【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21年9月3日(2009.9.3)

【公表番号】特表2009-503967(P2009-503967A)
【公表日】平成21年1月29日(2009.1.29)
【年通号数】公開・登録公報2009-004
【出願番号】特願2008-523317(P2008-523317)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/20　(2006.01)
Ｈ０４Ｌ　9/10　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６７５Ｄ
Ｇ０６Ｆ　15/00　３３０Ｃ
Ｈ０４Ｌ　9/00　６２１Ａ

【手続補正書】
【提出日】平成21年7月13日(2009.7.13)
【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）が有するコンピュータに登録（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）が有するコンピュータ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）が有するコンピュータ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、前記プロバイダが有するコンピュータ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が有するコンピュータ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が有するコンピュータ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。