(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2009-503967
(P2009-503967A)
(43)公表日　平成21年1月29日(2009.1.29)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5B285
G06F 21/20	(2006.01)	H04L	9/00	675D	5J104
H04L 9/10	(2006.01)	G06F	15/00	330C	
		H04L	9/00	621A	

審査請求 未請求　予備審査請求 未請求　（全 21 頁）

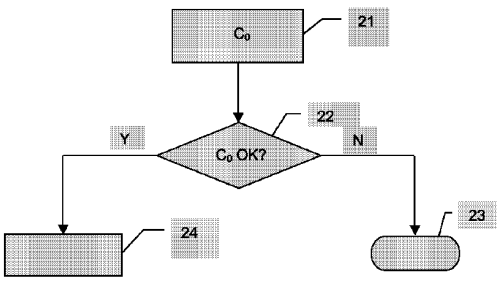
(21)出願番号　特願2008-523317 (P2008-523317)
(86)(22)出願日　平成18年7月18日 (2006.7.18)
(85)翻訳文提出日　平成20年3月28日 (2008.3.28)
(86)国際出願番号　PCT/EP2006/064383
(87)国際公開番号　WO2007/012583
(87)国際公開日　平成19年2月1日 (2007.2.1)
(31)優先権主張番号　0507990
(32)優先日　平成17年7月26日 (2005.7.26)
(33)優先権主張国　フランス(FR)

(71)出願人　591034154
フランス　テレコム
フランス国　パリ　７５０１５　プラス　ダルレ　６
(74)代理人　100099623
弁理士　奥山　尚一
(74)代理人　100096769
弁理士　有原　幸一
(74)代理人　100107319
弁理士　松島　鉄男
(74)代理人　100114591
弁理士　河村　英文
(74)代理人　100118407
弁理士　吉田　尚美

最終頁に続く

(54)【発明の名称】単一の物理デバイスを用いた保護されたトランザクションの制御方法、それに対応する物理デバイス、システム及びコンピュータプログラム

(57)【要約】
本発明は、ユーザの物理デバイス（１３）であって、デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも１対の非対称鍵を有する物理デバイス（１３）を用いる保護されたトランザクションの制御方法に関する。本方法は、物理デバイスの使用開始前に、特定の認証機関（１０）の第１の認証鍵（S_T）を用いて前記デバイス公開鍵（P_0）を認証し、前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることを確かめてから、デバイス証明書（C_0）を発行するステップと、第１の認証鍵（S_T）に対応する第２の認証鍵（P_T）を用いて前記デバイス証明書（C_0）を確認するステップと、確認結果が正常である場合に、前記ユーザをあるプロバイダに登録（２４）するステップとを含む。



【特許請求の範囲】
【請求項１】
あるユーザ（３０）の物理デバイス（１３）であって、デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも一対の非対称鍵を有する物理デバイス（１３）を用いる、保護されたトランザクションの制御方法であって、
前記物理デバイスの使用開始前に、前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることを確かめてから、デバイス証明書（C_0）を発行する特定の認証機関（ＡＣＰ、１０）が第１の認証鍵（S_T）を用いて署名することにより、前記デバイス公開鍵（P_0）を認証（２１）するステップと、
前記第１の認証鍵（S_T）に対応する第２の認証鍵（P_T）を用いて前記デバイス証明書（C_0）を確認するステップ（２２）と、
確認結果が正常である場合に、前記ユーザ（３０）をあるプロバイダ（３３）に登録（２４）するステップであって、前記デバイス公開鍵（P_0）と前記ユーザ（３０）の識別子（Id_i）とについての前記プロバイダ（３３）による署名に対応しているプロバイダ証明書（C_i）を発行する、登録（２４）するステップと
を含む制御方法。
【請求項２】
前記認証機関（１０）は前記物理デバイス（１３）の製造者である、請求項１に記載の制御方法。
【請求項３】
前記デバイス証明書（C_0）は、前記物理デバイス（１３）内の自由に読み取り可能なメモリ領域（１３１）に保存されるものである、請求項１又は２に記載の制御方法。
【請求項４】
前記デバイス証明書（C_0）は、前記物理デバイスを表す少なくとも１つの情報をさらに署名するものである、請求項１～３のいずれか一項に記載の制御方法。
【請求項５】
前記物理デバイスを表す前記情報は、
該物理デバイスのタイプと、
該物理デバイスの製造者の識別と、
該物理デバイスが用いる暗号化アルゴリズムのタイプと、
該物理デバイスのシリアル番号と
を含むものである、請求項４に記載の制御方法。
【請求項６】
前記確認するステップ（２２）は、前記プロバイダ（３３）により実行されるものである、請求項１～５のいずれか一項に記載の制御方法。
【請求項７】
前記第１の認証鍵（S_T）は秘密鍵であり、
前記第２の認証鍵（P_T）は公開鍵である、請求項１～６のいずれか一項に記載の制御方法。
【請求項８】
前記認証機関（１０）はある対称鍵（Ｋ）を使用するものであり、
その結果、前記第１の認証鍵（S_T）と前記第２の認証鍵（P_T）とは同一のものとなる、請求項１～６のいずれか一項に記載の制御方法。
【請求項９】
前記認証するステップは、前記物理デバイスの製造者からの要求を受けて前記認証機関が前記対称鍵に基づいて実行するものであり、
前記確認するステップは、前記プロバイダからの要求を受けて前記認証機関が実行するものである、請求項８に記載の制御方法。
【請求項１０】
保護されたトランザクションにおいて使用されるように設計された、あるユーザの物理

デバイスであって、
デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも１つの第１の非対称鍵の対と、
前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることが確かめられた後に、ある特定の認証機関の第１の認証鍵（S_T）による前記第１のデバイス公開鍵（P_0）の署名に対応して発行されるデバイス証明書（C_0）と
を有し、
前記デバイス証明書（C_0）は、前記物理デバイスが使用開始される前に該物理デバイスに保存されるものである、物理デバイス。
【請求項１１】
ある通信ネットワークからダウンロード可能であり、及び／又はコンピュータにより読み取り可能な媒体に保存され、及び／又はマイクロプロセッサにより実行可能なコンピュータプログラム製品であって、
請求項１～９のいずれか一項に記載の保護されたトランザクションの制御方法の少なくとも１つのステップを実行するプログラムコード命令を含むコンピュータプログラム製品。
【請求項１２】
あるユーザ（３０）の物理デバイス（１３）であって、デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも一対の非対称鍵を有する物理デバイス（１３）を用いた、通信ネットワーク（３２）における保護されたトランザクションを制御するシステムであって、
前記通信ネットワークへ接続された特定の認証サーバ（３５）であって、前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることを確かめてから、前記物理デバイスの使用開始前に、前記認証サーバ（３５）の第１の認証鍵（S_T）による前記デバイス公開鍵（P_0）の署名に対応したデバイス証明書（C_0）を前記物理デバイスに対して発行する認証サーバ（３５）と、
前記第１の認証鍵（S_T）に対応する第２の認証鍵（P_T）を用いて前記デバイス証明書（C_0）を確認する確認サーバ（３４）であって、前記通信ネットワークに接続された確認サーバ（３４）と、
前記確認サーバによる確認の結果が正常である場合に、前記デバイス公開鍵（P_0）と前記ユーザの識別子（Id_i）とについてのあるプロバイダによる署名に対応しているプロバイダ証明書（C_i）を前記ユーザ（３０）へ発行する前記プロバイダに対して前記ユーザ（３０）を登録する登録サーバ（３３）であって、前記通信ネットワークに接続された登録サーバ（３３）と
を少なくとも備えるシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
１．発明の分野
本発明は、インターネットなどの通信ネットワークを用いて、特に認証、電子署名及び決済処理を実行する電子商取引の保護の分野に関する。
【０００２】
より具体的には、本発明は、あるユーザが所有する物理デバイスを用いた保護されたトランザクションを制御する技術に関する。
【背景技術】
【０００３】
２．従来技術
インターネットなどの通信ネットワークの著しい成長とこれらのネットワーク上で行われる日々のトランザクション数の絶え間ない増加により、トランザクションの保護に対する要求が絶え間なく増加している。実際には、従来の郵便又は直接的な接触による物理的

なやりとりを巡る信頼環境が、これらの情報技術又は無線通信ネットワークにおいても引き継がれることが必要であると見られている。

【０００４】

従来技術では、コンピュータネットワークで用いられる公開暗号鍵の有効性を確かめるために証明書が特に用いられている。この証明書は、少なくとも公開鍵と、その所有者の識別子と、有効期間と、認証機関の特定と、この証明書を発行した認証機関の秘密鍵を用いて得られるこれらの異なるデータの暗号化署名とを含むメッセージである。

【０００５】

証明書を読み取ることにより、署名について受信したメッセージと認証について自己を認証するエンティティの識別子との送り手を確実に認証することが可能となる。

【０００６】

証明書のさらなる詳細については、特にＩＥＴＦ（Internet Engineering Task Force: インターネット技術タスクフォース）が公開したＲＦＣ３２８０（Request For Comment No. 3280）において定義されているＸ．５０９規格、より具体的にはＸ．５０９ｖ３を参照されたい。

【０００７】

上述した従来技術の１つの欠点は、プロバイダが発行した証明書C_iが所与の物理デバイスに記憶された秘密鍵S_0に対応する公開鍵P_0を真に認証するものであるかを、プロバイダが容易に、かつリモートで確かめることができないということである。

【０００８】

実際には、物理デバイスの動作をソフトウェアプログラムにより完全にシミュレーションすることで、物理デバイス又はそのようなデバイスのソフトウェアエミュレーションに対応するかをプロバイダがリモートで認識できないものとなる。

【０００９】

ここで、プロバイダにとって真正な物理デバイスと通信していることを認証するのが重要となるいくつかの状況がある。

【００１０】

実際には、物理デバイスの秘密鍵S_0がよいやり方に基づいて秘密かつアクセス不可の領域に保存されていれば、物理デバイスは複製できず、したがって、物理デバイスは、公開鍵P_0と、それゆえ証明書C_iと、それゆえ顧客を第ｉ番目のプロバイダへ知らせるための識別子Id_iとに対応する認証コード（authenticator）と署名とを単独で生成できるユニークなオブジェクトである。物理デバイスのプロセッサのみが、第ｉ番目のプロバイダについての識別子Id_iを用いて自己の認証又は署名を行うことができる。これにより、強力な否認防止（non-repudiation）の特性及びプロバイダにとってのセキュリティが得られる。

【００１１】

プロバイダが所与の物理デバイスを相手にしていると確認できることが重要であるもう一つの状況は、この物理デバイスが、プロバイダの提供するサービス（例えば、日刊紙上に掲載された新聞記事へのインターネットを通してのアクセス）へ有料で加入するための媒体であるときである。有料サービスへのアクセスは、ユーザにとって、プロバイダとのセッションの開始中にユーザが自己の物理デバイスを用いて自己を認証することが条件となる。

【００１２】

従ってプロバイダにとっては、数人がたった１度の加入に対して支払うだけでサービスに（同時に又は別の時に）アクセスすることができないようにするために、サービスへのアクセスを望む顧客が本当に物理デバイスを所有しているかを確認することが特に重要である。これは、加入媒体の複製ができる場合（例えば、加入媒体がハードディスクドライブに保存された「識別子とパスワード」の組合せ又は秘密鍵（暗号化されていても）である場合）にあたる。

【００１３】

本願の出願人のために出願された特許文献１は、デバイスのユーザがトランザクションを実行することを望む１以上のプロバイダとの間で認証を実行するのに用いられるこの種の物理デバイスをより詳細に開示している。

【００１４】

この方法において、一の秘密鍵S_0と一の公開鍵P_0とを含む１対の非対称鍵（P_0，S_0）へ従来のやり方で関連付けられたチップカードやＵＳＢ（ユニバーサルシリアルバス）ドングルのような物理デバイスがユーザに与えられる。秘密鍵S_0は秘密に保たれなくてはならない電子的要素であり、したがって物理デバイスの保護された領域に保存され、いかなる侵入の試みからも守られる。公開鍵P_0は自由に読み取られる状態で物理デバイスに保存されるか、又はフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ、紙の書類又はデータサーバの予約領域のような外部の媒体を通してユーザへ提供することができる。この鍵の対（S_0，P_0）は、デバイスの流通及び使用開始（commissioning）に先立って、工場で生成される。

【００１５】

また、この種の物理デバイスは、従来から、認証及び／又は署名についての非対称暗号化アルゴリズムを実行する計算手段を有している。これらのアルゴリズムのうち、例えばＲＳＡ（Rivest-Shamir-Adleman）、ＤＳＡ、ＧＱ（Guillou-Quisquater）又はＧＰＳ型のアルゴリズムが挙げられる。

【００１６】

この非対称暗号化アルゴリズムの使用は、物理デバイスを個人が所有する以前の段階で初期化されて本願の課題ではない従来の手法により管理されるキャリアコード（又はＰＩＮ（personal identification number）コード）の事前の提示に基づくことができる。

【００１７】

物理デバイスは、このようにして、いかなるプロバイダからも独立した頒布手段を用いてユーザに販売される。

【００１８】

プロバイダとの保護されたトランザクション（認証、署名）の実行を可能にするため、顧客とも呼ばれる物理デバイスのユーザは、デバイスの公開鍵P_0とプロバイダに関連する識別子Id_1とをリンクする証明書C_1についてプロバイダから発行を受けなければならない（注：プロバイダに対してユーザの匿名性を維持しなければならないシステムでは、識別子Id_1はユーザの民生的な識別（civil identity）とは異なる）。

【００１９】

一般に「登録」と呼ばれるこの処理がｎ個の個別のプロバイダとの間で実行され、（それぞれが所与のプロバイダに関連する）ｎ個の識別子｛Id_1、Id_2、…、Id_n｝を同じ公開鍵P_0へリンクするｎ個の証明書｛C_1、C_2、…、C_n｝が顧客へ割り当てられる。

【００２０】

その後、顧客が第ｉ番目のプロバイダとの保護されたトランザクションの実行を望む場合、顧客は自己の秘密鍵S_iを用いて、認証機関が標準化されたプロトコルに基づいて付与した対応する証明書C_iをS_iに関連付けて、自己の物理デバイスを用いてプロバイダから送られたランダム値（この場合は認証）又はメッセージ（この場合は電子署名）に対して署名する。

【００２１】

３．従来技術の欠点

従来技術によれば、進行中のトランザクションが所与の物理デバイスを用いて実際に行われることをプロバイダが確かめることのできる唯一の方法は、プロバイダによるデバイスの物理的な取扱いに依存する。実際には、公開鍵P_0がデバイス内に保存されていれば、デバイス内の公開鍵P_0を読み取ることができる。そうでない場合、デバイスに対して秘密鍵S_0を用いてランダム値を署名し、顧客により外部媒体上に与えられた公開鍵P_0を用いてこの署名の結果を確認することができる。

【００２２】

しかし、この従来技術のアプローチの欠点は、デバイス上で物理的に処理することができるプロバイダを必要とし、したがっていかなる遠隔操作も排除されてしまうことである。この点は、インターネットのような現在の通信ネットワークにおいてトランザクションを実行する場合に問題となり得る。

【特許文献１】仏国特許出願第FR 96 08692号「Procede de controle de transactions securisees independantes utilisant un dispositif physique unique（単一の物理デバイスを用いた独立かつ保護されたトランザクションの制御方法）」

【発明の開示】

【発明が解決しようとする課題】

【００２３】

４．本発明の目的

本発明は、特に従来技術の欠点を克服することを目的とする。

【００２４】

より具体的には、一対の非対称鍵（P_0、S_0）に関連付けられると共に、必要ならば遠隔から所与の物理デバイスによるトランザクションの実行を確実にするために用いられる物理デバイスを実現する、保護されたトランザクションの制御技術を提供することが本発明の一つの目的である。

【００２５】

言い換えれば、プロバイダが認証しなければならない公開鍵P_0が所与の物理デバイスに保存された秘密鍵S_0と真に対応することをプロバイダが確認できるこの種の技術を提案することが本発明の一つの目的である。

【００２６】

実現が容易で、使用される物理デバイスにさらなる複雑度をほとんどまたは全く導入しないこの種の技術を提案することが本発明の別の目的である。

【００２７】

プロバイダにとって信用できる環境を作るため、信頼でき、かつ強力な否認防止の特性を得るために用いることができるこの種の技術を提供することが本発明のさらなる目的である。

【課題を解決するための手段】

【００２８】

これらの目的及び以下に述べる他の目的は、デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも一対の非対称鍵を有する、ユーザの物理デバイスを実現する保護されたトランザクションの制御方法を用いて達成される。

【００２９】

本発明によれば、この制御方法は、

前記物理デバイスの使用開始（commissioning）前に、前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることを確かめてから、デバイス証明書（C_0）を発行する特定の認証機関（ＡＣＰ）が第１の認証鍵（S_T）を用いて署名することにより、前記デバイス公開鍵（P_0）を認証するステップと、

前記第１の認証鍵（S_T）に対応する第２の認証鍵（P_T）を用いて前記デバイス証明書（C_0）を確認するステップと、

確認結果が正常である場合に、ユーザをあるプロバイダに登録するステップであって、前記デバイス公開鍵（P_0）とユーザの識別子（Id_i）とについての前記プロバイダによる署名に対応しているプロバイダ証明書（C_i）を発行する、登録するステップと

を含む。

【００３０】

このように、本発明は、電子的トランザクションを保護するための全体として新規かつ進歩性のあるアプローチに基づいている。実際には、保護の程度を高めるために本発明の手法は、様々なプロバイダが信用を置く特定の認証機関（ＡＣＰ）を用いる。この特定の認証機関は、物理デバイス（ＵＳＢドングル、チップカードなど）の使用開始前に、物理

デバイスに関係する証明書（従来のようなデバイスの所有者の識別子に関係する証明書ではない）を発行する。そして、その有効性を確認することにより、たとえリモートであっても、不正にその動作を模倣する装置（コンピュータ、ＰＤＡなど）ではなく真正な物理デバイスであるということの保証をプロバイダに与える。

【００３１】

この保護は、特定の認証機関が、所与の物理デバイスに保存された秘密鍵S_0に対応する公開鍵P_0の場合を除いて、第１の認証鍵S_Tからこのようなデバイス証明書C_0を生成しないという強い制約に依拠している。

【００３２】

デバイス証明書の確認は、特定の認証機関がプロバイダへ伝達する特定の認証機関の第２の認証鍵に基づいてプロバイダが直接行うか、又は信頼された第三者が行うことができる。このようにして、本発明のトランザクションの制御方法は、保護されたトランザクションへの参加を望む顧客がＡＣＰにより認証された物理デバイスを真に所有していることについて、ＡＣＰがプロバイダに対し保証するということを利用するものである。このようにして、ユーザが物理デバイスを所有することについてリモートで何も保証しない従来技術とは、明らかに相違する。実際には、従来の制御技術は、必要があれば一連の認証機関の使用に基づく認証と証明の連鎖によりユーザの識別を保証するだけで、常にユーザのアイデンティティの認証という一つの結果を得るだけである。本発明の方法は、ユーザのアイデンティティの認証に加えて、このユーザがその後所有することになる物理デバイスの事前の認証を行う。このようにして、プロバイダとの間で自己の真正を認証するユーザが物理デバイスを所有することを、リモートであってもプロバイダに対して保証することを可能にする。この保証のみが、トランザクション制御プロセスの確立を継続させることができる。

【００３３】

デバイス証明書C_0の有効性が保証されると、プロバイダは従来のやり方でプロバイダ証明書C_iの発行先であるユーザの登録へ進むことができる。

【００３４】

前記特定の認証機関は前記物理デバイスの製造者であることが好ましく、そうすればデバイスが製造ラインを離れる時に直接的にデバイス証明書C_0を発行することができる。特定の認証機関は、１つ以上の別個の製造者が利用する第三者的な認証機関とすることもできる。

【００３５】

有利なことに、前記デバイス証明書（C_0）は、前記物理デバイス内の自由に読み取り可能な記憶領域に保存される。そうすることでプロバイダが容易に読み取ることができる。

【００３６】

本発明の有利な特徴によれば、前記デバイス証明書（C_0）は、

物理デバイスのタイプと、

該物理デバイスの製造者の識別と、

該物理デバイスが用いる暗号化アルゴリズムのタイプと、

該物理デバイスのシリアル番号と

を含む、前記物理デバイスを表す情報の少なくとも一部を署名する。

【００３７】

デバイス証明書C_0の確認段階で、このようにしてプロバイダは相手先の物理デバイスについて利用可能な付加的情報を得て、例えば想定されるトランザクションの性質にデバイスのタイプが適合するか確認したり、シリアル番号に基づいてデバイスのトレーサビリティを保証したりすることができる。

【００３８】

本発明の代替的で有利な実施形態においては、プロバイダが前記確認のステップを実行する。そうすると、プロバイダは第三者たる確認機関のサービスを求める必要がなく、直

接的にユーザを登録できるかできないかがわかる（この点は本発明のコンテキストにおいても想定できる）。

【００３９】

第１の有利な実施形態においては、前記第１の認証鍵（S_T）は秘密鍵であり、前記第２の認証鍵（P_T）は公開鍵である。このようにして一対の非対称鍵が使用され、秘密鍵（S_T）は、プロバイダに伝達されるか又は公開される公開鍵とは異なり、特定の認証機関によって秘密に保たれる。

【００４０】

第２の有利な実施形態においては、前記特定の認証機関はある対称鍵（Ｋ）を使用する。その結果、前記第１の認証鍵（S_T）と前記第２の認証鍵（P_T）とは同一のものとなる。

【００４１】

この場合、前記認証のステップは、前記デバイスの製造者からの要求を受けて前記特定の認証機関が前記対称鍵に基づいて実行する。そして、前記確認のステップは前記プロバイダからの要求を受けて前記特定の認証機関が実行する。

【００４２】

この場合もやはり、特定の認証機関はむろん製造者そのものとすることができる。

【００４３】

本発明はまた、ユーザの物理デバイスであって、保護されたトランザクションにおいて用いられるよう設計された物理デバイスに関する。この物理デバイスは、デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも一対の第１の非対称鍵を有する。

【００４４】

本発明によれば、このデバイスはまた、前記物理デバイス（１３）内の耐タンパ領域に前記デバイス秘密鍵S_0が保存されていることが確かめられた後に、特定の認証機関の第１の認証鍵S_Tによる前記第１のデバイス公開鍵P_0の署名に対応して発行されるデバイス証明書C_0を有する。ここで、前記デバイス証明書（C_0）は、前記物理デバイスの使用開始の前に該物理デバイスに保存される。

【００４５】

本発明はまた、通信ネットワークからダウンロード可能であり、及び／又はコンピュータにより読み取り可能な媒体に保存され、及び／又はマイクロプロセッサにより実行可能なコンピュータプログラム製品に関する。このコンピュータプログラム製品は、上述したように保護されたトランザクションの制御方法の少なくとも１つのステップを実行するプログラムコード命令を含む。

【００４６】

本発明はまた、ユーザの物理デバイスであって、デバイス公開鍵P_0と、対応するデバイス秘密鍵S_0とを含む少なくとも一対の非対称鍵を有する物理デバイスを用いた、通信ネットワークにおける保護されたトランザクションを制御するシステムであって、

前記ネットワークに接続された特定の認証サーバであって、前記デバイス秘密鍵S_0が前記物理デバイス（１３）内の耐タンパ領域に保存されていることを確かめてから、前記物理デバイスの使用開始の前に、前記認証サーバの第１の認証鍵S_Tによる前記デバイス公開鍵P_0の署名に対応したデバイス証明書C_0を前記物理デバイスに対して発行する特定の認証サーバと、

前記第１の認証鍵S_Tに対応する第２の認証鍵P_Tを用いて前記デバイス証明書C_0を確認する確認サーバであって、前記ネットワークに接続されている確認サーバと、

前記確認サーバによる確認の結果が正常である場合に、前記デバイス公開鍵（P_0）と前記ユーザの識別子（Id_i）とについてのあるプロバイダによる署名に対応しているプロバイダ証明書（C_i）を前記ユーザへ発行する前記プロバイダに対して前記ユーザを登録する登録サーバであって、前記通信ネットワークに接続された登録サーバと

を備えるシステムに関する。

【００４７】
６．図面のリスト
本発明の他の特徴及び利点は、簡潔かつ非限定的な説明を通じた以下の好ましい実施形態の説明、及び添付図面からより明確なものとなる。
【発明を実施するための最良の形態】
【００４８】
７．本発明の一実施形態の説明
本発明の一般的な原理は、保護されたトランザクション（リモートトランザクションの場合あり）の間に、公開鍵P_0に関連付けられた対応する秘密鍵S_0を保存した真正な物理デバイスをプロバイダが真に相手にしていることをプロバイダに対して保証することができる、物理デバイスの使用開始前に特定の認証機関により行われる物理デバイスの公開鍵P_0の認証に基づいている。
【００４９】
図１を参照して、所与の物理デバイス１３の使用開始前に行われる該物理デバイス１３の公開鍵P_0の認証の一実施形態について説明する。
【００５０】
特定の認証機関、すなわちＡＣＰ１０は、公開鍵P_Tと、秘密かつアクセス不可の領域１０１に保存された秘密鍵S_Tとを含む一対の非対称鍵（P_T，S_T）を有している。この種のＡＣＰ１０は例えば物理デバイスの製造者である。その場合に秘密鍵S_Tが記憶される秘密領域１０１は、製造者が有する特定の物理デバイス（例えばチップカード）又は製造者のコンピュータ設備のアクセス制限された保護メモリ領域である。
【００５１】
公開鍵P_Tは、ＡＣＰ１０により公開されるか、又はそれを必要とする可能性のあるプロバイダ（すなわち、物理デバイス１３の所有者とのトランザクションを担当するプロバイダ）のうちの１つの要求により提供される。
【００５２】
物理デバイス１３の製造段階で一対の非対称鍵（P_0，S_0）が記録される。この非対称鍵の対（P_0，S_0）は、デバイス１３内の読み取り可能領域１３１に保存された公開鍵P_0と、このデバイス１３の保護領域１３２に保存された秘密鍵S_0とを含んでいる。この保護された領域、すなわち耐タンパ領域１３２は、秘密鍵S_0の読み取りを防ぎ、ソフトウェア又はハードウェアのいかなる侵入の試みにも耐えられるように作られている。１つの変更例として、デバイスそのものによらない外部の補助を得て物理デバイス１３の所有者に公開鍵P_0を伝えることもできる。
【００５３】
ＡＣＰ１０が物理デバイス１３の製造者であれば、図１に示された処理は、物理デバイス１３の流通の前に、個人がデバイスを所有する（前の）段階で工場において実行される。あるいは製造者とは独立した認証機関であれば、これらの処理は、物理デバイスが製造ラインを離れる時に、エンドユーザに流通する前に実行することができる。
【００５４】
より具体的には、物理デバイス１３はデバイス公開鍵P_0をＡＣＰ１０へ伝達１１する。すると、ＡＣＰ１０は秘密鍵S_Tを用いて、デバイス１３の公開鍵P_0を署名する。この署名１２により、デバイスの公開鍵P_0のように物理デバイス１３内の自由に読み取り可能な領域１３１に書き込まれるか、又は外部の媒体（フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ、紙の書類など）を通してユーザに与えられる識別証明書$C_0 = A(S_T, P_0)$が得られる（ここでＡは例えばＲＳＡ型の暗号化署名アルゴリズムである）。
【００５５】
ＡＣＰ１０（製造者又は信頼された第三者）は、所与のタイプの物理デバイスに保存された秘密鍵に対応する公開鍵P_0を除いて、このようなデバイス証明書C_0（すなわち、秘密鍵S_Tを用いたこのような署名）を通常は生成しない。
【００５６】

また、図１の認証処理は、本発明の代替的な一実施形態において、異なるタイプの物理デバイスのいくつかの製造者に対して相互的に行ってもよい。この場合、ＡＣＰ１０は信頼された第三者であってどの製造者からも独立しており、秘密鍵S_Tを有している。そして、所与の物理デバイス１３のデバイス証明書C_0を生成するために、秘密鍵S_Tを用いて（P_0，＜デバイスタイプ＞）の対を署名する。このような＜デバイスタイプ＞の情報は、例えばデバイス１３の種類、つまりそれがＵＳＢドングル、チップカードなどであるかについての情報を得ることを可能にする。または、製造者が製造したデバイスの一つを指定するのに用いる製品番号（product reference）とすることもできる。

【００５７】

同様に、変更例として、例えば製造者名（＜製造者名＞）、用いられる暗号化アルゴリズムのタイプ（＜アルゴリズムタイプ＞）、デバイスのシリアル番号などの、物理デバイス１３の使用に関連する他の情報をデバイス証明書C_0に署名することもできる。

【００５８】

このようにして、プロバイダによりデバイス証明書C_0を確認する後続の段階において（図２及び図３を参照して以下でより詳細に述べる）、このプロバイダは、公開鍵P_0が、＜製造者名＞によって製造された＜デバイスタイプ＞のタイプのデバイス１３に保存された秘密鍵S_0に対応するという保証を得る。この保証は、プロバイダが特定の認証機関１０に付与した信用から生まれるものである。

【００５９】

図１に示した処理の変更例として、$P_T = S_T = K$を対称鍵とすることが考えられる。

【００６０】

この場合に鍵Ｋは、物理デバイス１３の製造者と、この鍵Ｋを秘密に保つ者として製造者が知っている一つの（又は稀にいくつかの）信頼された第三者との間で共有することができる。この場合、第三者又は製造者自身のみが証明書を確認することができる。

【００６１】

製造者から独立しているＡＣＰ１０であって、物理デバイス１３の製造者から要求されたときだけ対称鍵のデバイス証明書C_0に署名するＡＣＰ１０のみが、鍵Ｋを用いるという場合も想定することができる。同様に、このＡＣＰ１０が、関連付けられた物理デバイス１３とのトランザクション実行を望むプロバイダの要求に応じてデバイス証明書C_0を確認することができる唯一のエンティティであるとすることができる。この場合でも、このＡＣＰ１０はむろん製造者そのものとすることができる。

【００６２】

ＡＣＰ１０により証明書C_0が記録された物理デバイス１３は、いかなるプロバイダからも独立した、例えば大規模店舗又は認証を受けた小売店等の販路を通じて販売される。

【００６３】

次に図２と図３を参照して、物理デバイス１３の所有者３０とプロバイダ３３との間の保護されたトランザクションにおいてデバイス証明書C_0が用いられる方法を説明する。このようなプロバイダ３３は、例えばサービス（例えば気象ニュースサービスやジオロケーションサービスへのアクセス）のプロバイダ又は商品の販売者（例えばインターネット上のトレーダー）とすることができる。

【００６４】

物理デバイス１３は、通信ネットワーク３２、例えばインターネットとして知られたワールドワイドのネットワークを通じてプロバイダ３３により提案されるサービスにアクセスするために使用することを望むユーザ３０が入手したものである。この種の物理デバイス１３は、例えばユーザ３０がプロバイダ３３から受ける有料加入者サービス（例えばインターネット上で公開された毎日の星占いサービスへの加入）の媒体として用いられる。

【００６５】

ユーザ３０がプロバイダ３３のサービスへのアクセスを望む場合、通信端末３１（例えばコンピュータ）からリクエストを送信し、通信ネットワーク３２を通してプロバイダ３３へ伝達される。このリクエストには、公開鍵P_0と、ＡＣＰ１０により物理デバイス１

３（簡単のため図３には図示せず）に予め記録２１されたデバイス証明書C_0とが添付されている。

【００６６】

ユーザ３０のリクエストに同意する前に、プロバイダは、送られてきた公開鍵P_0が所与の物理デバイスに保存された秘密鍵S_0に本当に対応するものであることを確認しなければならない。この目的のため、プロバイダは特定の認証機関１０の公開鍵P_Tを用いて、リクエストと共に送られてきたデバイス証明書C_0の確認２２を実行する。

【００６７】

確認結果が異常（negative verification）の場合、すなわちデバイス証明書C_0がＡＣＰ１０の秘密認証鍵（certification key）S_Tによる物理デバイスの公開鍵P_0の署名（signing）に対応しない場合、プロバイダ３３はトランザクションを中止して、リクエストされた項目（article）又はサービスへのユーザ３０のアクセスを拒否することができる。

【００６８】

しかしながら、確認結果が正常（positive verification）の場合、プロバイダは、公開鍵P_0が所与の物理デバイス１３に保存された秘密鍵S_0に真に対応するということの確信を得て、したがって、関連する識別子（Id_i）を用いてこのユーザの登録２４を行った上でユーザ３０のリクエストを受け入れることができる。この目的のため、プロバイダ３３は、プロバイダ３３による公開鍵P_0と前記識別子（Id_i）との署名（signing）に対応させて、ユーザ３０に対しプロバイダ証明書C_iを発行する。このプロバイダ証明書C_iは、プロバイダ３３の登録サーバが接続された通信ネットワーク３２を通してユーザの通信端末３１へ送られる。

【００６９】

デバイス証明書C_0の確認２２は、プロバイダ３３自体によるか、又は同じくネットワーク３２に接続された確認専用サーバ３４によっても行うこともできる。この場合、プロバイダ３３はネットワーク３２を通してデバイス証明書C_0を確認サーバ３４へ送信する。物理デバイス１３のデバイス証明書C_0を生成したＡＣＰ１０の認証サーバ３５は、その公開鍵P_Tを確認サーバ３４へ伝達するか、又は既に伝達されている。その後、確認サーバ３４は、証明書C_0の信頼性を確認するために認証サーバ３５の公開鍵P_Tを用いた確認結果をプロバイダ３３へ送れば足り、そうすることによりプロバイダ３３はユーザ３０の登録２４を実行するか、あるいは終了２３へ進むべきかを認識する。

【００７０】

ユーザ３０のプロバイダへの登録２４がなされると、ユーザはプロバイダ３３との間で保護されたトランザクションの実行を開始することができる。そうするために、ユーザは物理デバイス１３を用いて、プロバイダから与えられたランダム値（この場合の用語は認証である）又はメッセージ（この場合の用語は署名である）を、デバイス秘密鍵S_iを用いて署名し、それに対して、本願の目的ではなくそれ故ここでは詳細に説明しない標準的なプロトコルに基づき、対応するプロバイダ証明書C_iを関連付ける。

【００７１】

次にユーザ３０は、プロバイダに関連すると考えられるユーザ３０のアイデンティティId_iへ物理デバイス１３の公開鍵P_0をリンクするための各プロバイダ証明書C_iを発行するいくつかの異なるプロバイダへ登録２４される。

【図面の簡単な説明】

【００７２】

【図１】物理デバイスの使用開始前に特定の認証機関によって行われる物理デバイスの公開鍵の認証の原理を示す説明図である。

【図２】保護されたトランザクションを制御する本発明に係る方法において実行される各ステップのブロック図である。

【図３】図２の方法における、通信ネットワークを通してユーザと本発明に係る各サーバとの間のそれぞれの送受信を示す説明図である。

【図１】

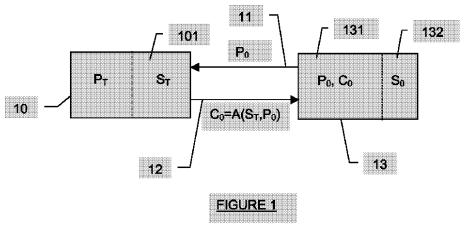


FIGURE 1

【図２】

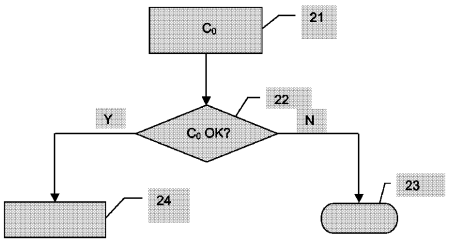


FIGURE 2

【図３】

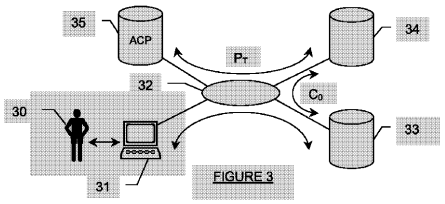


FIGURE 3

【手続補正書】
【提出日】平成20年3月31日(2008.3.31)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
あるユーザ（３０）の物理デバイス（１３）であって、デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも一対の非対称鍵を有する物理デバイス（１３）を用いる、保護されたトランザクションの制御方法であって、
前記物理デバイスの使用開始前に、前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることを確かめてから、デバイス証明書（C_0）を発行する特定の認証機関（ＡＣＰ、１０）が第１の認証鍵（S_T）を用いて署名することにより、前記デバイス公開鍵（P_0）を認証（２１）するステップと、
前記第１の認証鍵（S_T）に対応する第２の認証鍵（P_T）を用いて前記デバイス証明書（C_0）を確認するステップ（２２）と、
確認結果が正常である場合に、前記ユーザ（３０）をあるプロバイダ（３３）に登録（２４）するステップであって、前記デバイス公開鍵（P_0）と前記ユーザ（３０）の識別子（Id_i）とについての前記プロバイダ（３３）による署名に対応しているプロバイダ証明書（C_i）を発行する、登録（２４）するステップと
を含む制御方法。
【請求項２】
前記認証機関（１０）は前記物理デバイス（１３）の製造者である、請求項１に記載の

制御方法。
【請求項３】
前記デバイス証明書（C_0）は、前記物理デバイス（１３）内の自由に読み取り可能なメモリ領域（１３１）に保存されるものである、請求項１又は２に記載の制御方法。
【請求項４】
前記デバイス証明書（C_0）は、前記物理デバイスを表す少なくとも１つの情報をさらに署名するものである、請求項１～３のいずれか一項に記載の制御方法。
【請求項５】
前記物理デバイスを表す前記情報は、
該物理デバイスのタイプと、
該物理デバイスの製造者の識別と、
該物理デバイスが用いる暗号化アルゴリズムのタイプと、
該物理デバイスのシリアル番号と
を含むものである、請求項４に記載の制御方法。
【請求項６】
前記確認するステップ（２２）は、前記プロバイダ（３３）により実行されるものである、請求項１～５のいずれか一項に記載の制御方法。
【請求項７】
前記第１の認証鍵（S_T）は秘密鍵であり、
前記第２の認証鍵（P_T）は公開鍵である、請求項１～６のいずれか一項に記載の制御方法。
【請求項８】
前記認証機関（１０）はある対称鍵（Ｋ）を使用するものであり、
その結果、前記第１の認証鍵（S_T）と前記第２の認証鍵（P_T）とは同一のものとなる、請求項１～６のいずれか一項に記載の制御方法。
【請求項９】
前記認証するステップは、前記物理デバイスの製造者からの要求を受けて前記認証機関が前記対称鍵に基づいて実行するものであり、
前記確認するステップは、前記プロバイダからの要求を受けて前記認証機関が実行するものである、請求項８に記載の制御方法。
【請求項１０】
保護されたトランザクションにおいて使用されるように設計された、あるユーザの物理デバイスであって、
デバイス公開鍵（P_0）と、対応するデバイス秘密鍵（S_0）とを含む少なくとも１つの第１の非対称鍵の対を有し、
前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることが確かめられた後に、ある特定の認証機関の第１の認証鍵（S_T）による前記第１のデバイス公開鍵（P_0）の署名に対応して発行されるデバイス証明書（C_0）へ関連付けられ、
前記デバイス証明書（C_0）は、前記物理デバイスが使用開始される前に該物理デバイスに保存されるものであるか、又はある外部の媒体を通して前記物理デバイス（１３）の前記ユーザへ提供されるものである、物理デバイス。
【請求項１１】
ある通信ネットワークからダウンロード可能であり、及び／又はコンピュータにより読み取り可能な媒体に保存され、及び／又はマイクロプロセッサにより実行可能なコンピュータプログラムであって、
請求項１～９のいずれか一項に記載の保護されたトランザクションの制御方法の少なくとも１つのステップを実行するプログラムコード命令を含むコンピュータプログラム。
【請求項１２】
あるユーザ（３０）の物理デバイス（１３）であって、デバイス公開鍵（P_0）と、対

応するデバイス秘密鍵（S_0）とを含む少なくとも一対の非対称鍵を有する物理デバイス（１３）を用いた、通信ネットワーク（３２）における保護されたトランザクションを制御するシステムであって、

前記通信ネットワークへ接続された特定の認証サーバ（３５）であって、前記デバイス秘密鍵（S_0）が前記物理デバイス（１３）内の耐タンパ領域に保存されていることを確かめてから、前記物理デバイスの使用開始前に、前記認証サーバ（３５）の第１の認証鍵（S_T）による前記デバイス公開鍵（P_0）の署名に対応したデバイス証明書（C_0）を前記物理デバイスに対して発行する認証サーバ（３５）と、

前記第１の認証鍵（S_T）に対応する第２の認証鍵（P_T）を用いて前記デバイス証明書（C_0）を確認する確認サーバ（３４）であって、前記通信ネットワークに接続された確認サーバ（３４）と、

前記確認サーバによる確認の結果が正常である場合に、前記デバイス公開鍵（P_0）と前記ユーザの識別子（Id_i）とについてのあるプロバイダによる署名に対応しているプロバイダ証明書（C_i）を前記ユーザ（３０）へ発行する前記プロバイダに対して前記ユーザ（３０）を登録する登録サーバ（３３）であって、前記通信ネットワークに接続された登録サーバ（３３）と

を少なくとも備えるシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/064383

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32

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)
H04L G07F

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 practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC , XP002376605 page 491 page 547 - page 549 page 559 - page 560 page 572 - page 576	1-12
X	US 2003/097592 A1 (ADUSUMILLI KOTESHWERRAO) 22 May 2003 (2003-05-22) abstract paragraph [0035] - paragraph [0036]	1-12
A	US 5 903 721 A (SIXTUS ET AL) 11 May 1999 (1999-05-11) abstract figures 1,2 column 3, line 26 - column 5, line 31	1-12

-/—

[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 document 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
12 September 2006	19/09/2006

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	SAN MILLAN MAESO, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/064383

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01/16900 A (AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY,) 8 March 2001 (2001-03-08) abstract	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/064383

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003097592 A1	22-05-2003	CN 1575579 A	02-02-2005
		DE 10297362 T5	09-09-2004
		GB 2395877 A	02-06-2004
		HK 1062752 A1	07-10-2005
		US 2003081783 A1	01-05-2003
		WO 03036913 A2	01-05-2003
US 5903721 A	11-05-1999	AU 6549498 A	29-09-1998
		BR 9809045 A	22-01-2002
		CA 2283933 A1	17-09-1998
		DE 1008022 T1	25-01-2001
		EA 1825 B1	27-08-2001
		EP 1008022 A2	14-06-2000
		ES 2150892 T1	16-12-2000
		JP 2001518212 T	09-10-2001
		NO 994428 A	09-11-1999
		WO 9840809 A2	17-09-1998
WO 0116900 A	08-03-2001	AT 258328 T	15-02-2004
		AU 775976 B2	19-08-2004
		AU 7090700 A	26-03-2001
		AU 2004231226 A1	23-12-2004
		BR 0013822 A	23-07-2002
		CA 2382922 A1	08-03-2001
		CN 1376292 A	23-10-2002
		CZ 20020744 A3	18-02-2004
		DE 60007883 D1	26-02-2004
		DE 60007883 T2	14-10-2004
		DK 1212732 T3	07-06-2004
		EP 1212732 A2	12-06-2002
		ES 2215064 T3	01-10-2004
		HK 1048550 A1	21-10-2004
		HR 20020180 A2	30-06-2004
		HU 0202471 A2	28-11-2002
		JP 2003508838 T	04-03-2003
		MA 27459 A1	01-08-2005
		MX PA02002081 A	30-07-2004
		NO 20020996 A	24-04-2002
		NZ 517840 A	24-03-2005
		PL 353773 A1	01-12-2003
		PT 1212732 T	30-06-2004
		TR 200201280 T2	21-08-2002
		TR 200202436 T2	21-01-2003
		TW 548564 B	21-08-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2006/064383

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/32

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)
H04L G07F

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 estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC , XP002376605 page 491 page 547 - page 549 page 559 - page 560 page 572 - page 576	1-12
X	US 2003/097592 A1 (ADUSUMILLI KOTESHWERRAO) 22 mai 2003 (2003-05-22) abrégé alinéa [0035] - alinéa [0036]	1-12
A	US 5 903 721 A (SIXTUS ET AL) 11 mai 1999 (1999-05-11) abrégé figures 1,2 colonne 3, ligne 26 - colonne 5, ligne 31	1-12

-/--

[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
12 septembre 2006	19/09/2006

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	SAN MILLAN MAESO, J

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2006/064383

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	WO 01/16900 A (AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY,) 8 mars 2001 (2001-03-08) abrégé	1-12

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2006/064383

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)			Date de publication
US 2003097592	A1	22-05-2003	CN	1575579	A	02-02-2005
			DE	10297362	T5	09-09-2004
			GB	2395877	A	02-06-2004
			HK	1062752	A1	07-10-2005
			US	2003081783	A1	01-05-2003
			WO	03036913	A2	01-05-2003
US 5903721	A	11-05-1999	AU	6549498	A	29-09-1998
			BR	9809045	A	22-01-2002
			CA	2283933	A1	17-09-1998
			DE	1008022	T1	25-01-2001
			EA	1825	B1	27-08-2001
			EP	1008022	A2	14-06-2000
			ES	2150892	T1	16-12-2000
			JP	2001518212	T	09-10-2001
			NO	994428	A	09-11-1999
			WO	9840809	A2	17-09-1998
WO 0116900	A	08-03-2001	AT	258328	T	15-02-2004
			AU	775976	B2	19-08-2004
			AU	7090700	A	26-03-2001
			AU	2004231226	A1	23-12-2004
			BR	0013822	A	23-07-2002
			CA	2382922	A1	08-03-2001
			CN	1376292	A	23-10-2002
			CZ	20020744	A3	18-02-2004
			DE	60007883	D1	26-02-2004
			DE	60007883	T2	14-10-2004
			DK	1212732	T3	07-06-2004
			EP	1212732	A2	12-06-2002
			ES	2215064	T3	01-10-2004
			HK	1048550	A1	21-10-2004
			HR	20020180	A2	30-06-2004
			HU	0202471	A2	28-11-2002
			JP	2003508838	T	04-03-2003
			MA	27459	A1	01-08-2005
			MX	PA02002081	A	30-07-2004
			NO	20020996	A	24-04-2002
			NZ	517840	A	24-03-2005
			PL	353773	A1	01-12-2003
			PT	1212732	T	30-06-2004
			TR	200201280	T2	21-08-2002
			TR	200202436	T2	21-01-2003
			TW	548564	B	21-08-2003

フロントページの続き

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

(74)代理人 100125380
弁理士 中村 綾子
(74)代理人 100130960
弁理士 岡本 正之
(74)代理人 100125036
弁理士 深川 英里
(74)代理人 100142996
弁理士 森本 聡二
(72)発明者 アルディッティ，ダヴィド
フランス国，９２１４０ クラマール，リュ・ポール・ヴァイヤン‐クチュリエ，４６ テル
(72)発明者 フリッシュ，ローラン
フランス国，７５０１３ パリ，アヴニュ・ディタリー ２７
(72)発明者 シベール，エルヴェ
フランス国，１４０００ カーン，リュ・ロベール・ル・マニフィーク １７

Ｆターム(参考) 5B285 AA01 BA03 CA04 CA43 DA05
5J104 AA07 AA16 EA01 EA04 EA05 EA15 EA16 JA21 KA02 KA05
MA01 NA02 NA27 NA37 NA38