電子装置１０２に入力される対応してアップデートされた証明書１３０を生成し、前の証明書１３０を上書きする。

【０１０６】

図１０は、対応するフローチャートを示す。自動車電子装置が修理された後、ステップ６０２において自動車電子装置と自動車修理場のコンピュータとの間でデータ接続が確立され（ステップ６００）、自動車修理場のコンピュータとトラストセンターとの間にもデータ接続が確立される。次に、ステップ６０４において、自動車修理場のコンピュータの身元がトラストセンターにより暗号的に識別および／または認証される。

【０１０７】

例えば、トラストセンターによる自動車修理場のコンピュータの暗号化認証が成功した後、ステップ６０６において、自動車修理場のコンピュータは電子部品の１つ以上の構成要素の交換から生じた新しいコードを自動車電子装置から読み取り（ステップ６０６）、これに基づきステップ６０８において対応する新しい証明書のリクエストをトラストセンターに送信する。

【０１０８】

このリクエストは、新しいコードも含む。次に、トラストセンターは、ステップ６１０において新しい証明書を確定し、ステップ６１２においてそれを自動車修理場のコンピュータに送信する。ステップ６１４において、自動車修理場のコンピュータは、例えば、古い証明書を新しい証明書で上書きすることにより、新しい証明書を自動車電子装置内にインストールする。例えば、新しい証明書は、安全なメッセージ送信により、自動車電子装置の制御デバイスのチップカードに直接書き込まれる（図６の制御デバイス１２０およびチップカード１４４参照）。

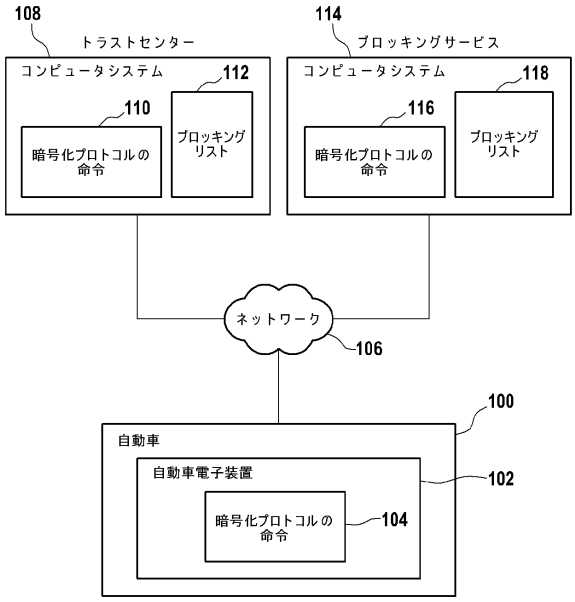
【参照符号】

【０１０９】

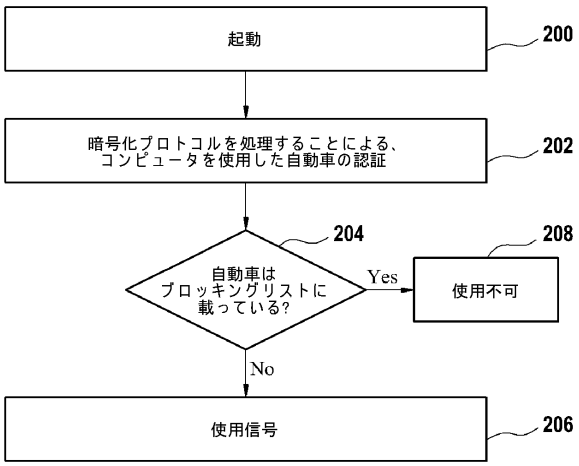
１００　自動車１０２　自動車電子装置１０４　命令１０６　ネットワーク１０８　コン

ピュータシステム１１０　命令１１２　記憶装置１１４　コンピュータシステム１１６　命令１１８　アプリケーションプログラム１２０　構成要素１２２　ネットワーク１２４　記憶装置１２６　公開キー１２８　秘密キー１３０　証明書１３２　公開キー１３４　秘密キー１３６　属性テーブル１３８　移動無線アンテナ１４０　サーバ１４２　チップカード１４４　チップカード１４６　対のキー１４８　自動車修理場のコンピュータ１５０　ケーブル１５２　公開キー１５４　秘密キー１５６　証明書１５８　証明書生成機

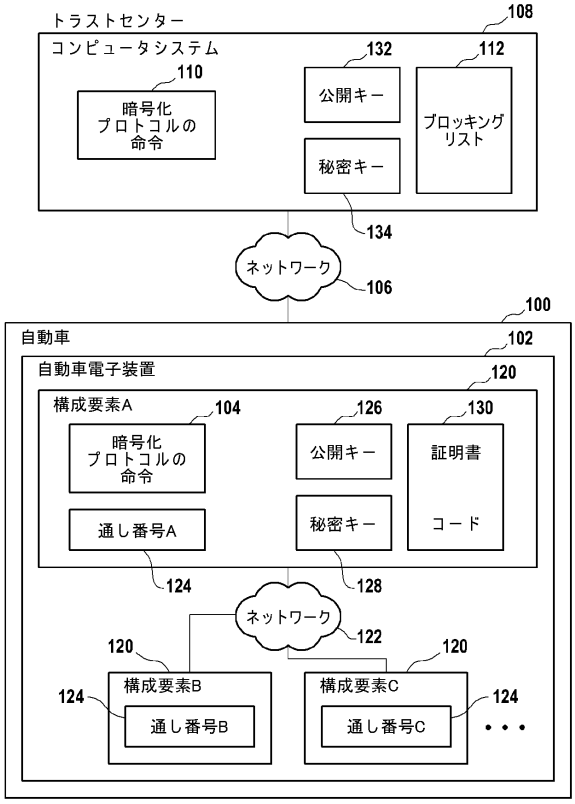
【図１】



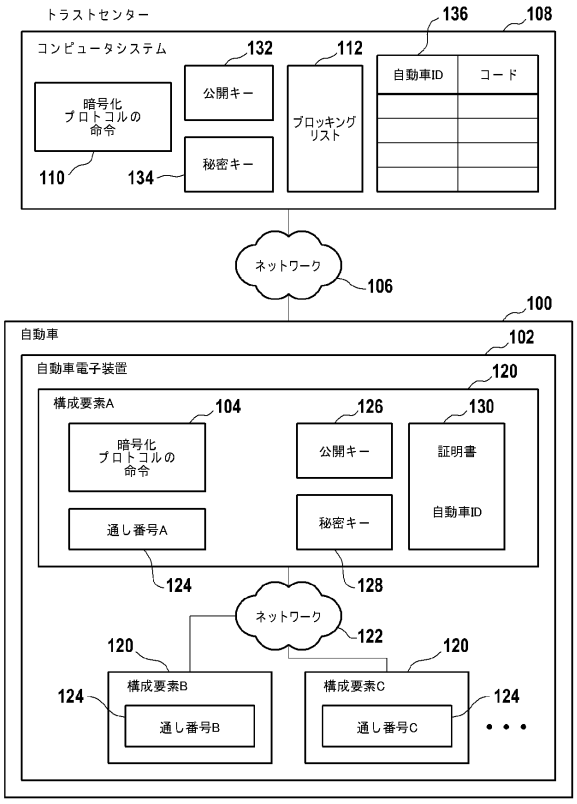
【図２】



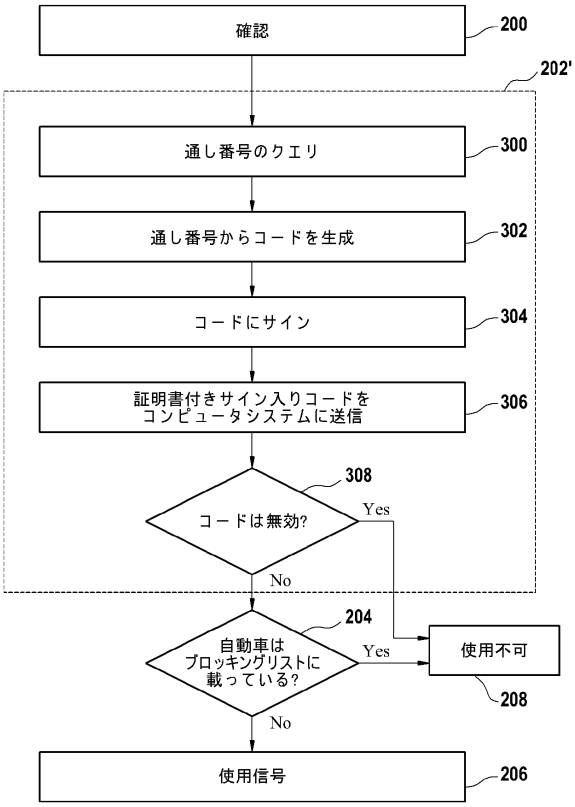
【図３】


トラストセンター
108
コンピュータシステム
132
112
110
暗号化
プロトコルの
命令
公開キー
ブロッキング
リスト
秘密キー
134
ネットワーク
106
100
自動車
102
自動車電子装置
120
構成要素A
104
126
130
暗号化
プロトコルの
命令
公開キー
証明書
通し番号A
秘密キー
コード
124
128
ネットワーク
122
120
120
構成要素B
構成要素C
124
通し番号B
通し番号C
124
・・・

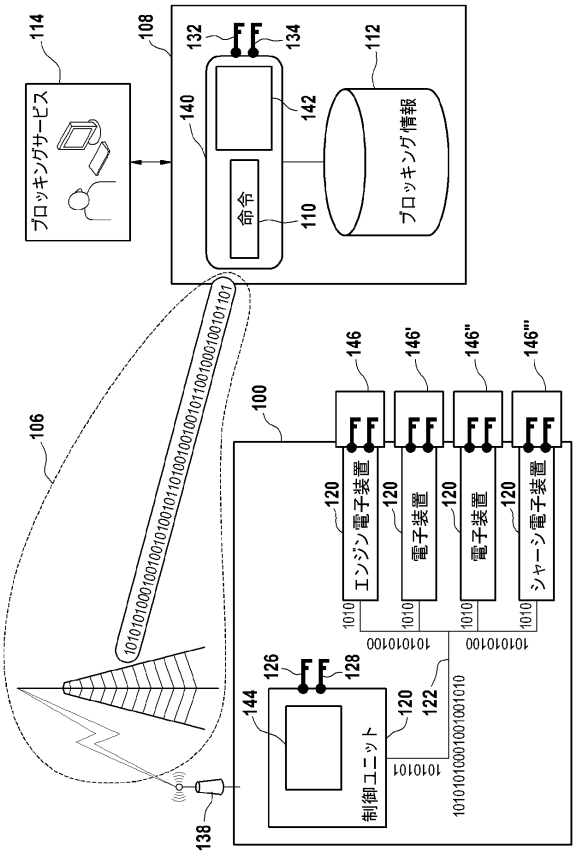
【図４】


トラストセンター
136
108
コンピュータシステム
132
112
自動車ID
コード
暗号化
プロトコルの
命令
公開キー
ブロッキング
リスト
110
134
秘密キー
ネットワーク
106
100
自動車
102
自動車電子装置
120
構成要素A
104
126
130
暗号化
プロトコルの
命令
公開キー
証明書
通し番号A
秘密キー
自動車ID
124
128
ネットワーク
122
120
120
構成要素B
構成要素C
124
通し番号B
通し番号C
124
・・・

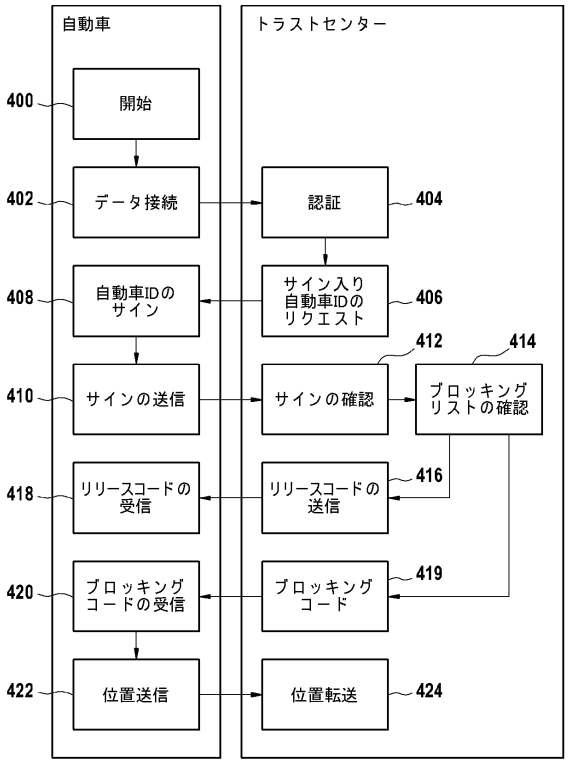
【図５】


確認
200
202'
通し番号のクエリ
300
通し番号からコードを生成
302
コードにサイン
304
証明書付きサイン入りコードを
コンピュータシステムに送信
306
308
コードは無効?
Yes
No
204
自動車は
ブロッキングリストに
載っている?
Yes
使用不可
208
No
使用信号
206

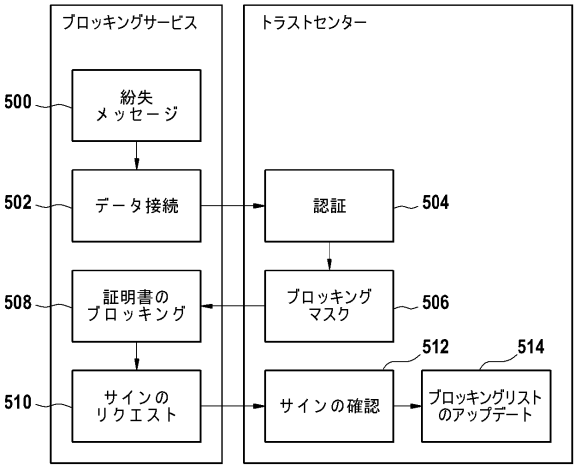
【図６】


114
108
132
134
112
ブロッキングサービス
140
142
ブロッキング情報
命令
110
106
100
146
146'
146"
146'''
120
エンジン電子装置
電子装置
電子装置
シャーシ電子装置
126
128
144
122
制御ユニット
138

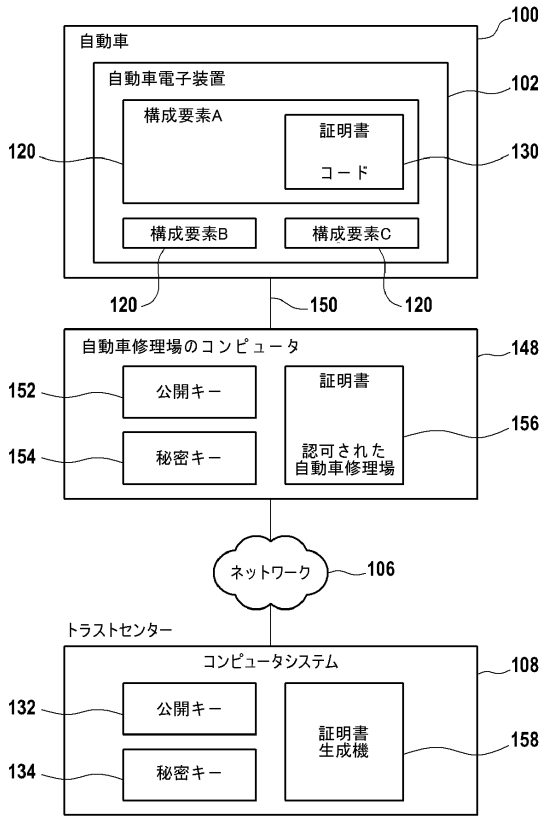
【図７】


自動車
トラストセンター
400
開始
402
データ接続
404
認証
408
自動車IDの
サイン
406
サイン入り
自動車IDの
リクエスト
412
414
410
サインの送信
サインの確認
ブロッキング
リストの確認
418
リリースコードの
受信
416
リリースコードの
送信
420
ブロッキング
コードの受信
419
ブロッキング
コード
422
位置送信
位置転送
424

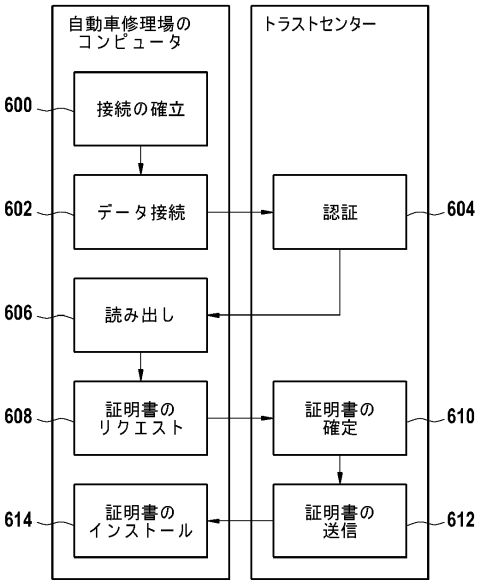
【図８】


ブロッキングサービス
トラストセンター
500
紛失
メッセージ
502
データ接続
504
認証
508
証明書の
ブロッキング
506
ブロッキング
マスク
512
514
510
サインの
リクエスト
サインの確認
ブロッキングリスト
のアップデート

【図９】


100
自動車
自動車電子装置
102
構成要素A
120
証明書
コード
130
構成要素B
構成要素C
120
150
120
自動車修理場のコンピュータ
148
152
公開キー
証明書
154
秘密キー
認可された
自動車修理場
156
ネットワーク
106
トラストセンター
コンピュータシステム
108
132
公開キー
証明書
生成機
134
秘密キー
158

【図１０】


自動車修理場の
コンピュータ
トラストセンター
600
接続の確立
602
データ接続
604
認証
606
読み出し
608
証明書の
リクエスト
610
証明書の
確定
614
証明書の
インストール
証明書の
送信
612

フロントページの続き

(74)代理人 100156591
弁理士 高田 学
(72)発明者 ジスカ、アンドリアス
ドイツ連邦共和国、１２１０７ ベルリン、イーエム レザハタール ４２
(72)発明者 ムフェルマン、ガンダ
ドイツ連邦共和国、１５５６６ シェーンアイヒェ、ヘウヴェク ４３
(72)発明者 クター、ジョアキム
ドイツ連邦共和国、１０１７９ ベルリン、アーエム カローゲル ３
(72)発明者 ボートフェルトーヘーアケンデル、シャーリー
ドイツ連邦共和国、１０１１７ ベルリン、ライプチガー シュトラッセ ６６

審査官 石田 信行

(56)参考文献 特開２００３－１４６１８５（ＪＰ，Ａ）
特開平０８－２６８２３１（ＪＰ，Ａ）
特開２００３－１６５４１７（ＪＰ，Ａ）
特開２００３－２５８７９４（ＪＰ，Ａ）
特開２００５－０５７５７１（ＪＰ，Ａ）
特開２００７－１０２４４１（ＪＰ，Ａ）
特開２００７－０１２０４６（ＪＰ，Ａ）
特開２００６－２９３５９４（ＪＰ，Ａ）
特開２００５－２２５４２２（ＪＰ，Ａ）
特開２００５－０９７８３５（ＪＰ，Ａ）
特開２００５－００１５０４（ＪＰ，Ａ）
特開２００５－００１５３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32
G09C 1/00
B60R 25/04
B60R 25/10
G06F 21/20
G06F 1/00