【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25年11月14日(2013.11.14)

【公表番号】特表2013-509805(P2013-509805A)
【公表日】平成25年3月14日(2013.3.14)
【年通号数】公開・登録公報2013-013
【出願番号】特願2012-536825(P2012-536825)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｄ
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ

【手続補正書】
【提出日】平成25年9月20日(2013.9.20)
【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】
第１鍵の証明書を要求する方法であって、
前記第１鍵を証明させる証明書要求を作るステップと、
トラステッド・プラットフォーム・モジュールから、前記証明書要求に結び付けられた証明識別鍵を要求するステップと、
前記トラステッド・プラットフォーム・モジュールから、前記証明識別鍵を前記証明書要求に結び付ける識別結合を受け取るステップと、
前記トラステッド・プラットフォーム・モジュールが前記第１鍵に前記証明識別鍵で署名することを要求するステップと、
前記トラステッド・プラットフォーム・モジュールから、前記第１鍵を含み、前記証明識別鍵によって署名された鍵証明構造を受け取るステップと、
前記証明識別鍵を認証機関が信頼することを最初に確立することなく前記認証機関に、前記証明書要求、前記識別結合、前記鍵証明構造、および前記トラステッド・プラットフォーム・モジュールの公開裏書き鍵の第１証明書を含む情報を送るステップと、
前記認証機関から、前記第１鍵の第２証明書を受け取るステップであって、前記第２証明書が、前記トラステッド・プラットフォーム・モジュールによって動作が行われた後でのみ使用可能となる形態となっている、ステップと、
を含む、方法。
【請求項２】
請求項１記載の方法であって、更に、
前記証明書要求のダイジェストを計算するステップを含み、
前記証明識別鍵が、前記証明識別鍵を前記ダイジェストに結び付けることによって、前記証明書要求に結び付けられる、方法。
【請求項３】
請求項１記載の方法において、前記第１証明書が、前記認証機関の署名を含み、前記署名が、前記トラステッド・プラットフォーム・モジュールの秘密裏書き鍵を使用するプロ

セスのみによって解読可能であり、前記動作が、前記トラステッド・プラットフォーム・モジュールの秘密裏書き鍵の使用を含む、方法。
【請求項４】
請求項３記載の方法であって、更に、
前記認証機関から、前記トラステッド・プラットフォーム・モジュールの公開裏書き鍵によって暗号化された対称鍵を受け取るステップを含み、
前記第２証明書が、前記対称鍵によって暗号化された形態で前記署名を含み、前記トラステッド・プラットフォーム・モジュールの秘密裏書き鍵を使用する前記プロセスが、
前記対称鍵を解読するために、前記トラステッド・プラットフォーム・モジュールの秘密裏書き鍵を使用するステップと、
前記署名を解読するために、前記対称鍵を使用するステップと、
を含む、方法。
【請求項５】
請求項１記載の方法において、前記第２証明書が、暗号化された形態で受け取られる署名を含み、前記動作が、更に、
前記暗号化された形態の前記署名を、クリア形態の署名と置き換えるステップを含む、方法。
【請求項６】
請求項１記載の方法において、前記第１鍵が移行不可であり、前記鍵証明構造が、前記第１鍵が移行不可であるステートメントを含む、方法。
【請求項７】
請求項１記載の方法において、前記第１鍵が、前記トラステッド・プラットフォーム・モジュールが配置された装置においてデーターに署名するプロセスの一部として使用される、方法。
【請求項８】
請求項１から７のいずれか１項記載の方法を実行するためのコンピューター実行可能命令を有するコンピューター読み取り可能媒体。
【請求項９】
第１鍵を証明する要求に対して動作する方法であって、
第１鍵を証明する証明書要求と、
クライアントが実行する装置においてトラステッド・プラットフォーム・モジュールによって作られた証明識別鍵の識別結合と、
前記第１鍵の機構を明らかにするために前記証明識別鍵を使用する鍵証明構造と、
前記トラステッド・プラットフォーム・モジュールの公開裏書き鍵の第１証明書と、
を含む情報を前記クライアントから受け取るステップと、
前記公開裏書き鍵に基づいて、前記トラステッド・プラットフォーム・モジュールが、前記動作を実行する認証機関によって信頼されていることを検証するステップと、
前記識別結合が前記証明識別鍵を前記証明書要求に結び付けていることを検証するステップと、
前記鍵証明構造が、前記証明識別鍵の秘密部分の保持者による、前記第１鍵が前記機構を有することのステートメントを表すことを検証するステップと、
前記クライアントに、前記第１鍵の第２証明書を送るステップであって、前記第２証明書の使用が、前記証明識別鍵の信頼を最初に確立することなしでの前記トラステッド・プラットフォーム・モジュールの存在という条件が付いた、ステップと、
を含む、方法。
【請求項１０】
請求項９記載の方法において、前記第２証明書の使用が、前記トラステッド・プラットフォーム・モジュールの秘密裏書き鍵の使用後にのみ前記証明書を使用可能にすることによって、前記トラステッド・プラットフォーム・モジュールの存在という条件が付いたものとする、方法。

【請求項１１】
請求項９記載の方法において、前記第２証明書が、前記認証機関の署名を含み、当該署名が、前記トラステッド・プラットフォーム・モジュールの秘密裏書き鍵の使用によってのみ解読可能な形態となっている、方法。
【請求項１２】
請求項９記載の方法において、前記第２証明書が、前記認証機関の署名を含み、前記署名が対称鍵で暗号化され、前記方法が、更に、
前記トラステッド・プラットフォーム・モジュールの公開裏書き鍵によって暗号化された前記対称鍵を、前記クライアントに送るステップを含む、方法。
【請求項１３】
請求項９記載の方法において、前記機構が、前記第１鍵が移行不可であることを含み、前記鍵証明構造が、前記第１鍵が移行不可であることの明示的または暗示的ステートメントを含む、方法。
【請求項１４】
請求項９記載の方法において、前記識別結合が、前記証明書要求の第１ダイジェストを含ませることによって、前記証明識別鍵を前記証明書要求に結び付け、前記方法が、更に、
前記証明書要求の第２ダイジェストを計算するステップと、
前記第２ダイジェストが前記第１ダイジェストと一致することを検証するステップと、
を含む、方法。
【請求項１５】
請求項９から１４のいずれかに記載の方法を実行するためのコンピューター実行可能命令を有するコンピューター読み取り可能媒体。