

【公報種別】特許法第 17 条の 2 の規定による補正の掲載  
 【部門区分】第 7 部門第 3 区分  
 【発行日】平成 18 年 1 月 26 日 (2006.1.26)

【公表番号】特表 2005-510951(P2005-510951A)  
 【公表日】平成 17 年 4 月 21 日 (2005.4.21)  
 【年通号数】公開・登録公報 2005-016  
 【出願番号】特願 2003-548457(P2003-548457)  
 【国際特許分類】

**H 0 4 L      9/32      (2006.01)**

**G 0 9 C      1/00      (2006.01)**

【F I】

H 0 4 L      9/00      6 7 5 B

G 0 9 C      1/00      6 4 0 E

H 0 4 L      9/00      6 7 5 D

【手続補正書】  
 【提出日】平成 17 年 11 月 25 日 (2005.11.25)  
 【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】

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インフラストラクチャーの方法であって、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 P K I 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 G S M もしくは 3 G ネットワークであり、前記端末が G S M もしくは 3 G 携帯電話であり、前記スマートカードが S I M 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 M S I S D N 及び I C C I D 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 P K I 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、S M S、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。