(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2005-510951
(P2005-510951A)
(43)公表日　平成17年4月21日(2005.4.21)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/32	H04L	9/00	675B	5J104
G09C 1/00	G09C	1/00	640E	
	H04L	9/00	675D	

審査請求 未請求　予備審査請求 有　（全 9 頁）

(21)出願番号	特願2003-548457 (P2003-548457)
(86)(22)出願日	平成14年11月26日 (2002.11.26)
(85)翻訳文提出日	平成16年5月28日 (2004.5.28)
(86)国際出願番号	PCT/NO2002/000446
(87)国際公開番号	WO2003/047161
(87)国際公開日	平成15年6月5日 (2003.6.5)
(31)優先権主張番号	20015812
(32)優先日	平成13年11月28日 (2001.11.28)
(33)優先権主張国	ノルウェー(NO)

(71)出願人　504206964
テレノア・エイエスエイ
ノルウェー国，エヌ－１３３１　フォルネブ，スナレイヴェイエン　３０
(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
(72)発明者　サンドベリ，レイフ
スウェーデン国，エス－１３２　３５　サルトフェー－ボー，イェンタンス・ヴェイ　１４

最終頁に続く

(54)【発明の名称】ＰＫＩ機能の登録及び有効化の方法

(57)【要約】
本発明は、各封筒に、未開封の状態では秘匿された起動コードと、封筒上には視覚確認できるように印刷された照会番号もしくはコードを記載した複数の封印された封筒を事前に印刷することにより、ＳＩＭ（加入者識別モジュール）カードのＰＫＩ機能の登録と起動を行う方法を開示している。各封筒の照会番号もしくはコードと関連した起動コードは、前記ＰＫＩに組み込まれるか、接続されたセキュリティサーバー内のテーブルに保存される。申請用紙とともに封印された封筒の一つがユーザに提供される。前記ユーザは、個人データとともに前記照会コードもしくは番号を前記申請用紙に記入し、これが前記ＰＫＩとセキュリティサーバーに転送される。前記ＰＫＩによって登録が承認されると、承認情報がユーザに送信され、ユーザの端末において、前記起動コードを入力するよう依頼する。同時に、前記テーブルの前記照会コードもしくは番号に関連した前記起動コードと、前記ユーザのスマートカードに対応するスマートカードの識別情報とが前記ＰＫＩの起動モジュールに提供される。前記端末において前記起動コードが入力されると、前記スマートカードの識別情報とともに前記起動コードとが、前記端末から前記起動モジュールへ送信される。前記起動コードとスマートカード識別情報が受信されると、前記起動モジュールは、受信した前記起動コードとスマートカードの識別情報が、前記セキュリティサーバーによって事前に提供された情報と一致するか判断する。一致する場合は、前記起動モジュールは、前記スマートカードのＰＫＩ部を有効にするために必要な手続きを行う。

【特許請求の範囲】
【請求項１】
公開鍵インフラストラクチャー（ＰＫＩ）のユーザを登録し、前記ユーザのスマートカードにあるＰＫＩ部を有効にする公開鍵の方法であって、前記スマートカードを端末に関連付け、前記端末を前記ＰＫＩへのアクセスを提供する通信ネットワークに接続し、前記ユーザに、申請書への個人データの記入と有効な身分証明書での本人確認とが登録のために求め、前記データを、前記身分証明書と照合して、前記登録の承認へ向けて前記ＰＫＩに電子送信し、
ａ）未開封の状態では秘匿された起動コードと、前記封筒上に視覚認識できるように印刷された照会番号もしくはコードとがそれぞれに記載された複数の封印された封筒を事前に印刷するステップであって、前記各封筒の照会番号もしくはコードと関連する前記起動コードとが、前記ＰＫＩに組み込まれるか、もしくは接続されたセキュリティサーバー内のテーブルに保存されているものである、ステップと、
ｂ）前記ユーザに、前記照会番号もしくはコードが事前に印刷することが可能である申請書とともに、前記封印された封筒のいずれかを提供するステップと、
ｃ）前記照会番号が前記申請書に事前に印刷されていない場合は、前記ユーザに前記申請書に前記照会番号もしくはコードを記入するよう依頼するステップと、
ｄ）前記個人データとともに、前記照会番号もしくはコードを前記ＰＫＩ及びセキュリティサーバーに転送するステップと、
ｅ）前記登録が前記ＰＫＩによって承認されると、前記ユーザに承認情報を送信して、ユーザの端末において前記起動コードを入力するように依頼し、前記テーブルの前記照会番号もしくはコードに関連した前記起動コードと、前記ユーザのスマートカードに対応するスマートカードの識別情報とを、前記ＰＫＩの起動モジュールに提供するステップと、
ｆ）前記起動コードの入力後、前記端末から、前記スマートカードの識別情報とともに前記起動コードを前記起動モジュールに対して送信し、そして、前記起動コードとスマートカードの識別情報を受信するステップと、
ｇ）前記受信された起動コードとスマートカードの識別情報が、前記セキュリティサーバーによって事前に提供された情報に一致するかを判断し、一致する場合、前記スマートカードのＰＫＩ部を動作可能にするステップと
を有することを特徴とする公開鍵インフラストラクチャーの方法。
【請求項２】
前記通信ネットワークがＧＳＭもしくは３Ｇネットワークであり、前記端末がＧＳＭもしくは３Ｇ携帯電話であり、前記スマートカードがＳＩＭカードであることを特徴とする請求項１に記載の方法。
【請求項３】
前記スマートカードの識別情報がＭＳＩＳＤＮ及びＩＣＣＩＤであることを特徴とする請求項２に記載の方法。
【請求項４】
前記ＰＫＩ機能が前記スマートカードに保存されており、有効とされるまで前記ユーザに対して秘匿されていることを特徴とする請求項１～３のいずれかに記載の方法。
【請求項５】
前記承認情報が、ＳＭＳ、電子メールもしくは郵便で送信されることを特徴とする請求項１～４のいずれかに記載の方法。
【請求項６】
前記封印された封筒ごとに、前記照会番号もしくはコード及び起動コードとともに状態が前記テーブルに保存されていることを特徴とする請求項１～５のいずれかに記載の方法。
【請求項７】
前記状態が初期段階では「不使用」に設定され、ステップｄ）においては「検討中」へ、ステップｅ）の承認の場合には「承認済みであるが非起動」へ、ステップｅ）の非承認

の場合には「非承認」へ、ステップｇ）において一致する場合には「起動」へ変更されることを特徴とする請求項６に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ＰＫＩ（公開鍵インフラストラクチャー）に関し、特にＳＩＭ（加入者識別モジュール）カードにおけるＰＫＩ（公開鍵インフラストラクチャー）機能の登録及び起動に関する。

【背景技術】

【０００２】

通信ネットワークの可能性を最大限に引き出すには、電子処理を行う際に、書類による処理の場合と同等の信頼性をもてるような標準化されたシステムが無くてはならない。

【０００３】

そのために、グローバルな商取引及び通信の根幹をなすものとしてＰＫＩが開発されてきた。ＰＫＩによって、機密性を有する電子通信が非公開とされ、不正な陰謀からの保護が保証される。ＰＫＩは、デジタル署名、認証および暗号化に用いられる。

【０００４】

ＰＫＩは、暗号の使用に基づくものである。すなわち、数式やバーチュアル鍵により情報をスクランブルすることであり、そうすることで、認証を受けた対象のみが関連する鍵を使用して解読できる。ＰＫＩには、認証権限者（ＣＡ）として認知された、信任を受けた第三者から提供された一組の暗号鍵が用いられる。ＰＫＩ運用の要として、ＣＡは所有者の身元が確認できるデジタルの証明書を発行する。ＣＡは、有効な証明書のアクセス可能なディレクトリと、無効にした証明書のリストを保持する。

【０００５】

従来、ＰＫＩ機能は、外部スマートカードに保存された証明書と鍵を用いてデータ端末によって利用されてきた。しかし、携帯電話が普及してデータ端末に加わり、将来、電話においてもまた、ＰＫＩ機能の必要性が発生するであろう。その際には、証明書と鍵は通常、例えばＧＳＭ電話におけるＳＩＭ（加入者識別モジュール）カードのように、加入者カードに保存されるであろう。

【０００６】

信頼性のあるＰＫＩシステムとしては、デジタル証明書を発行することによって新規ユーザを登録する際に、確実な手順が必須要件である。デジタル証明書を要求している人物が、本人が主張している身元と確かに一致することに１００％の確証がなくてはならない。このやり方として、通常は、そのユーザ本人が、例えば郵便局などの公認機関に直接出向き、所定のフォームに記入して、パスポートのような公的な証明書により、本人確認をする。郵便局の窓口担当者が身元確認情報を検証し、データ・フォームがＣＡに電子送信される。ＣＡは、データを制御、体裁を整えて（whitewash）、ＳＩＭカードもしくはスマートカードのどちらかの形態で、起動コード（activation code）とともにＰＫＩカードを発行する。次に、ＰＫＩカードと起動コードは書留郵便でユーザに送付される。ユーザは再度、郵便局に出向き、例えばパスポートによって身元確認を行い、その郵便物を受け取ることができる。

【０００７】

このように、二度にわたって公認機関に足を運ぶ必要があることが、ＰＫＩの普及の足枷になっている。というのは、それは単に、新規技術を利用するにあたって最初に課題がある、すなわち、多大な努力が初期段階で求められることへの一般大衆からの抵抗があるからであると考えられる。また、前記の手続きには時間がかかり、証明書がユーザに対して発行されてからユーザがＰＫＩ機能を利用できるまでに、最低でも一週間を要する。

【０００８】

デジタル証明書の発行者の立場から見ると、発行手続きにかかる費用は、特に書留郵便による送付を用いることから、比較的高いものとなっている。

【０００９】
このように、発行者とユーザ、両方の利益のために、発行手続きを簡略化する必要がある。
【発明の開示】
【発明が解決しようとする課題】
【００１０】
本発明の目的は、上記の障害を排除する方法を提供することである。添付された特許請求の範囲に明示された構成にはこの方法の特徴が記述されている。
【課題を解決するための手段】
【００１１】
詳しくは、本発明は、事前に印刷された複数の封印済み封筒を用意し、各々の封筒内に未開封の状態では秘匿されている起動コードを記載し、前記封筒上に照会番号もしくはコードを視覚確認できるように印刷することで、ＰＫＩのユーザを登録し、ユーザのスマートカードにおけるＰＫＩ部を有効にする公開鍵インフラストラクチャー（ＰＫＩ）の方法を提供する。各封筒の照会番号もしくはコード及び関連する起動コードは、ＰＫＩに組み込まれるか、もしくは接続されたセキュリティサーバー内のテーブルに保存されている。ユーザには申請書とともに封印された封筒のいずれかが渡される。ユーザは、申請書に、個人データとともに照会番号もしくはコードを記入するよう求められ、それがＰＫＩとセキュリティサーバーに転送される。
【００１２】
前記登録がＰＫＩによって承認されると、承認情報がユーザに伝送され、ユーザの端末において起動コードを入力するように指示がある。同時に、前記テーブルの照会コードもしくは番号に関連付けられた起動コードと、ユーザのスマートカードに対応するスマートカードの識別情報とが、ＰＫＩの起動モジュールに提供される。前記端末において起動コードが入力されると、スマートカードの識別情報とともに起動コードが、端末から起動モジュールへ送信される。起動コードとスマートカードの識別情報とが受信されると、起動モジュールは、受信した起動コードとスマートカードの識別情報とが、セキュリティサーバーから事前に提供されているものと一致するか判断し、一致すれば、起動モジュールは、スマートカードのＰＫＩ部を有効にするのに必要な手続きを行う。
【発明を実施するための最良の形態】
【００１３】
本発明は、ユーザが当人の持つＧＳＭ電話に対して、ＰＫＩ機能を有するＳＩＭカードを発注しようとしている実施形態により、以下に説明される。
【００１４】
上述したように、ユーザは、郵便局や銀行のような公認機関か、もしくは当人が登録されている電話会社に直接足を運ぶ必要がある。
【００１５】
前記公認機関において、ユーザには、記入を指示された申請書とともに、事前に印刷された封印済みの封筒が渡される。封筒上のわかりやすい場所に印刷された照会番号によって封筒が確認される。前記照会番号を申請書上にも印刷することにより、もしくはユーザに記入を要請するデータの一つとすることによって、ユーザが公認機関で受け取る申請書と封印された封筒とが互いに一意に関連付けされている。
【００１６】
申請書の記入後、ユーザの提示する身分証明書にある情報と記入された個人情報が一致するか、および、照会番号が封筒に印刷されているものに相当するかを担当者が確認する。前記個人情報と番号に問題がない場合、申請書は次の処理に回され、ユーザは、新しいＳＩＭカードを受け取るまで、前記封筒を未開封の状態で保持するよう指示される。
【００１７】
封印された封筒には、封筒が未開封の状態では不可視の起動コードが記載されている。事前に印刷された封筒全体に関するデータは、例えば、ＰＫＩに接続されたか、もしくは

組み込まれたセキュリティサーバー内のテーブルに保存される。封筒ごとに、少なくとも対応する照会番号、起動コード及び状態が保存される。これにより、セキュリティサーバーが一旦申請書の照会番号もしくはコードを把握すると、申請書とともに封筒によってユーザに与えられた起動コード、およびその申請処理が現時点でどの段階にあるかがわかるようになっている。前記状態とは、以下に挙げるいずれかである。不使用、検討中、承認済みであるが非起動、起動、非承認。初期段階では、前記状態は「不使用」に設定されている。

【００１８】

前記ユーザの例に戻ると、申請書のデータは、好ましくは電子処理により読み出され、セキュリティサーバーに転送される。同時に、前記テーブルに保存された封筒の状態は、「不使用」から「検討中」に変更される。本実施例においてはＰＫＩのＳＩＭカード用として申請として審査されるべき申請書のデータは、当業者が認知している先行技術による方法で、ＣＡの管理の下、ＰＫＩのサーバーにより処理される。さらに、前記処理の結果に基づいて、前記封筒の状態がセキュリティサーバーにおいて変更される。申請が拒否された場合、対応する状態は「非承認」に変更される。逆に、申請が承認された場合、当然、対応する状態は「承認」に変更される。

【００１９】

申請処理の結果はその後、通信ネットワーク、好ましくはＳＭＳか同様のものによる伝達、あるいは電子メールか郵便を介したメッセージで、ユーザに送付される。新しいＳＩＭカードがユーザに送られることはあっても、ユーザが封筒に秘匿されている起動コードを用いて身元を確認できるので、書留郵便を利用する必要はない。あるいは、ユーザがすでにＰＫＩ機能を搭載しているが現時点まで利用不可であるＳＩＭカードを所有している場合は、新しいＳＩＭカードを発行する必要はない。同時に、セキュリティサーバーによって、対応するＳＩＭカードに関して必要な識別情報とともに、照会番号、もしくはコードに関連する起動コードが起動モジュールに提供される。

【００２０】

肯定的な結果を示すメッセージは、例えば以下である。「あなたの申請は承認されましたので、封筒を開封して、中に記載した起動コードをあなたのＳＩＭカードに御使用ください。」

【００２１】

しかし、ユーザが起動コードを入力する前に、「ＳＩＭ　ＰＫＩ　メニュー」を有効にする必要がある。「ＳＩＭ　ＰＫＩ　メニュー」が有効になると、ユーザは所有する携帯機器において、起動コードを入力してサービスへの登録を行う。起動コードは、ＳＭＳによって、ＳＩＭカードの識別情報とともにＰＫＩへ送られる。ユーザは、３回まで、コードを正しく入力する機会を与えられる。

【００２２】

起動モジュールは、起動コードおよびＳＩＭカードの識別情報を入手し、それがセキュリーティサーバーからすでに提供されている起動コードおよびＳＩＭカード識別情報と一致するかどうか検証する。その後、起動モジュールはＳＩＭに対して、「コマンドを可能にするＰＫＩ鍵を生成」を送り返し、そのＳＩＭにおける鍵生成の申請によって、一つの私有鍵と一つの検証用公開鍵から成る一組の鍵が生成される。

【００２３】

検証用公開鍵（verification public key：ＶＰｕＫ）はＳＭＳによって起動モジュールに送信され、前記ＳＭＳは、ＧＳＭ０３．４８に従って、機密性を有する情報の保護のために好適には暗号化される。

【００２４】

その後ユーザは、例えば、処理に対する署名及び認証に用いられる、本人自ら選んだ署名ＰＩＮである、ＰＩＮ＿ＳＩＧＮＫＥＹを選択するように指示される。

【００２５】

検証が問題なく行われた場合、起動モジュールはＣＡに接続され、ユーザに関連する公

開鍵で有効な証明書を発行する。この証明書は同時に認証ディレクトリに送られる。

【００２６】

認証が滞りなく行われた確認がユーザに返信され、ＰＫＩメニューがＳＩＭにおいて無効になり、その結果、ＳＩＭカードにおけるＰＫＩ機能が有効になる。

【００２７】

本発明は、ユーザが公的機関に二度以上直接出向く必要がなくなる、ＰＫＩ（公開鍵インフラストラクチャー）機能の登録及び起動の方法を提供する。最初に身元確認をした後は、とりわけＲＡにおいて、ユーザの身元が起動コードに割り当てられる前に、起動コードを保有するため、ＰＫＩ機能に関連する項目やデータを送付する必要がなくなる。これによって、ユーザが最初に公認機関に姿を現した時点で、確実に、正当な起動コードが正当な保有者により保有される。

【００２８】

ユーザの観点からは、本発明は、ＰＫＩ機能の提供において、労力が省ける。発行者の観点からは、本発明は、ＰＫＩ使用者数を増加させる可能性が非常に高い。さらに、処理時間が減少し、書留郵便の必要性がなくなることから、登録ごとにかかる費用が削減される。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 02/00446

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32
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)

IPC7: H04L

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6061791 A (MOREAU, T.), 9 May 2000 (09.05.00), the whole document ---	1-7
P,A	EP 1162781 A2 (TRW INC.), 12 December 2001 (12.12.01), the whole document ---	1-7
P,A	WO 02060210 A1 (TELENOR ASA), 1 August 2002 (01.08.02), the whole document ---	1-7
P,A	EP 1185027 A2 (HITACHI, LTD.), 6 March 2002 (06.03.02), the whole document --- --------	1-7

☐ Further documents are listed in the continuation of Box C. ☒ 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
27 February 2003	03 -03- 2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson /OGU Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

30/12/02

International application No.
PCT/NO 02/00446

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6061791 A	09/05/00	AU 733803 B	24/05/01
		AU 7202698 A	08/12/98
		BR 9809272 A	27/06/00
		EP 1000481 A	17/05/00
		WO 9852316 A	19/11/98
EP 1162781 A2	12/12/01	EP 1162779 A	12/12/01
		EP 1162780 A	12/12/01
		EP 1162782 A	12/12/01
		EP 1162783 A	12/12/01
		EP 1162807 A	12/12/01
		EP 1164745 A	19/12/01
		EP 1175037 A	23/01/02
		EP 1175038 A	23/01/02
		EP 1175039 A	23/01/02
		JP 2002033726 A	31/01/02
		JP 2002049311 A	15/02/02
		JP 2002057660 A	22/02/02
		JP 2002057661 A	22/02/02
		JP 2002064485 A	28/02/02
		JP 2002082913 A	22/03/02
		JP 2002123492 A	26/04/02
		JP 2002124944 A	26/04/02
		JP 2002135244 A	10/05/02
		JP 2002135245 A	10/05/02
		US 2002138724 A	26/09/02
		US 2002141592 A	03/10/02
		US 2002144111 A	03/10/02
		US 2002176582 A	28/11/02
WO 02060210 A1	01/08/02	NO 313480 B	07/10/02
		NO 20010427 A	25/07/02
EP 1185027 A2	06/03/02	JP 2002072876 A	12/03/02
		US 2002046340 A	18/04/02

Form PCT/ISA/210 (patent family annex) (July 1998)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,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,IE,IT,LU,MC,NL,PT,SE,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,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

Ｆターム(参考) 5J104 AA01 AA07 AA09 AA16 EA04 EA15 EA22 JA21 KA01 KA04
MA01 MA05 NA02 NA35 NA37 NA38 NA40 PA01 PA07