【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17年8月25日(2005.8.25)

【公表番号】特表2005-520364(P2005-520364A)
【公表日】平成17年7月7日(2005.7.7)
【年通号数】公開・登録公報2005-026
【出願番号】特願2003-512893(P2003-512893)
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/32
　Ｇ０６Ｆ　15/00
　Ｇ０６Ｆ　17/60
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６７５Ｚ
　Ｇ０６Ｆ　15/00　　３１０Ａ
　Ｇ０６Ｆ　17/60　　１４０
　Ｈ０４Ｌ　 9/00　　６７５Ｂ
　Ｈ０４Ｌ　 9/00　　６７５Ｄ

【手続補正書】
【提出日】平成16年1月9日(2004.1.9)
【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】
　トランザクションのための新しいデジタル証明書を生成するシステムであって、
　通信ネットワークと、
　該通信ネットワークに接続される第１のプロセッサであって、該第１のプロセッサは、デジタル証明書の第１のグループを格納する第１のメモリと通信する、第１のプロセッサと、
　該通信ネットワークに接続される第２のプロセッサであって、該第２のプロセッサは、デジタル証明書の第２のグループを格納する第２のメモリと通信する、第２のプロセッサと、
　該通信ネットワークに接続される第３のプロセッサであって、該第３のプロセッサは、証明書の該第１および第２のグループの少なくとも１つの中の該第１および第２のプロセッサの少なくとも１つからの少なくとも１つの証明書をリクエストするためのものであり、該第１および第２のプロセッサの該少なくとも１つは、該少なくとも１つの証明書を発行するためのものである、第３のプロセッサと、
　該通信ネットワークに接続される第４のプロセッサであって、該第４のプロセッサは、第４のメモリと通信し、該第４のプロセッサは、該少なくとも１つの証明書を検証し、該第３のプロセッサは、新しい証明書を該第３のプロセッサに提供することを該第４のプロセッサにリクエストし、該第４のプロセッサは、該第３のプロセッサに該トランザクションのための該新しい証明書を送信する、第４のプロセッサと
　を備える、システム。
【請求項２】
　前記第３のプロセッサは、前記少なくとも１つの証明書が利用可能でない場合に新しい証明書を該第３のプロセッサに提供することを、前記第４のプロセッサにリクエストする

、請求項１に記載のシステム。
【請求項３】
前記新しい証明書は、前記第４のメモリ内に格納される、請求項１に記載のシステム。
【請求項４】
前記新しい証明書は、前記少なくとも１つの証明書と関連する情報を利用して、前記第４のプロセッサによって計算される、請求項１に記載のシステム。
【請求項５】
前記新しい証明書は、前記少なくとも１つの証明書と関連する情報を利用して、前記第４のプロセッサによって計算され、該第４のプロセッサは、前記第３のプロセッサに前記トランザクションのための該新しい証明書を送信し、該少なくとも１つの証明書のリストは、該第４のプロセッサが該第３のプロセッサに該証明書を送信する場合に該新しい証明書に添付される、請求項１に記載のシステム。
【請求項６】
前記新しい証明書は、前記少なくとも１つの証明書と関連する情報を利用して、前記第４のプロセッサによって、直ちに計算される、請求項１に記載のシステム。
【請求項７】
前記第３のプロセッサは、証明書の前記第１および第２のグループの少なくとも１つの中の前記第１および第２のプロセッサの少なくとも１つからの複数の証明書をリクエストし、該第１および第２のプロセッサは、該複数の証明書を発行し、該第３のプロセッサは、新しい証明書を該第３のプロセッサに提供することを前記第４のプロセッサにリクエストし、該第４のプロセッサは、該複数の証明書の中の各証明書に関連する情報に基づき該新しい証明書を計算する、請求項１に記載のシステム。
【請求項８】
前記第３のプロセッサは、証明書の前記第１および第２のグループの少なくとも１つの中の前記第１および第２のプロセッサの少なくとも１つからの複数の証明書をリクエストし、該第１および第２のプロセッサは、該複数の証明書を発行し、該第３のプロセッサは、新しい証明書を該第３のプロセッサに提供することを前記第４のプロセッサにリクエストし、該第４のプロセッサは、該複数の証明書の中の１つより多い証明書であって、該複数の証明書の中の全証明書よりも少ない証明書に関連する情報に基づき該新しい証明書を計算する、請求項１に記載のシステム。
【請求項９】
前記新しい証明書は、ユーザと第３のプロセッサとの間のやりとりに関連する情報を利用して、前記第４のプロセッサによって計算される、請求項１に記載のシステム。
【請求項１０】
前記第３のプロセッサは、証明書の前記第１および第２のグループの少なくとも１つの中の前記第１および第２のプロセッサの少なくとも１つからの複数の証明書をリクエストし、該第１および第２のプロセッサは、該複数の証明書を発行し、該第３のプロセッサは、新しい証明書を該第３のプロセッサに提供することを前記第４のプロセッサにリクエストし、該新しい証明書は、該複数の証明書に加えられ、かつ、該複数の証明書の一部にされる、請求項１に記載のシステム。
【請求項１１】
前記第３のプロセッサは、証明書の前記第１および第２のグループの少なくとも１つの中の前記第１および第２のプロセッサの少なくとも１つからの複数の証明書をリクエストし、該第１および第２のプロセッサは、該複数の証明書を発行し、該第３のプロセッサは、新しい証明書を該第３のプロセッサに提供することを前記第４のプロセッサにリクエストし、該新しい証明書は、該複数の証明書の中の少なくとも１つの証明書と置き換える、請求項１に記載のシステム。
【請求項１２】
前記第１、第２、および第４のプロセッサは、サーバである、請求項１に記載のシステム。

【請求項１３】
前記第１、第２、および第４のプロセッサの少なくとも１つは、暗号化コプロセッサを備える、請求項１に記載のシステム。
【請求項１４】
前記第３のプロセッサは、パーソナルコンピュータである、請求項１に記載のシステム。
【請求項１５】
前記通信ネットワークは、イーサネット（Ｒ）、インターネット、イントラネット、ワイドエリアネットワーク、ローカルエリアネットワーク、バーチャルプライベートネットワーク、無線、非同期伝送方法、同期、ダイアルアップ、分散型ネットワークの少なくとも１つである、請求項１に記載のシステム。
【請求項１６】
前記新しい証明書は、前記少なくとも１つの証明書と関連する情報を利用して、前記第４のプロセッサによって計算され、該第４のプロセッサは、該新しい証明書を計算する前に該少なくとも１つの証明書を検証する、請求項１に記載のシステム。
【請求項１７】
トランザクションのための新しいデジタル証明書を生成する方法であって、
第１および第２のプロセッサそれぞれに接続される第１および第２のメモリそれぞれに格納される証明書の第１および第２のグループの少なくとも１つから、少なくとも１つの証明書をユーザプロセッサに送信するリクエストを、ユーザプロセッサから受信することを提供するステップと、
該少なくとも１つの証明書を該ユーザプロセッサへ送信することを提供するステップと、
該少なくとも１つの証明書を第４のプロセッサで受信することを提供するステップと、
該少なくとも１つの証明書を検証することを提供するステップと、
該第４のプロセッサから該ユーザプロセッサへ該トランザクションのための新しい証明書を送信することを提供するステップと
を包含する、方法。
【請求項１８】
デジタル証明書の前記第１のグループを前記第１のプロセッサに接続される前記第１のメモリへ格納することを提供するステップと、
デジタル証明書の前記第２のグループを前記第２のプロセッサに接続される前記第２のメモリへ格納することを提供するステップと
をさらに包含する、請求項１７に記載の方法。
【請求項１９】
前記第１、第２、ユーザ、および第４のプロセッサは、通信ネットワークに接続される、請求項１７に記載の方法。
【請求項２０】
前記第４のプロセッサが前記ユーザプロセッサに新しい証明書を提供するためのリクエストを受信することを提供する前記ステップは、前記少なくとも１つの証明書が利用可能でない場合に実行される、請求項１７に記載の方法。
【請求項２１】
前記新しい証明書は、第４のメモリ内に格納される、請求項１７に記載の方法。
【請求項２２】
前記少なくとも１つの証明書に関連する情報を利用して、前記新しい証明書を計算することを提供するステップ
をさらに包含する、請求項１７に記載の方法。
【請求項２３】
前記計算は、前記第４のプロセッサによって実行される、請求項２２に記載の方法。
【請求項２４】

前記第４のプロセッサが前記ユーザプロセッサに前記新しい証明書を送信する場合に、該新しい証明書に前記少なくとも１つの証明書を添付することを提供するステップ
をさらに包含する、請求項２３に記載の方法。
【請求項２５】
リクエストを受信することを提供する前記ステップは、証明書の前記第１および第２のグループの少なくとも１つの中から、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信することを提供するステップを包含し、前記少なくとも１つの証明書を送信することを提供する前記ステップは、前記ユーザプロセッサへ該複数の証明書を送信することを提供するステップを包含し、
前記第４のプロセッサが該ユーザプロセッサへ新しい証明書を提供するリクエストを受信することを提供するステップと、
該複数の証明書の中の各証明書に関連する情報に基づいて該新しい証明書を計算することを提供するステップと
をさらに備える、請求項１７に記載の方法。
【請求項２６】
リクエストを受信することを提供する前記ステップは、証明書の前記第１および第２のグループの少なくとも１つの中から、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信することを提供するステップを包含し、前記少なくとも１つの証明書を送信することを提供するステップは、前記ユーザプロセッサへ該複数の証明書を送信することを提供するステップを包含し、
前記第４のプロセッサが該ユーザプロセッサへ新しい証明書を提供するリクエストを受信することを提供するステップと、
該複数の証明書の中の１つより多い証明書であって、該複数の証明書の中の全証明書より少ない証明書に関連する情報に基づいて該新しい証明書を計算することを提供するステップと
をさらに備える、請求項１７に記載の方法。
【請求項２７】
リクエストを受信することを提供する前記ステップは、証明書の前記第１および第２のグループの少なくとも１つの中の、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信することを提供するステップを包含し、前記少なくとも１つの証明書を送信することを提供する前記ステップは、前記ユーザプロセッサへ該複数の証明書を送信することを提供するステップを包含し、
前記第４のプロセッサが該ユーザプロセッサへ新しい証明書を提供するリクエストを受信することを提供するステップと、
該新しい証明書を計算することを提供するステップと、
該複数の証明書に該新しい証明書を加えるために、該新しい証明書を該ユーザプロセッサへ送信することを提供するステップと
をさらに備える、請求項１７に記載の方法。
【請求項２８】
リクエストを受信することを提供する前記ステップは、証明書の前記第１および第２のグループの少なくとも１つの中から、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信することを提供するステップを包含し、前記少なくとも１つの証明書を送信することを提供する前記ステップは、前記ユーザプロセッサへ該複数の証明書を送信することを提供するステップを包含し、
前記第４のプロセッサが該ユーザプロセッサへ新しい証明書を提供するリクエストを受信することを提供するステップと、
該新しい証明書を計算することを提供するステップと、
該複数の証明書の中の該少なくとも１つの証明書を置き換えるために、該新しい証明書を該ユーザプロセッサに送信することを提供するステップと
をさらに備える、請求項１７に記載の方法。

【請求項２９】
トランザクションのための新しいデジタル証明書を生成するコンピュータプログラム製品であって、
第１および第２のプロセッサそれぞれに接続される第１および第２のメモリそれぞれに格納される証明書の第１および第２のグループの少なくとも１つから、少なくとも１つの証明書をユーザプロセッサに送信するリクエストを、ユーザプロセッサから受信するための第１のコードセグメントと、
該少なくとも１つの証明書を該ユーザプロセッサへ送信するための第２のコードセグメントと、
該少なくとも１つの証明書を第４のプロセッサで受信するための第３のコードセグメントと、
該少なくとも１つの証明書を検証するための第４のコードセグメントと、
該第４のプロセッサから該ユーザプロセッサへ該トランザクションのための新しい証明書を送信するための第５のコードセグメントと
を含む、コンピュータプログラム製品。
【請求項３０】
デジタル証明書の前記第１のグループを前記第１のプロセッサに接続される前記第１のメモリへ格納するための第６のコードセグメントと、
デジタル証明書の前記第２のグループを前記第２のプロセッサに接続される前記第２のメモリへ格納するための第７のコードセグメントと
をさらに含む、請求項２９に記載の製品。
【請求項３１】
前記少なくとも１つの証明書と関連する情報を利用して、前記新しい証明書を計算するための第６のコードセグメント
をさらに含む、請求項２９に記載の製品。
【請求項３２】
前記第４のプロセッサが前記ユーザプロセッサへ前記新しい証明書を送信する場合に、前記少なくとも１つの証明書のリストを該新しい証明書に添付するための第７のコードセグメント
をさらに含む、請求項３１に記載の製品。
【請求項３３】
前記第１のコードセグメントは、証明書の第１および第２のグループの少なくとも１つの中から、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信するためのコードセグメントを含み、前記の第２のコードステップは、前記ユーザプロセッサに該複数の証明書を送信するためのコードセグメントを含み、
前記第４のプロセッサが新しい証明書を該ユーザプロセッサに提供するリクエストを受信するための第６のコードセグメントと、
該複数の証明書の中の各証明書と関連する情報に基づいて該新しい証明書を計算するための第７のコードセグメントと
をさらに含む、請求項２９に記載の製品。
【請求項３４】
前記第１のコードセグメントは、証明書の第１および第２のグループの少なくとも１つの中から、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信するためのコードセグメントを含み、前記の第２のコードステップは、前記ユーザプロセッサに該複数の証明書を送信するためのコードセグメントを含み、
前記第４のプロセッサが新しい証明書を該ユーザプロセッサに提供するリクエストを受信するための第６のコードセグメントと、
該複数の証明書の中の１つより多い証明書であって、該複数の証明書の中の全証明書より少ない証明書と関連する情報に基づいて該新しい証明書を計算するための第７のコードセグメントと

をさらに含む、請求項２９に記載の製品。
【請求項３５】
前記第１のコードセグメントは、証明書の第１および第２のグループの少なくとも１つの中から、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信するためのコードセグメントを含み、前記の第２のコードステップは、前記ユーザプロセッサに該複数の証明書を送信するためのコードセグメントを含み、
前記第４のプロセッサが新しい証明書を該ユーザプロセッサに提供するリクエストを受信するための第６のコードセグメントと、
該新しい証明書を計算するための第７のコードセグメントと、
該複数の証明書に該新しい証明書を加えるために、該ユーザプロセッサに該新しい証明書を送信するための第８のコードセグメントと
をさらに含む、請求項２９に記載の製品。
【請求項３６】
前記第１のコードセグメントは、証明書の第１および第２のグループの少なくとも１つの中から、前記第１および第２のプロセッサの少なくとも１つからの複数の証明書に対するリクエストを受信するためのコードセグメントを含み、前記の第２のコードステップは、前記ユーザプロセッサに該複数の証明書を送信するためのコードセグメントを含み、
前記第４のプロセッサが新しい証明書を該ユーザプロセッサに提供するリクエストを受信するための第６のコードセグメントと、
該新しい証明書を計算するための第７のコードセグメントと、
該複数の証明書の中の少なくとも１つの証明書を置き換えるために、該ユーザプロセッサに該新しい証明書を送信するための第８のコードセグメントと
をさらに含む、請求項２９に記載の製品。
【請求項３７】
トランザクションのための新しい証明書を生成する方法であって
複数の証明書を含む証明書の初期リストを受信することを提供するステップと、
該複数の証明書の各々の確実性を検証することを提供するステップと、
作成アルゴリズムを用いて新しい証明書を計算すること提供するステップと、
該新しい証明書にサインすることを提供するステップと、
証明書の該リストを修正することを提供するステップと、
修正時に、該リストを該新しい証明書に添付させることを提供するステップと
を包含する、方法。
【請求項３８】
前記複数の証明書は、デジタルタイムスタンプである、請求項３７に記載の方法。
【請求項３９】
前記複数の証明書は、公開鍵証明書である、請求項３７に記載の方法。
【請求項４０】
前記複数の証明書は、デジタル署名サービスにより発行されるサインされたステートメントであり、該複数の証明書はそれぞれ、少なくとも１つのユーザアイデンティフィケーションとドキュメントの暗号化ダイジェスト有する、請求項３７に記載の方法。
【請求項４１】
前記複数の証明書は、電子公証サービスにより発行されるサインされたステートメントであり、該複数の証明書はそれぞれ、少なくとも１つのユーザアイデンティフィケーション、ドキュメントの暗号化ダイジェスト、およびタイムスタンプを有する、請求項３７に記載の方法。
【請求項４２】
前記新しい証明書は、デジタルタイムスタンプを含み、該タイムスタンプの数値は、該新しい証明書が計算される該複数の証明書の対応する値の最小値である、請求項３７に記載の方法。
【請求項４３】

前記新しい証明書は、デジタルタイムスタンプを含み、該タイムスタンプの数値は、該新しい証明書が計算される該複数の証明書の対応する値の最大値である、請求項３７に記載の方法。

【請求項４４】

前記新しい証明書は、デジタルタイムスタンプを含み、該タイムスタンプの数値は、該新しい証明書が計算される該複数の証明書の対応する値のｋ番目に小さいものである、請求項３７に記載の方法。

【請求項４５】

前記新しい証明書は、デジタルタイムスタンプを含み、該タイムスタンプの数値は、該新しい証明書が計算される該複数の証明書の対応する値のｋ番目に大きいものである、請求項３７に記載の方法。

【請求項４６】

前記作成アルゴリズムは、決定論的であり、その出力は、受信した証明書のリストが直接含まない決定論的データに依存する、請求項３７に記載の方法。