(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2005-520364
(P2005-520364A)
(43)公表日　平成17年7月7日(2005.7.7)

| (51)Int.Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| H04L 9/32 | H04L 9/00 | 675Z | 5B085 |
| G06F 15/00 | G06F 15/00 | 310A | 5B185 |
| G06F 17/60 | G06F 17/60 | 140 | 5J104 |
| | H04L 9/00 | 675B | |
| | H04L 9/00 | 675D | |

審査請求 有　予備審査請求 有　（全 27 頁）

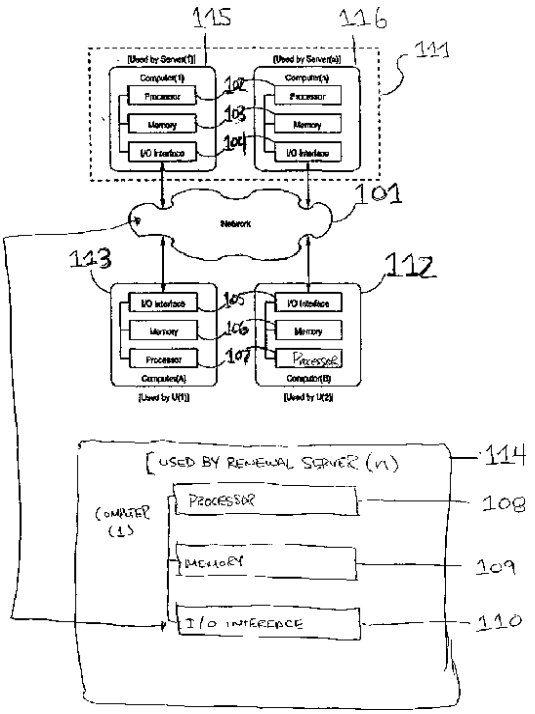
(21)出願番号　特願2003-512893 (P2003-512893)
(86)(22)出願日　平成14年7月3日 (2002.7.3)
(85)翻訳文提出日　平成16年1月9日 (2004.1.9)
(86)国際出願番号　PCT/IB2002/002643
(87)国際公開番号　WO2003/007203
(87)国際公開日　平成15年1月23日 (2003.1.23)
(31)優先権主張番号　60/303,951
(32)優先日　平成13年7月9日 (2001.7.9)
(33)優先権主張国　米国 (US)
(81)指定国　EP (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), CA, CN, IN, JP, MX, US

(71)出願人　504014118
リナックスプローブ株式会社
東京都港区赤坂２－１４－５プラザミカド
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹
(72)発明者　サアレペラ，　マート
東京都大田区東馬込２０８０２マツシタビルディング３０１

最終頁に続く

(54)【発明の名称】デジタル署名された証明書を更新しかつ拡張するシステムおよび方法

(57)【要約】
新しくデジタル署名されたステートメント（証明書）を生成するシステム、方法、およびコンピュータプログラム製品が提供される。生成された新しい証明書は、損なわれた署名のための更新手順内で利用され得る。本発明のシステム、方法、およびコンピュータプログラム製品は、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によって新しい証明書を生成し、各複数の証明書の確実性を検証し、作成アルゴリズムを利用して新しい証明書を計算し、新しい証明書に署名し、証明書のリストを修正し、および修正時に新しい証明書にリストを添付する。



【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のプロセッサに該新しい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】
ユーザと前記第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２９】
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３０】
前記少なくとも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と
をさらに包含する、請求項１７に記載の方法。
【請求項３１】
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４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３２】
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５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６のコードセグメントと

をさらに含む、請求項３１に記載の製品。
【請求項３３】
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５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３４】
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３３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５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６のコードセグメントと
をさらに含む、請求項３１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５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６のコードセグメントと
をさらに含む、請求項３１に記載の製品。
【請求項３７】
ユーザと前記第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、前記新しい証明書を計算するための第５のコードセグメント
をさらに備える、請求項３１に記載の製品。
【請求項３８】
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５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６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７のコードセグメントと
をさらに含む、請求項３１に記載の製品。
【請求項３９】
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５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６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７のコードセグメントと
をさらに含む、請求項３１に記載の製品。
【請求項４０】
前記少なくとも１つの証明書を検証するための第５のコードセグメントと、
該少なくとも１つの証明書と関連する情報を利用して、該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と
をさらに備える、請求項３１に記載の製品。
【請求項４１】
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４２】
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４３】
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４２に記載の方法。
【請求項４４】
前記複数の証明書は、公開鍵証明書である、請求項４２に記載の方法。
【請求項４５】
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４２に記載の方法。
【請求項４６】
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４２に記載の方法。
【請求項４７】
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４２に記載の方法。

【請求項４８】
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４２に記載の方法。
【請求項４９】
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４２に記載の方法。
【請求項５０】
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４２に記載の方法。
【請求項５１】
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４２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は概して、電子署名されたステートメントに関する。本発明は特に、電子署名されたステートメントを用いて人／または物のアイデンティティを認証し、かつ、電子通信ネットワークを介して送られるトランザクションに関する時刻を認証することに関する。
【背景技術】
【０００２】
印刷された書類に対して手書きの署名が用いられるのと同様の様式で、電子書類に対しては電子署名が用いられる。電子署名は、電子メール、電子商取引、グループウェア、および電子ファンド伝送を含む様々な電子トランザクションに用いられ得る。
【０００３】
書類に署名する目的の１つは、証拠としての機能である。書類の所有者（依存側）は、署名をした者が書類の内容に同意したということを後で証明することができる。例えば、約束手形に署名がなされた後では、手形の所有者が金銭を取り戻すために（ほとんどの場合）十分な証拠を作り出すことができる。例えば、アリスがボブに１００ドル貸したとする。見返りにボブは約束手形に署名してアリスに渡す。数ヶ月後、アリスは、１００ドルを取り戻すために、ボブにその約束手形を提示する。アリスがボブの署名入りの約束手形を紛失すると、ボブはアリスから金銭を受け取ったことを否定することができ、アリスはそうでないという証拠を持たないことになる。しかしアリスが約束手形を確実に保存していれば、ボブはアリスに金銭を借りていることを否定することはできない。なぜなら、いつでもボブの署名がベリファイされ得るからである。
【０００４】
今日、ますます多くの書類が作成され、管理され、電子形態で伝送されている。暗号化技術は、電子署名に、秘密の暗号化鍵（署名者のみが知る）で作成され公開鍵（何人も知っている）でベリファイされる「署名」を提供することができる。秘密鍵にアクセスすることができなければ、有効な（対応する公開鍵で首尾良くベリファイされる）暗号化署名を作成することは不可能である。しかし暗号化署名に関する主要な懸念は、秘密鍵が公開される（他人に暴露される）可能性を完全に排除する方法がないということである。漏洩されると、鍵は偽造され得、漏洩前に提供された「善意の」署名と漏洩後にハッカーによって提供された「悪意の」署名とを見分けることは困難である。アリスとボブの場合に戻って、ボブが暗号化署名を用いて約束手形に署名したとする。ボブに誠意がなければ、約束手形に署名した直後に「誤って」署名を漏らしてしまい、金銭を受け取ったことを後に否定するということがあり得る。アリスが約束手形を持ち出しても、ボブは、「誤って」漏らされた鍵を用いてアリスが自分自身で手形を作成したと主張する。

【０００５】
暗号化署名には、署名者（ボブ）にも依存側（アリス）にも依存しない、さらに深刻な脅威がある。暗号化署名のメカニズムおよびアルゴリズムは、当てにならずセキュアでないものになり得る。遅かれ早かれすべての暗号化メカニズムは、セキュアでなくなる。暗号化署名が無効になることに対して、追加の防止または回復手段が必要である。さもなければ、電子署名は役立たずになる。
【０００６】
今日までに提供されている方法はほとんど、防止の性質を有するものである。例えば、Ｈａｂｅｒは、入れ子式暗号化機能を用いる方法を提案している。これによると、１つの暗号化機能（暗号化署名など）がセキュアでなくなる前に、別の暗号化機能（例えば別の鍵による署名）が、第１の暗号化機能の結果に適用される。
【０００７】
暗号化の弱みに対処する１つの方法は、ボブ（および他の人々）が署名したすべてのステートメントを格納するサーバ（または冗長サーバのネットワーク）をセットアップすることである。この解決策によると、暗号化署名は不要である。ボブまたは他の人々が署名しようとする書類をサーバに送ったときに、パスワードを用いて彼らを認証し得る。この問題に対する唯一の公知の解決策は、冗長、すなわち同じ１つの事実（例えば、「ボブがアリスに１００ドル借りている」）を確認する書類に署名するために複数の暗号化鍵および方法を用いることである。１つの方法または鍵が無効になっても、まだ有効な鍵セットがあり、事実を証明することができる。同じ１つのことを証明するためにデジタル署名された証明書のリストを用いることは周知である。しかし、冗長でさえもそれ自体、長い目で見れば書類を保護するためには十分でない。すべてのコンポーネントは最終的には１つ１つ破られていき、最終的には同じ結果となる。事実を証明することはもはやできない。
【０００８】
本発明は、これらおよび他の問題点を解決するために提供される。
【発明の開示】
【課題を解決するための手段】
【０００９】
（発明の要旨）
本発明は、暗号署名を用いる電子証明書のリスト内で表わされた証明の有効性を保存するための方法、システム、およびプログラムである。本方法、システム、およびプログラムは、暗号化方法が安全ではなくなるか、または鍵が損なわれたとしても、無限に長期間にわたって証明が検証可能になることを可能にする。一実施形態では、送信されたリストにおける電子証明書の内容は、新しい電子証明書を生成するための信頼された情報源として使用される。新しい電子証明書は、元のリストのさらなるメンバとなる。このようなサービスを用いると、無効の電子証明のリストを新しい電子証明書と置換することが可能になる。その結果、さらなる新しい電子証明書を有する電子証明書のリストは、等強度内にある事実を確認する。証明として新しいリストの品質は低下されない。
【００１０】
一実施形態では、デジタル署名電子証明書のリストは、電子サービスＳから最初に獲得され、クライアントからクエリｘを受信すると、デジタル署名電子証明書$Sign_S\{A(x)\}$を用いて返答する。ここで、Ａ（ｘ）は、ｘに関する所定のステートメントである。例えば、ｘがクレジットカード番号である場合、Ａ（ｘ）は、「ｘはｔで有効であった」等のステートメントであり得、ここで、ｔは、時間／日付を表わす。別の例は、デジタルタイムスタンピングに関連する。そこでは、ステートメントＡ（ｘ）は、「ｘはｔにおいてＳに提示されていた」を意味し得、Ｓはまた、「ｘはＵＳの市民である」等のステートメントを発行し得る。
【００１１】
デジタル署名付き電子証明書がクライアントコンピュータによって受信された後、主な関心の内の１つは、これらの発行された証明書の証拠値に関係する。デジタル署名方式は

、永久に安全ではない。なぜなら、秘密鍵がリークするかまたは暗号化アルゴリズムが破壊され得るためである。一実施形態では、Ｓの鍵が損なわれる場合、Ｓは新しい鍵を生成し、古い鍵を使用して作成された署名を新しい鍵を用いて作成された署名に置換する。古い鍵によって署名された証明書が与えられる場合に限り、このような再生プロセスが意味をなし、Ｓは、証明書が（１）認証される（Ｓ自体によって実際に発行された）または（２）偽造（損なわれた鍵へのアクセスを取得した悪意のある者によって作成された）であるかどうかを決定することが可能である。サービスプロバイダＳが発行された全てのステートメントのデータベースを有する場合、認証および偽造証明書は区別が簡単である。時には、このようなデータベースは他の理由のために必要であり、それにより、再生目的でこのデータベースを使用することは、さらなるコストを作成しない。しかし、デジタルタイムスタンプ等の他のサービスに対して、このようなデータベースを保守することは、不合理にも贅沢であるように思われる。サービス自体はほとんど「状態がない（ｓｔａｔｅｌｅｓｓ）」。変更可能な唯一の状態は、現在の時間／日付である。従って、なぜなら証明書は、将来のＴＳＡの挙動に対する影響を有さないために、以前に発行された証明書を格納する必要がない。しかし、発行された以前の証明書の認証リストは、ＴＳＡの署名鍵が損なわれる場合、高価なデータベースおよび取り出し機構を必要とする。

【００１２】

破壊された暗号方式および鍵損傷に関連した脅威を克服するために、サーバ$S_1$、．．．、$S_s$の（分散型）ネットワークからなるサービスは、同じタイプのステートメントを表わす証明書を作成する。これらのステートメントを署名するために、上記サーバは、異なる鍵または署名方式を使用し得る。鍵または方式の内の１つが損傷される場合、他の鍵または方式によって署名された証明書は認証されたままであり、損傷された方式によって作成された証明書を復元する（再生する）ために、信頼された情報として使用され得る。再生のために、再生／拡張サーバ$R_1$、．．．、$R_r$の（分散型）ネットワークからなるサービスは、署名$S_1$、．．．、$S_s$を検証し、新しい証明書を生成する。再生／拡張サービスは、$S_1$、．．．、$S_s$によって提示されるか、または独立して動作されるサービスの一部であり得る。

【００１３】

一実施形態では、本発明は、デジタル署名された証明書のリストを再生するための方法である。本方法は、１）署名された証明書の初期セットのサブリストを再生サーバのセットに転送するステップと、２）サブリストにおける証明書上の暗号署名を検証するステップと、３）サブリストにおける証明書の内容を結合し、作成アルゴリズムを用いて新しいステートメントを計算するステップと、４）新しいステートメントを暗号署名するステップと、５）初期リストの損傷された証明書を新しい証明書で置換するステップとを少なくとも包含する。

【００１４】

代替的な実施形態では、本発明は、デジタル署名証明書のリストを拡張するための方法である。本方法は、１）署名された証明書の初期セットのサブリストを再生サーバのセットに転送するステップと、２）サブリストにおける証明書上の暗号署名を検証するステップと、３）サブリストにおける証明書の内容を結合し、作成アルゴリズムを用いて新しいステートメントを計算するステップと、４）新しいステートメントを暗号署名するステップと、５）さらなる証明書を証明書の初期リストに追加するステップとを少なくとも包含する。

【００１５】

別の実施形態では、本発明は、多数の元のサーバによって署名された複数のデジタル署名証明書から使用できない証明書を再生するために提供されたシステムおよび方法である。本実施形態におけるシステムおよび方法は、元のサーバのセット、ユーザコンピュータ、および通信ネットワークに接続された再生サーバのセットを含む。さらに、ユーザコンピュータからの初期リクエストに応じて、元のサーバのセットは、安全な電子取引における使用のために１つ以上のデジタル証明書を発行する。さらに、証明書の内の１つは、暗

号鍵の破損または証明書の不正によって使用不可能になる場合、残りの有効な証明書のリストは再生サーバに送信される。再生サーバは、最初に公開鍵の組を用いて証明書上の署名を有効にする。次いで、計算アルゴリズムを利用することによって、再生サーバは、ユーザコンピュータから転送された有効かつ認証された証明書のリストを獲得し、新しい証明書を生成する。新しい証明書のユーザコンピュータへの再転送の前に、ステートメントは、再生サーバおよび添付された更新されたリストによってデジタル署名される。新しい証明書は、ユーザコンピュータに再送信され、使用不可能な証明書を置換し、それにより再生プロセスを完成する。

【００１６】

例えば、電子タイプスタンプにおいて、クエリｘを受信したサービスＳは、デジタル署名電子証明書$Ｓｉｇｎ_{ｓ}\{Ａ（ｘ）\}$を用いて返答する。ここで、Ａ（ｘ）は、「ｘはｔにおいてＳに提示された」の形態のｘに関するステートメントである。ステートメントｘは、手形上のＢｏｂの署名であり得る。ｘに対する証明書を取得するために、Ａｌｉｃｅは、ｎの異なるサーバを選択し、ｎの異なる証明書を取得する。これらの証明書の内の１つが無効になる場合、Ａｌｉｃｅは、新しい証明書を取得するために本発明のこの再生方法をインプリメントする再生サービスを使用する。Ａｌｉｃｅは、依然として有効である証明書のサブリストを選択し、その証明書をサーバに送信する。その結果、Ａｌｉｃｅは。新しい証明書の内容は、「Ｒは、ｘがｔ’において存在することを確認する」という形態であり得る。ここで、ｔ’は、証明書のサブリストが含む時間値の関数である。

【００１７】

別の実施形態では、本発明は、証明書拡張のために提供されたシステムおよび方法である。すなわち、多くの元のサーバによって署名された複数のデジタル署名証明書を拡張する。ユーザコンピュータと相互作用するユーザは、１より多くの証明書だけリストを拡張することによって鍵損傷に対してより抵抗のあるデジタル証明書のセットを作成するようにこの手続を開始することを望み得る。本実施形態では、ユーザコンピュータ上の使用不可能な証明書を置換するのではなく、新しい証明書がｎ個の元の証明書のリストに追加される。ここでユーザコンピュータは、ｎ＋１個のデジタル証明書を有する。

【００１８】

別の実施形態では、本発明は、デジタル署名された証明書を再生または拡張する方法をインプリメントする証明書サービスシステムである。サービスは、ａ）証明書発行サーバ、およびｂ）再生／拡張サーバである２種類の（分散型）サーバのネットワークを含む。クライアントコンピュータは、証明書に対する要求を準備し、そのリクエストを複数の証明書発行サーバに同時に送信する。各証明書発行サーバは、リクエストに応じて証明書を発行し、証明書をクライアントに送信する。クライアントは、上記証明書を受信し、その証明書の全てを１つのディレクトリに保持する。クライアントコンピュータは、証明書の検証のためのプログラムを含む。クライアントは、そのディレクトリ内の証明書が有効であることが確信される証明書検証プログラムを頻繁に使用する。そのディレクトリ内のいくつかの証明書がもはや有効でない場合、クライアントコンピュータは、有効でない証明書を除去し、証明書再生リクエストを準備し、証明書再生リクエストは、上記ディレクトリ内の全ての有効な証明書を含み、その証明書を再生／拡張サーバの内の１つに送信する。再生／拡張サーバは、本発明の方法を用いることによってクライアントのリクエストに基づいて新しい証明書を発行し、新しい証明書を再度クライアントに送信する。クライアントコンピュータが新しい証明書を証明書のディレクトリに置く。クライアントが無効な証明書を発見する場合、クライアントは、再度再生手続を繰り返す。

【００１９】

さらなる実施形態では、本発明は、デジタルタイムスタンプサービスにおける証明書拡張または再生のために提供されたシステム、方法、および製品である。タイムスタンピングサーバ（ＴＳＡ）によって発行された各デジタルタイムスタンプは、ステートメント「時間／日付」を有する。ここで、計算アルゴリズムはまた、新しい証明書を生成する際の引数のリストのｋ番目の最大要素を利用し得る。他の代替的なサービスの実施形態は、以

下に限定されないが、公開鍵証明書サービス、デジタル署名サービス、証明書有効性サービス、および電子文書サービスを含む。

【００２０】

通信ネットワークのタイプは、以下に限定されないが、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、非対称転送方法、同期、ダイヤルアップ、分散型、および他のタイプを含み得る。有利にも、本発明を用いると、サービスは、暗号鍵における不正または破損のために使用不可能になるデジタル証明書を効率的かつコスト効率的に再生し得る。デジタル署名のセキュリティをさらに高めるために、本発明はまた、既存のグループのデジタル証明書を拡張する。

【００２１】

本発明の他の特徴および利点は、以下の図面と共に考慮することによって以下の明細書から明らかになる。

【発明を実施するための最良の形態】

【００２２】

（詳細な説明）

本発明は、多くの異なる形態の実施形態の影響を受けやすいが、本発明の開示が本発明の原理の例証として考慮され、本発明の幅広い局面を示された実施形態に限定することが意図されないことを理解する共に、本発明の好適な実施形態が本明細書中で図面に示され、かつ詳細に説明される。

【００２３】

本発明は、有効な証明書のデータベースを保守する必要のないデジタル署名された証明書を再生するためのシステム、方法、およびプログラムに関する。本発明の一実施形態は、元のサーバ１１１のセットを使用し、このサーバは、同じタイプのデジタル証明書２０５を発行する。リクエストｘ２０１に対する証明書を獲得するために、ユーザは、ｎ個の異なるサーバ１１６を選択およびｎ個の異なる証明書２０４を獲得する。これらの証明書の内の１つが使用不可能になる場合、依然として有効な証明書Ｃ（１）、．．．、Ｃ（ｍ）のｍのエレメント（ｍ＜ｎ）リストが再生サーバＲ１１４に送信される。鍵が損傷され、証明書がこわされ、または暗号方式が破壊されると、証明書は使用不可能になる。一般性を失うことなく、有効な証明書のリストが、

$$C(1)=Sign_{S(1)}\{A_1(x)\},\ldots,$$
$$C(m)\ Sign_{S(m)}\{A_m(x)\}$$

であることを想定し得る。

これらの証明書上の署名が正確である場合、Ｒ１１４は、新しい証明書Ｃ（ｍ＋１）＝$Sign_R\{A(x)\}$（ただし、$A(x)=F[A_1(x),\ldots,A_m(x)]$）であり、ここで、Ｆ４０１は、作成アルゴリズムである。損傷された古い証明書は、新しい証明書Ｃ（ｍ＋１）２０７と置換される。リスト中の証明書の内の１つのみが損傷された場合、再び、新しいリストのｎ個の有効なコンポーネントおよび鍵の損傷に対する抵抗が以前の証明書と同じになる。データベースはこの手続で必要とされない。デジタル署名が使用不可能になるこれらの場合では、本発明のシステム、方法、およびプログラムは、新しい証明書を生成することによって証明書を再生し得る。本発明の別の実施形態は、さらなるデジタル署名を生成し、それにより１つ以上の証明書によってリストを拡張するように手続を開始するユーザを含む。この証明書拡張プロセスは、損傷に対する抵抗を強化する効果を有する。

【００２４】

図１では、コンピュータ１１２（人間ユーザとやり取りし、かつネットワーク１０１にアクセスするためのＩ／Ｏインターフェース１０５を含む従来のパーソナルコンピュータ）、デジタル証明書のグループおよび説明される他のデータを格納するためのメモリ１０６、およびデジタル証明書をリクエスト、受信、および置換するためのプロセッサ１０７は、通信ネットワーク１０１にアクセスするためにユーザによって利用される。あるいは

、ネットワークに接続されるのは、元のサーバコンピュータ１１１のグループおよび再生サーバ１１４である。元のサーバコンピュータ１１１のグループは、デジタル証明書の最初のセットをユーザコンピュータ１１２に配信するために使用される少なくとも２つ以上のコンピュータから構成される。複数の元のサーバ１１１からの第１のサーバ１１５および第２のサーバ１１６は、デジタル証明書の最初のセットを作成するために、Ｉ／Ｏインターフェース１０４、メモリ１０６、およびプロセッサ１０７から構成される。再生サーバ１１３は、ユーザコンピュータ１１２から受信されたｎ個の有効な証明書のセットに基づいて新しいデジタル署名を生成するために使用される少なくとも１つ以上のコンピュータから構成され、このコンピュータは、デジタル証明書を送受信するためのＩ／Ｏインターフェース１１０、新しく計算された証明書を格納するためのメモリ１０９、および新しいデジタル証明書を計算するためのプロセッサを有する。

【００２５】

プロトコルは、いくつかの異なるネットワークコンピュータ環境において使用され得る。図１は、例示的なネットワークアーキテクチャのブロック図である。このようなネットワークは、以下に限定されないが、パーソナルコンピュータ、ワークステーション、小型またはメインフレームコンピュータ、あるいはコンピュータの分散型ネットワークを用いてインプリメントされ得る。コンピュータはまた、専用ハードウエア（暗号コプロセッサ、ルータ等）を含み得る（または使用し得る）。コンピュータはまた、専用ＶＬＳＩゲートまたはフィールドプログラマブルゲートアレイ（ＦＰＧＡ）、あるいは同様の他の技術に基づいて一体型にインプリメントされ得る。簡略化のために、図１におけるネットワークは、プロセッサ、メモリ、および入力／出力インターフェースを用いて構成された汎用（簡略化された）モデルを用いて構成される。これらのコンポーネントは、バスを介して互いに結合される。通信ネットワーク１０１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、非同期転送方法、同期、ダイヤルアップ、分散型の組み合わせを用いて構成され得る。

【００２６】

図２は、本発明の証明書のグループを修正するため１つのシステム内部のメッセージブロック図を示す。ユーザ１１２に対する１つの証明書２０３またはそれ以上の証明書２０４を獲得するために１つの証明書２０１またはそれ以上の証明書２０２に対する開始されたリクエストｘは、ｎ個のサーバＳ（１），．．．，Ｓ（ｎ）（サーバＳ（１），．．．，サーバＳ（ｎ）と表わす）を選択する。各元のサーバ１１５に、リクエストｘ２０２（ｘ（１），．．．，ｘ（ｎ）によって表わされる）が送信される。元のサーバ１１１は、それぞれ証明書Ｃ（１），．．．，Ｃ（ｎ）を用いて返答する。

【００２７】

【数１】

$$1.\ \forall i:\quad U(1) \rightarrow S(i):\ x$$

$$2.\ \forall i:\quad S(i) \rightarrow U(1):\ C(i) = \mathrm{Sign}_{S(i)}\{Ai(x)\}$$

その結果、Ｕ（１）１１２は、証明書２０４のｎ組Ｃ（１），．．．，Ｃ（ｎ）を獲得し、各証明書Ｃ（ｉ）２０３（Ｓ（ｉ）によって発行され、そしてＵ（１）に送信される）は、署名されたメッセージＣ（ｉ）＝$\mathrm{Sign}_{S(i)}\{A_i(x)\}$である。証明書２０３を発行する前に、各サーバは、アイデンティティチェック等のいくつかのさらなるチェック手続を実行し得る。次いで、証明書は、成功チェックの後のみで発行される。証明書のリスト（Ｕ（１）によって獲得され、次いでＵ（２）に転送される）を有する別のユーザＵ（２）１１３は、以下のプロトコルを実行する（その証明書の内の１つは、損傷された可能性がある）。

【００２８】

１：Ｕ（２）：有効な証明書のリストＣ（１），．．．，Ｃ（ｍ）を選択する。

【００２９】
２：Ｕ（２）→Ｒ：Ｃ（１）＝Ｓｉｇｎ$_{Ｓ（１）}$｛Ａ$_{1}$（ｘ）｝，．．．，
Ｃ（ｍ）Ｓｉｇｎ$_{Ｓ（ｍ）}$｛Ａ$_{m}$（ｘ）｝
署名が有効であり、ｘが全てのＡ$_{1}$（ｘ）で同一である場合、
３：Ｒ→Ｕ（２）：Ｃ（ｍ＋１）＝Ｓｉｇｎ$_{Ｒ}$｛Ｆ［Ａ$_{1}$（ｘ），．．．，Ａ$_{m}$（ｘ）］｝
このプロトコルに従って、再生サーバＲ１１４は、Ｃ（１），．．．，Ｃ（ｍ）上の署名ｍを検証する。署名が有効である場合、Ｒ１１４は、計算アルゴリズムに基づいて新しい証明書Ｃ（ｍ＋１）２０７を作成し、通信ネットワーク１０１を介してその証明書をユーザＵ（２）１１３に再送信する。ユーザＵ（２）１１３は、証明書のリストにＣ（ｍ＋１）２０７を追加し、そして、Ｕ（２）１１３は、無効コンポーネントがあった場合、リストからこの無効コンポーネントを除去する。

【００３０】
図３は、本発明の証明書を修正する１つの方法を示すフローチャートである。本方法は、ユーザコンピュータ１１２上に格納される元のサーバ１１１から最初に送信された証明書の内の１つが使用不可能になる場合に使用され得る。鍵が損傷され、証明書がこわされ、または暗号化方式が破壊される場合、証明書は使用不可能になる。本方法は、（１）複数の証明書２０６を含む証明書の最初のリストを受信するステップと、（２）公開鍵３０２を用いて複数の証明書の各々の確実性を検証するステップと、（３）作成アルゴリズム３０３を用いて新しい証明書を計算するステップと、（４）新しい証明書３０４を署名するステップと、（５）証明書のリストを修正するステップと、および（６）修正された場合、リストを新しい証明書３０５に添付するステップとを包含する。ユーザコンピュータ１１３の証明書が使用不可能になる場合、ユーザＵ（２）は、するその証明書を、ステップ（１）、（２）、（３）、および（４）において再生サーバＲ１１４によって計算された新しい証明書を伴い、その証明書を置換するように本発明の方法を開始し得る。本方法はまた、さらなるエレメントを追加することによって署名されたステートメントのリストを拡張するように使用され得る。この場合、ユーザＵ（２）は、構成ステップ（５）および（６）を利用するステップ（１）、（２）、（３）および（４）において再生サーバＲ１１４によって計算されたさらなる証明書を追加するように本発明の方法を開始し得る。

【００３１】
図４は、本発明の証明書のグループを修正するための１つのシステムを示すブロック図である。再生サーバＲ２０６のプロセッサ１０８は、複数（ｍエレメントリスト、ただしｍ＜ｎ）の依然として有効な証明書（Ｃ（１），．．．，Ｃ（ｍ））２０６をユーザコンピュータＵ（２）１１３からリクエストする。再生サーバＲ１１４のプロセッサ１０８は、公開鍵４０２および検証プログラムセグメント４０３のセットを用いて有効な証明書２０６の確実性を検証する。一旦検証される（３０２）と、再生サーバＲ１１４は、作成アルゴリズムＦ４０１を用いて、新しいデジタル証明書を、ユーザコンピュータＵ（２）１１３から受信された１つ以上の有効化された証明書３０２を組み合わせることによって計算する。しかし、作成アルゴリズムＦ４０１は、その再生サーバＲ１１４が新しい証明書を発行しないことを意味するエラー出力を戻し得る。Ｆ４０１は、決定論的であるかまたは確率論的であり得、その出力は、決定論的データに依存し得、そのリストＡ$_{1}$（ｘ），．．．，Ａ$_{m}$（ｘ）は、直接的に含まれない。いくつかの実施形態では、計算アルゴリズムＦは、Ｉ／Ｏデバイスを介して人間とのコンピュータのやり取りをさらに組み込み得る。次に、組み合わせられたステートメント４０４は、秘密鍵４０６を用いて再生サーバによって署名される（４０５）。新しい証明書ｃ（ｍ＋１）２０７が生成され、かつ新しい証明書ｃ（ｍ＋１）２０７は、ユーザコンピュータＵ（２）１１３上の証明書の元のセットの再生または拡張準備状態である。

【００３２】
図５は、本発明の証明書のグループを修正するための方法を詳述する別のブロック図であり、より詳細には、ユーザコンピュータＵ（２）１１４上の古い証明書のリストを更新

することに関する。ユーザコンピュータＵ（２）１１３のプロセッサ１０８は、依然として有効な証明書５０２の複数のｍエレメントリスト（ここで、ｍ＜ｎ）を再生サーバＲ１１４に送信する。証明書Ｃ（１），．．．，Ｃ（ｍ）２０６のｍエレメントリストを受信した後で、再生サーバＲ１１４のプロセッサは、修正手続３０３、３０４を開始する。一旦完了すると、新しいデジタル署名ｃ（ｍ＋１）が生成され、通信ネットワーク１０１を介してユーザコンピュータＵ（２）１１３に再送信する。ユーザＵ（２）１１３は、証明書のリストにＣ（ｍ＋１）を追加し、１１３は、リストから任意の無効コンポーネント５０３を除去する。いくつかの理由のために損傷された古い証明書は、次いで新しい証明書Ｃ（ｍ
＋１）２０７と置換される。リスト中の１つのみの証明書が損傷された場合、再び、新しいリストのｎ個有効なコンポーネント３０５および鍵損傷に対する抵抗が以前の証明書５０１と同じになる。

【００３３】

このセクションでは、再生／拡張手続が有用であるサービスのいくつかの例を提示する。本明細書中で説明するサービスは、（１）デジタルタイムスタンピング、（２）公開鍵証明、（３）デジタル署名サービス、（４）証明書有効化サービス、および（５）電子公証サービスである。

【００３４】

（デジタルタイムスタンピング）

本発明は、デジタルタイムスタンピング実施形態においてインプリメントされ得る。ここで、ステートメント$A_i$（ｘ）は、（ｘ，$t_i$）形態を有し、ここで、$t_i$は、時間／日付を表わし、リクエストｘは、ｉ番目のタイムスタンピングサーバ$TSA_i$によって受信された。サーバは、以下の作成アルゴリズムＦを使用し得る。

【００３５】

【数２】

$$F[(x_1,t_1),\ldots,(x_m,t_m)]=\begin{cases}x_1=\ldots=x_m\text{の場合 }(x_1,\min_k\{t_1,\ldots,t_m\})\\ \text{上記以外の場合、エラー}\end{cases}$$

ここで、$min_k$は、引数のリストのｋ番目の最小エレメントを見出すことを表わす。（ｘ；ｍａｘ｛$t_i$，．．．，$t_m$｝または（ｘ；（$t_i$＋．．．＋$t_m$）／ｍ）等の他の機能はまた、合理的であり得る。なお、時間値$t_i$，．．．，$t_m$が、ある意味で、異なりすぎる場合、または時間値がいくつかの他の（以前に固定された）関係を満足しない場合にＦがエラーに戻すように、Ｆが定義され得る。公開鍵証明書は、公開鍵ｘについてのステートメントＡ（ｘ）を作成するために認可されたサービスである。サービスプロバイダは、しばしば、認証機関（ＣＡ）と呼ばれる。例えば、Ａ（ｘ）は、ｘがアイデンティティ$ID_x$を有する人に属すると言われ得る。この場合、証明書$Sign_{CA}$｛ｘ，$ID_x$｝は、アイデンティティ証明書と呼ばれる。公開鍵証明書の別の例は、公開鍵ｘをアクセス権利$r_x$のリストに関連付ける認可証明書である。第１の場合、Ｆは以下のように定義され得る。

【００３６】

【数３】

$$F[A_1(x_1),\ldots,A_m(x_m)]=\begin{cases}\text{全ての}A_i(x_i)\text{が同一である場合 }A_i(x_i)\\ \text{上記以外の場合、エラー}\end{cases}$$

（証明書有効化サービス）

本発明は、証明書有効化サービスにおいてインプリメントされ得る。これは、デジタル証明書の有効性を証明するサービスである。リクエストを受信すると、そのリクエストは、証明書の識別子ｃ（恐らくシーケンスナンバーまたは暗号ハッシュ）および随意に、公

開鍵に列挙された証明書ｃを用いて生成されたデジタル署名であり得るいくつかのさらなるデータｙを含む。証明書が有効である場合（無効ではない）、サーバは、証明書の識別子ｃおよびリクエストに随意に含まれたさらなるデータｙを含む有効化ステートメントＡ＝（ｃ，ｙ）を署名する。有効化ステートメント$A_i$＝（$c_i$，$y_i$），．．．，$A_m$＝（$c_m$，$y_m$）のリストを有することによって、作成アルゴリズムＦは、公開鍵証明書と同じ態様で定義される。すなわち、

【００３７】

【数４】

$$F[A_1(x_1),\ldots,A_m(x_m)]=\begin{cases}\text{全ての}A_i(x_i)\text{が同一である場合 }A_1(x_1)\\ \text{上記以外の場合、エラー}\end{cases}$$

（デジタル署名サービス）

本発明は、デジタル署名サービスにおいてさらにインプリメントされ得る。このサービスは、ユーザの名前における公開鍵デジタル署名を生成するように認可される。デジタル署名サービスでは、クエリｘは、ユーザによって署名されることが意図されたドキュメントＸの暗号ダイジェストである。クエリは、認証された態様でサーバＳに送信される。すなわち、いくつかのクライアント認証メカニズム（パスワード等）が使用される。ユーザＵが首尾よく認証された場合、Ｓは、返答$Sign_S\{A(x)\}$を生成する。ここで、Ａ（ｘ）は、ユーザのアイデンティティ$ID_U$および暗号ダイジェストｘ含む。リクエストのリスト$A_i(x_i)=(ID_i,x_i),\ldots,A_m(x_m)=(ID_m,x_m)$を入力として有することによって、作成アルゴリズムＦは、公開鍵認証と同じ態様で定義される。すなわち、

【００３８】

【数５】

$$F[A_1(x_1),\ldots,A_m(x_m)]=\begin{cases}\text{全ての}A_i(x_i)\text{が同一である場合 }A_1(x_1)\\ \text{上記以外の場合、エラー}\end{cases}$$

である。

【００３９】

（電子公証サービス）

本発明は、電子公証サービスにおいてインプリメントされ得る。このサービスは、デジタル署名およびタイムスタンプサービスを組み合わせる。ダイジェストｘを認証された態様で獲得した後で、公証サーバＳは、公証ステートメントＡ（ｘ）＝（$ID_U$，ｘ，ｔ）を生成し、ここで、$ID_U$は、ユーザのアイデンティティであり、次いで、ｔは、サーバが時間ソースから獲得する現在の時間である。リクエストのリスト$A_i(x_i)=(ID_i,x_i,t_i),\ldots,A_m(x_m)=(ID_m,x_m,t_m)$を入力とすることによって、関数Ｆが以下のように定義され得る。

【００４０】

【数６】

$$F[(ID_1,x_1,t_1),\ldots,(ID_m,x_m,t_m)]=$$

$$\begin{cases}x_1=\ldots=x_m\text{ かつ }ID_1=\ldots=ID_m\text{ の場合}\\ \qquad(ID_1,x_1,\min_k\{t_1,\ldots,t_m\})\\ \text{上記以外の場合、エラー}\end{cases}$$

特定の実施形態が示されかつ説明されてきたが、多数の改変が本発明の精神から著しく逸脱することなく想起され、保護の範囲は、添付の特許請求の範囲の範囲によってのみ限定

される。

【図面の簡単な説明】

【００４１】

【図１】図１は、コンピュータネットワーク内部にインプリメントされた場合、本発明の証明書のグループを修正するための１つのシステムである。

【図２】図２は、本発明の証明書のグループを修正するための１つのシステム内部のメッセージフローチャートである。

【図３】図３は、本発明の証明書を修正する１つの方法のフローチャートである。

【図４】図４は、本発明の証明書のグループを修正するための１つのシステムのブロック図である。

【図５】図５は、本発明の証明書のグループを修正する１つの方法の別のブロック図である。

【図１】

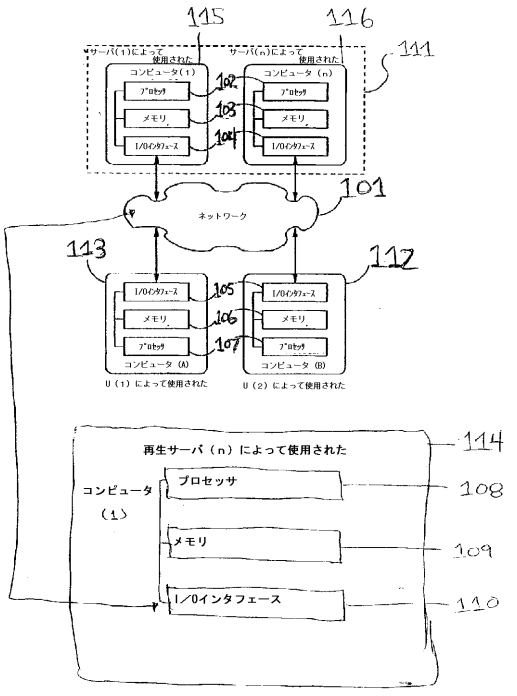



FIGURE 1.

【図２】

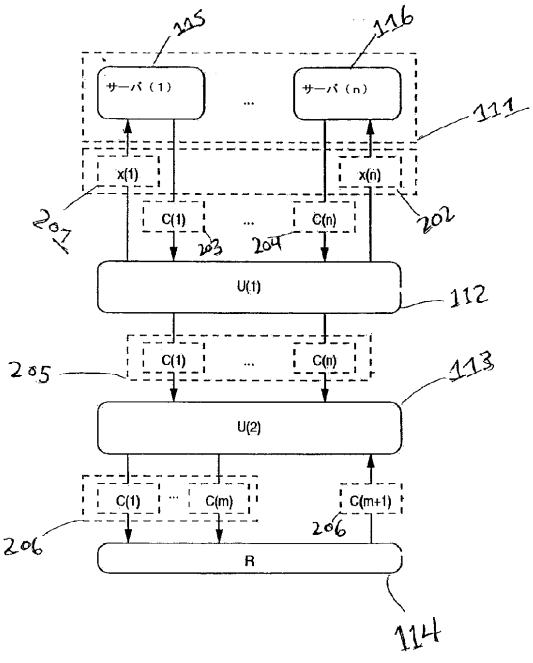



FIGURE 2.

【図３】

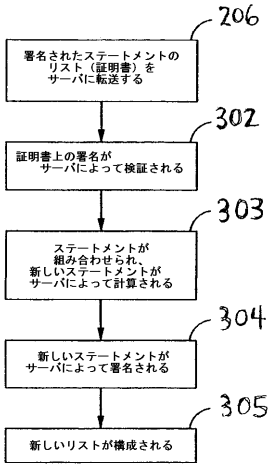



Figure 3.

【図４】

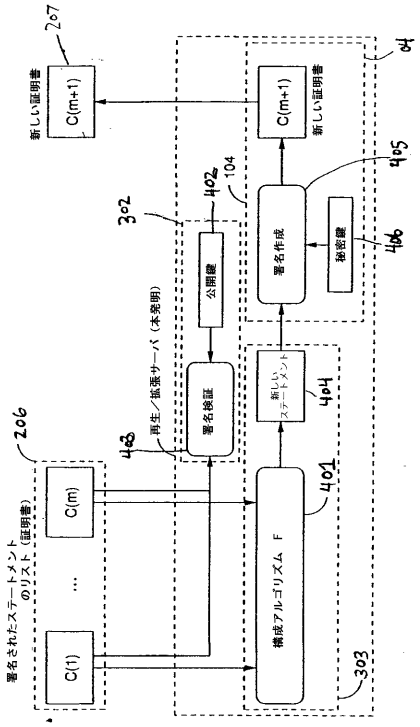



FIGURE 4.

【図５】

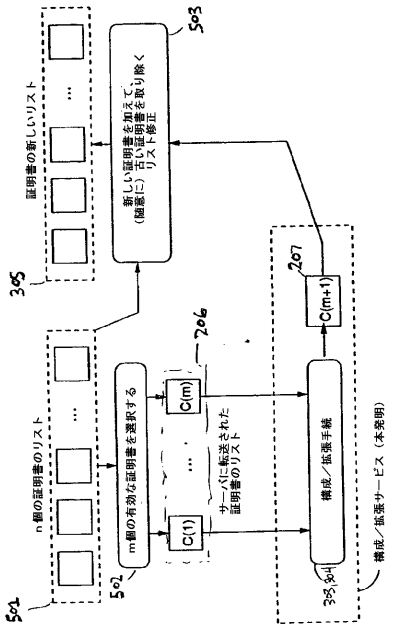



FIGURE 5.

【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。

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/02643

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

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)
IPC 7 H04L G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, INSPEC, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | WO 01 31841 A (VISA INTERNAT SERVICE ASS ;TRENCH TERENCE V (US)) 3 May 2001 (2001-05-03) page 12, line 5 - line 14; figure 2 | 41 |
| Y | US 6 192 130 B1 (OTWAY JOSANNE) 20 February 2001 (2001-02-20) column 4, line 44 - line 59 column 5, line 47 - line 54 | 41 |
| A | column 7, line 36 - line 39 | 1,17,31, 42 |

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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 document 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 |
|---|---|
| 17 February 2003 | 26/02/2003 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Holper, G |

Form PCT/ISA/210 (second sheet) (July 1992)

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 02/02643

| Patent document cited in search report | | Publication date | Patent family member(s) | | Publication date |
|---|---|---|---|---|---|
| WO 0131841 | A | 03-05-2001 | AU | 1654501 A | 08-05-2001 |
| | | | WO | 0131841 A1 | 03-05-2001 |
| US 6192130 | B1 | 20-02-2001 | US | 6317829 B1 | 13-11-2001 |

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(72)発明者　バルダス,　アート
エストニア国　イーイー１２９１５　タリン,　エヒタゲート　ティー　７０－１１３

Ｆターム(参考) 5B085 AA08
5B185 AA08
5J104 AA09　LA03