

【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24年1月19日(2012.1.19)

【公表番号】特表2011-529314(P2011-529314A)

【公表日】平成23年12月1日(2011.12.1)

【年通号数】公開・登録公報2011-048

【出願番号】特願2011-520607(P2011-520607)

【国際特許分類】

H 0 4 L 9/32 (2006.01)

G 0 6 F 21/20 (2006.01)

【F I】

H 0 4 L 9/00 6 7 5 Z

G 0 6 F 15/00 3 3 0 A

【手続補正書】

【提出日】平成23年7月25日(2011.7.25)

【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】

対象物の真正性をデジタル的に証明するための方法であって、

公開鍵と秘密鍵とからなる非対称暗号化鍵対が記憶手段に格納されるように、対象物に固有の少なくとも 1 つの特徴を表したデジタル署名済情報を含んだデジタル真正性証明書を格納した記憶手段を発行する段階（1，2，3，4，5）と、

要求がある度に、ネットワーク演算手段を使用して、デジタル真正性証明書の正当性をチェックする段階（6，7）と、

要求がある度に、前記デジタル真正性証明書の正当性のステータスを修正する段階とを有し、

前記秘密鍵は、前記記憶手段に取り出し不可能なように格納され、

前記ネットワーク演算手段は、前記記憶手段並びに検証局及び／又は認証局と協働して、実質的にリアルタイムで、前記デジタル真正性証明書の正当性のステータスを出力するように構成されることを特徴とする方法。

【請求項 2】

前記記憶手段を発行する段階が、

前記記憶手段上に生成しようとする前記デジタル真正性証明書の発行リクエストを生成する段階（2，3）と、

承認を得るために、前記リクエストを認証局へ送信する段階（4）と、

前記認証局による検証を行い、検証に合格した場合に、前記リクエストにデジタル署名を加える段階と、

署名済リクエストを記憶手段へ送信する段階（5）と、

認証局の承認を含む前記署名済リクエストとの対話によって、前記記憶手段上へのデジタル真正性証明書の生成を完了させる段階と

を有し、

前記リクエストには、前記少なくとも 1 つの固有の特徴を表す情報が含まれることを特徴とする請求項 1 に記載の方法。

【請求項 3】

前記記憶手段上に生成しようとする前記デジタル真正性証明書の発行リクエストを生成する段階が、非対称暗号化鍵対を生成する段階（３）を有し、

前記非対称暗号化鍵対は、公開鍵と、前記記憶手段上の秘密鍵とからなり、

前記秘密鍵に対しては、取り出し不可能となるように前記生成が行われることを特徴とする請求項１又は２に記載の方法。

【請求項４】

前記記憶手段上に非対称暗号化鍵対を生成する段階（３）が、公開鍵暗号化アルゴリズムを使用して実行されることを特徴とする請求項３に記載の方法。

【請求項５】

デジタル真正性証明書の正当性をチェックする段階が、

デジタル真正性証明書を格納した記憶手段を、ネットワーク演算手段を介して、検証局及び／又は認証局に接続する段階（６）と、

前記検証局及び／又は認証局による、デジタル真正性証明書へのアクセス、及び／又は、対象物に固有の少なくとも１つの特徴を表した情報へのアクセスがなされるように、記憶手段と検証局及び／又は認証局とをネットワーク演算手段を介して対話させる段階（７）と、

ネットワーク演算手段を介して、実質的にリアルタイムで、前記デジタル真正性証明書の正当性のステータスを出力する段階と

を有することを特徴とする請求項１ないし４のいずれか１項に記載の方法。

【請求項６】

記憶手段を、ネットワーク演算手段を介して、検証局及び／又は認証局に接続する段階（６）と、記憶手段と検証局及び／又は認証局とをネットワーク演算手段を介して対話させる段階（７）とが、暗号化通信プロトコルであるＴＬＳプロトコル又はＳＳＬプロトコルと、相互認証機能とを使用して実行されることを特徴とする請求項５に記載の方法。

【請求項７】

記憶手段上の前記デジタル真正性証明書の正当性のステータスを修正する段階が、

認証局によって、対象物のステータス情報が受信される段階と、

対象物のステータス情報に対応する項目をデータベース内に生成する段階とを有し、

前記項目は、記憶手段上のデジタル真正性証明書の正当性のチェックが発生する度に、検証局によって読み取られるように構成されることを特徴とする請求項１ないし６のいずれか１項に記載の方法。

【請求項８】

認証局によって、対象物の１つ以上の別の特徴を表した補足情報、又は、当該対象物及び／又は該対象物の所有者及び／又は該対象物の製造者に関する任意の情報が受信される段階と、

リクエストに応じて、前記補足情報の任意の部分を、ネットワーク演算手段を介して出力する段階と

をさらに有することを特徴とする請求項１ないし７のいずれか１項に記載の方法。

【請求項９】

請求項１ないし８のいずれか１項に記載の方法を実行するように構成された、コンピュータ可読記録媒体に格納されたコンピュータプログラム手段。

【請求項１０】

請求項１ないし８のいずれか１項に記載の方法を実現するための記憶手段であって、

対象物の少なくとも１つの特性を表したデジタル署名済情報を含んだデジタル真正性証明書を格納し、

ネットワーク演算手段並びに検証局及び／又は認証局と協働して、検証局及び／又は認証局による前記デジタル真正性証明書の正当性のステータスの出力を許可するように構成されることを特徴とする記憶手段。

【請求項１１】

オンボードで生成された情報、又は、セキュアな手段によって、少なくとも部分的に取り出し不可能にチップに入力された情報を格納する機能を有した、コンピュータプログラム手段及び／又は電子回路手段からなる暗号化スマートチップであることを特徴とする請求項 10 に記載の記憶手段。

【請求項 12】

暗号化スマートチップが、暗号化情報の生成をオンボードで行う機能を有したコンピュータプログラム手段を具備することを特徴とする請求項 11 に記載の記憶手段。

【請求項 13】

暗号化スマートチップが、暗号化スマートカードに埋め込まれたものであることを特徴とする請求項 11 又は 12 に記載の記憶手段。

【請求項 14】

価値を有した対象物の真正性をデジタル的に証明するための、請求項 1 ないし 8 のいずれか 1 項に記載の方法の使用法。

【請求項 15】

価値を有した対象物が、贅沢品である高級腕時計又は宝飾品であることを特徴とする請求項 14 に記載の使用法。