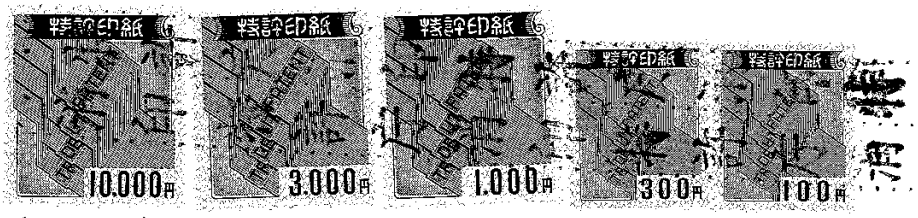
【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年12月2日(2005.12.2)

【公表番号】特表2001-509926(P2001-509926A)
【公表日】平成13年7月24日(2001.7.24)
【出願番号】特願平10-532404
【国際特許分類第７版】
　Ｇ０７Ｆ　 7/10
　Ｇ０６Ｆ　17/60
【ＦＩ】
　Ｇ０７Ｆ　 7/10
　Ｇ０６Ｆ　17/60　　２２２
　Ｇ０６Ｆ　17/60　　５１０
　Ｇ０６Ｆ　17/60　　５１２

【手続補正書】
【提出日】平成17年4月22日(2005.4.22)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】補正の内容のとおり
【補正方法】変更
【補正の内容】



(14,400円)

手 続 補 正 書

平成１７年４月２２日

特許庁長官　殿

１．事件の表示

平成１０年特許願第５３２４０４号 ~~(PCT/CA98/00056)~~

２．補正をする者

名　称　　サーティカム　コープ.

３．代理人

住　所　　〒222-0033神奈川県横浜市港北区新横浜３丁目２０番１２号 望星ビル７階 加藤内外特許事務所

電話（０４５）４７６－１１３１

氏　名　　（８０８１）弁理士　加藤　朝道

４．補正により増加する請求項の数

9

５．補正の対象

明細書全文及び請求の範囲

６．補正の内容

（１）明細書　　別紙の通り

（２）請求の範囲　　別紙の通り

（１）明細書の補正

明細書

[発明の名称]　データカード検証装置

[技術分野]

本発明は、電子取引システムにおいてのデータ転送及び確認のための方法及び装置に、より詳しくは、スマートカードを用いた電子取引システムに関する。

[背景技術]

金融取引もしくは証券の交換のような取引を電子式に行うことは、広く受入れられている。自動化されたテラーマシン（ＡＴＭ）及びクレジットカードは、個人の取引に広く使用されており、その使用が拡大されるのに伴って、かかる取引を検証する必要性も増大してきている。スマートカードは、多少クレジットカードに類似しており、いくらかの演算処理能力及び記憶能力を備えている。スマートカードは、例えば、疑いをもたないユーザーから情報を収集するためのダミー端局などによって不正使用され易い。そのため、端局とスマートカードとの間もしくは逆にスマートカードと端局との間の重要な情報の交換が行われる前に、端局並びにカードの真正さを検証することが必要となる。これらの検証の１つは、取引の真正さが後のセッションに加わる両当事者によって検証されうるように、最初の取引をデジタルに「署名」する形式を取り得る。この署名は、ランダムなメッセージ即ち取引と当事者に関連したシークレットキーとを使用したプロトコルに従って行われる。

署名は、当事者のシークレットキーを定めることができないように行われねばならない。シークレットキーの配分の複雑さをさけるために、署名の発生において公共キー暗号化スキーム（パブリックキー暗号方式）を利用することが好ましい。これらの能力は、比較的大きな計算リソースにアクセスする当事者間で行う場合に使用可能となるが、スマートカードの場合のように計算リソースがより限定されている個人レベルにおいてこれらの取引を容易化することも同様に大切である。

取引カード又はスマートカードは、現在は限られた計算能力と共に利用しうるが、これらは、商業的に存続し得る形で既存のデジタル署名プロトコルを実現す

るには十分ではない。前述したように、検証署名を作成するには、公共キー暗号化スキーム（パブリックキー暗号方式）を利用することが必要となる。現在、多くの公共キースキーム（パブリックキー方式）は、ＲＳＡに基づいているが、ＤＳＳ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ｓｔａｎｄａｒｄ）並びによりコンパクトなシステムに対する需要は、これを急速に変えつつある。ディフィー・ヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）公共キープロトコル（パブリックキープロトコル）を具現したＤＳＳ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ｓｔａｎｄａｒｄ）スキームは、整数Z_pの集合を使用する。ここにｐは大きな素数である。適切なセキュリティのためには、ｐは５１２ビットのオーダーとする必要がある。結果する署名は、減少ｍｏｄ　ｑ（ここにｑは（ｐ－１））を割算し、１６０ビットのオーダーとすることができる。

最初の十分に完成した公共キーアルゴリズム（パブリックキーアルゴリズム）の１つであり、暗号化にもデジタル署名にも役立つ、別の暗号化スキームは、ＲＳＡアルゴリズムである。ＲＳＡは、大きな数を因数分解することの困難さに、そのセキュリティを求めている。公共キー（パブリックキー）及びプライベートキーは、１対の（１００－２００桁又はそれ以上の）大きな素数の関数である。ＲＳＡ暗号化の公共キー（パブリックキー）は、２つの素数ｐ、ｑ（ｐ及びｑは秘密に保つものとする）の積であるｎと、（ｐ－１）×（ｑ－１）に対して比較的に素であるｅとである。従って、暗号化キーｄは、e^{-1}（ｍｏｄ（ｐ－１）×（ｑ－１））である。ここにｄ、ｎは互いに素である。

メッセージｍを暗号化するには、各々の数字ブロックがユニーク表示モジュラス（ｕｎｉｑｕｅ　ｒｅｐｒｅｓｅｎｔａｔｉｏｎ　ｍｏｄｕｌｏ）ｎであるような、複数の数字ブロックに割算する。その場合、暗号化メッセージブロックc_iは単純にm_i^e（ｍｏｄ　ｎ）である。メッセージを解号するには、各々の暗号化ブロックc_iを取り、

$m_i = c_i^d$（ｍｏｄ　ｎ）を計算する。

比較的小さなモジュラス（ｍｏｄｕｌｕｓ）で高いセキュリティを与える別の暗号化スキームは、有限なフィールド2^mにおいて楕円曲線を利用するスキームである。１５５のオーダーのｍの値は、５１２ビットモジュラスＤＳＳと比較可

能なセキュリティを与えるので、実施にとって大きな利点を提供する。

ディフィー・ヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）公共キー暗号化（パブリックキー暗号化）は、ディスクリート・ログ（ｄｉｓｃｒｅｔｅ　ｌｏｇｓ）の性質を利用するので、ゼネレーターβ及びその指数化（ｅｘｐｏｎｅｎｔｉａｔｉｏｎ）β^kが既知でも、ｋの値は定められない。任意の曲線上の２点の和が同じ曲線上の第３の点を生ずる楕円曲線の場合にも同様の性質が存在する。同様に、曲線上の点Ｐに整数ｋを掛算すれば、同じ曲線上に別の点を生ずる。楕円曲線の場合、点ｋＰは、単に点Ｐのコピーｋ個を互いに加算することによって得られる。

しかし、開始点と終点とを知ることによっては、暗号化のためのセッションキーとして次に使用しうる整数ｋの値は明らかにされない。従って、値ｋＰ（Ｐは最初の既知の点）は、指数形β^kと同様である。更に、楕円曲線の暗号化システムは、帯域効率、計算量の減少及び最小コードスペースがアプリケーションの目標である場合に、他のキー暗号化システムに比べて利点を提供する。

更に、スマートカード及び自動化テラーマシン取引の文脈においては、両当事者の確認（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）に、２つの主要なステップが含まれる。第１のステップは、スマートカードによる端局の確認であり、第２のステップは、端局によるスマートカードの確認である。一般に、確認には、端局によって生成されスマートカードによって受信される証明書の検証と、スマートカードによって署名され端局によって検証される証明書の検証が含まれる。２つの証明書が肯定的に検証されたら、スマートカードと端局との間の取引は、継続（続行）することができる。

スマートカードの処理能力は限定されているので、スマートカードによって実行される検証及び署名処理は、一般に、簡単な暗号化アルゴリズムに限定される。よりこみいった暗号化アルゴリズムは、一般に、スマートカードに含まれる処理能力の範囲を超えている。そのため、スマートカードにおいて実現され、比較的セキュリティの高い、署名検証及び発生方法に対する需要が存在する。

［発明の概要］

本発明は、一つの視点においてスマートカードと端局との間のデータの検証方

法を提供することを目的としている。

この視点によれば、電子取引の１対の参加者を検証する方法が提供され、該方法は以下の各工程を含む：即ち第１の参加者から第２の参加者によって受信された情報を、第１の署名アルゴリズムに従って検証する工程と、第２の参加者から第１の参加者によって受信された情報を、第２の署名アルゴリズムに従って検証する工程と、を有し、どちらかの検証が失敗に終った場合には、取引は拒絶されるようにした検証方法が提供される。

第１の署名アルゴリズムは、検証よりも署名において計算上一層困難なアルゴリズムであることができ、また第２の署名アルゴリズムが署名よりも検証において計算上一層困難なアルゴリズムであるようにしてもよい。このような実施の形態においては、ハイレベルのセキュリティを保ちながら、第２の参加者が、比較的低い計算力をもって取引に参加することが可能となる。

別の実施の形態によれば、第１の署名アルゴリズムは、ＲＳＡ型又はＤＳＳ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ｓｔａｎｄａｒｄ）型アルゴリズムに基づいたものであり、第２の署名アルゴリズムは、楕円曲線アルゴリズムに基づいている。

［図面の簡単な説明］

図１ａは、スマートカードと端局とを示す概略図である。

図１ｂは、スマートカード取引システムにおいての検証プロセスの間に生起する一連の事象を示す概略図である。

図２は、特定のプロトコルを示す詳細な模式図である。

［発明を実施するための最良の形態］

図１ａにおいて端局（ターミナル）１００は、スマートカード１０２を受入れるようになされている。通常は、端局中にカード１０２を挿入することによって取引が開始される。次に、図１ｂに示すように、端局とカードとの間の相互の確認が行われる。非常に一般的には、この相互の確認は、「チャレンジーレスポンス」（ｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ）プロトコルに従って行われる。一般に、カードは、端局に情報を転送し、端局１００は、ＲＳＡに基づいたアルゴリズム１１２によって、情報に署名し、次にカード１０２に送られ、カード１

０２は、ＲＳＡに基づいたアルゴリズム１１４によって情報を確認する。カードと端局との間の情報交換（１１６）は、カードによって発生させた情報をも含み、この情報は、ＲＳＡアルゴリズムに従って端局によって署名されるべく端局に送られ、ＲＳＡアルゴリズムを用いて検証されるべくカードに返送される。関連する検証が行われる（１１８）と、別のステップが行われ、このステップでは、情報は、楕円曲線プロトコル１２０を用いて、カードによって署名され、楕円曲線に基づいたプロトコルを用いて端局により検証（１２４）されるべく端局に送られる。同様に、カードと端局との間の情報交換（１２２）は、端局によって発生される情報を含むことができ、この情報は、カードによって署名されるべくカードに送られ、検証されるべく端局に返送される。適正な情報が検証１２６されると、端局とカードとの間の以降の取引が進行可能（１２８）となる。

次に図２を参照すると、「チャレンジーレスポンス」（ｃｈａｌｌｅｎｇｅｄ－ｒｅｓｐｏｎｓｅ）プロトコルによる端局とカードとの相互の確認の詳細な実施形態が、全体として符号２００によって示されている。端局１００は、最初に、カード１０２によって検証され、次にカードが端局によって検証される。端局は、最初に、そのＩＤ、T_{ID}を含む証明書C_I、２０と、公共キー（パブリックキー）を含む公共情報（パブリック情報）とを、カードに送る。証明書２０は、端局から受領した公共キー（パブリックキー）と端局ＩＤ　T_{ID}との関連付けをカードが検証できるように、証明オーソリティないし官庁（ＣＡ）により署名されてもよい。端局とＣＡとによって用いられる、この実施の形態によるキーは、どちらも、ＲＳＡアルゴリズムに基づくことができる。

ＲＳＡアルゴリズムによれば、各々のメンバーないし当事者は、公共キー（パブリックキー）及びプライベートキーをもち、各々のキーは、２つの部分を有する。署名は、

$$S=m^d \pmod{n}$$

を形をもち、ここに、

ｍは署名されるべきメッセージであり、

ｎは公共キー（パブリックキー）であり、モジュラスであり、かつ２つの素数ｐ、ｑの積、

eは、ランダムに選ばれたキーであり、公共キー（パブリックキー）でもあり、（p－1）×（q－1）に対して相対的に素であるように選ばれた数である。

dは、e^{-1}（mod（p－1）×（q－1））に対して一致する（合同な）プライベートキーである。

ＲＳＡアルゴリズムに対して、対の整数（n、e）は、署名のために用いられる公共キー（パブリックキー）情報である。他方では、対の整数（d、n）は、公共キー（パブリックキー）情報（n、e）を用いて暗号化されたメッセージを解号するために使用しうる。

図２に戻って、数n、eは、ＣＡの公共キー（パブリックキー）であり、システムパラメーターとして設定することができる。公共キー（パブリックキー）eは、スマートカード（以下「カード」とも略称）に格納しておいても、また別の実施の形態に従って、カードにおいて、ハード回路の論理回路にしておいてもよい。更に、eを比較的小さい値に選ぶことによって、指数化（ｅｘｐｏｎｅｎｔｉａｔｉｏｎ）が比較的すみやかに実行されることが保証される。

証明書２０C_1は、ＣＡによって署名され、パラメーター（n、e）を有する。証明書は、端局ＩＤ　T_{Id}と端局公共キー（パブリックキー）情報T_n、T_e（ＲＳＡアルゴリズムに基づく）を有する。証明書C_1は、カード抽出T_{ID}、T_n、T_eによって検証（２４）される。この情報は、簡単に、C_1^e mod nを実行することによって抽出される。カードは、次に、ランダムな数Ｒ１を発生（２６）させることによって端局を確認する。これらの数は、カードによって端局に送られる。端局は、$R1^{Te}$ MODT_nを実行することによって、そのシークレットキーT_dを用いて、メッセージＲ１に署名し、値C_2を発生させる（２８）。なお、端局によって使用されるキーは、やはりＲＳＡキーであり、このＲＳＡキーは、公共キー（パブリックキー）T_eがおそらくはシステムワイドであるような、値３を有する小さなパラメーターから成り、公共キー（パブリックキー）の他の部分は、端局に関連されるモジュラス（ｍｏｄｕｌｕｓ）T_nであるように、オリジナルに作り出されたものである。端局プライベートキーT_dは、小さな公共キー（パブリックキー）T_eに対応するものであれば、小さくできない。端局の場合、端局は、指数化（ｅｘｐｏｎｅｎｔｉａｔｉｏｎ）を比較的す

みやかに実行するための計算能力を備えているため、プライベートキーT_dが大きく選ばれることは問題ではない。

端局は、値C_2を計算する（２８）と、ランダムなシークレットナンバーＲ２を発生させ（２９）、端局は、Ｒ２、C_2をカードに送る（３２）。カードは次に端局のｍｏｄｕｌｕｓ　T_nを用いて、小さな指数T_eによって、署名された値C_2に対して、モジュールの指数化（ｍｏｄｕｌａｒ　ｅｘｐｏｎｅｎｔｉａｔｉｏｎ）を実行する（３４）。これは、$R1' = C_2^{Te} \mod T_n$を計算することによって行う。Ｒ１′がＲ１に等しい（３６）と、カードは、そのＩＤT_{ID}がモジュラスT_nに関連（３８）されている端局と取引していることを知る。カードは、一般に、前記の演算を実行するためのモジュール（ｍｏｄｕｌｏ）算術プロセッサー（不図示）を備えている。

ランダムなシークレットナンバーＲ２は、カードによって署名（４０）され、カードＩＤをその公共情報（パブリック情報）に関連付けるＣＡによって署名された証明書と共に、端局に返却される。カードによる署名は、楕円曲線署名アルゴリズムに従って実行される。

カードによる検証は、端局の検証と同様にして行われるが、カードによる署名は、楕円曲線暗号化システムを利用する。

典型的に、楕円曲線で実施の場合について、署名成分ｓは、次の形式を有する。

$$s = ae + k \pmod n$$

ここに、

Ｐは、システムの所定のパラメーターである曲線上の点、

ｋは、短い項（ｔｅｒｍ）のプライベートキー又はセッションキーとして選ばれたランダムな整数であり、対応した短い項の公共キー（パブリックキー）Ｒ＝ｋＰを有する。

ａは、送信側（カード）の長い項のプライベートキーであり、対応する公共キー（パブリックキー）ａＰ＝Ｑを有する。

ｅは、メッセージｍ（この場合Ｒ２）及び短い項の公共キー（パブリックキー）Ｒの確実なハッシュ、例えばＳＨＡハッシュ関数である。

ｎは曲線の次数である。

単純化のために、この署名成分ｓは、前述したようにｓ＝ａｅ＋ｋの形とするが、それ以外の署名プロトコルを用いても差支えない。

署名を検証するには、ｓＰ－ｅＱを計算し、Ｒと比較しなければならない。カードは、例えばフィールド算術演算器（不図示）を用いて、Ｒを発生させる。カードは、図２のブロック（４４）に示したｍ、ｓおよびＲを含むメッセージを端局に送出し、ｋＰに対応するべき値（ｓＰ－ｅＱ）を計算（４６）することによって、端局によって署名を検証する。計算された値が対応すれば（４８）、署名は検証されるので、カードは、検証され、取引は継続（続行）することができる。

端局は、証明書をチェックし、次に、Ｒ２を含む取引データの署名をチェックし、端局に対してカードを確認する。本（第１の）実施形態によれば、カードによって発生させた署名は、楕円曲線署名であり、これは、カードが生成させるのは容易にできるが、端局による検証には、より多くの計算が必要とされる。

以上の式からわかるように、ｓの計算は比較的率直であり、大きな計算力を必要としない。しかし検証を行うには、ｓＰ、ｅＱを得るために多数の点乗算を必要とし、その各々は計算が複雑である。他のプロトコル例えばＭＱＶプロトコル（Ｍｅｎｅｚｅｓ，　Ｑｕ，　Ｖａｎｓｔｏｎｅ　Ｐｒｏｔｏｃｏｌ）は、楕円曲線に基づいて実施された場合、同様の計算を必要とし、計算能力が限られている場合、検証が遅くなる。しかし、一般に端局ではこのようにはならない。

端局及びカードの検証のための特定のプロトコルについて、本発明の実施の形態を以上に説明したが、これ以外のプロトコルも使用可能である。

（２）請求の範囲の補正

請求の範囲

１．第１の署名スキームと楕円曲線暗号を利用し前記第１の署名スキームとは異なる第２の署名スキームとを有し、データ伝送システムを介して行われる電子取引の１対の通信者間で交わされるメッセージの正当性の検証方法において、以下の各工程：

第１の通信者が、前記第１の署名スキームに従って、メッセージに署名し、第１の署名付きメッセージを前記第２の通信者に送る工程、

前記第２の通信者が、前記第１の署名スキームを用いて前記第１の通信者から受信した第１の署名付きメッセージを検証する工程、

前記第２の通信者が、前記第２の署名スキームに従って、メッセージに署名し、第２の署名付きメッセージを前記第１の通信者に送る工程、

前記第１の通信者が、前記第２の署名スキームを用いて前記第２の通信者から受信した前記第２の署名付きメッセージを検証する工程、

どちらかの検証が失敗に終ったときは、前記各通信者が前記電子取引を拒絶する工程、を有するメッセージの正当性の検証方法。

２．前記第１の署名スキームは、検証の場合よりも署名の場合が計算上より困難であり、前記第２の署名スキームは、署名の場合よりも検証の場合の方が計算上より困難であり、それにより、前記取引のセキュリティを保ちながら一方の前記通信者が比較的低い計算力を持って参加することを可能とする請求の範囲第１項記載のメッセージの正当性の検証方法。

３．前記第１の署名スキームがＲＳＡ型スキームである請求の範囲第１項記載のメッセージの正当性の検証方法。

４．前記第１の署名スキームがＤＳＳ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ｓｔａｎｄａｒｄｓ）型スキームである請求の範囲第１項のメッセージの正当性の検証方法。

５．各通信者が、第１の署名スキームと前記第１の署名スキームと異なる第２の署名スキームとを有し、データ伝送システムを介して行われる電子取引の１対の

通信者間で交わされるメッセージの正当性の検証方法において、以下の各工程：

前記第１の通信者が、公共キー（パブリックキー）及び該第１の通信者の識別情報を含む第１の証明書C_1を、前記第２の通信者に送信する工程、

前記第２の通信者が、該第１の証明書C_1を検証し、それから前記公共キー（パブリックキー）及び識別情報を抽出する工程、

前記第２の通信者が、第１チャレンジＲ１を発生させ、該第１チャレンジＲ１を、前記第１の通信者に送信する工程、

該第１の通信者が、前記第１の署名スキームに従って、受信した該チャレンジＲ１に署名し、第２の証明書C_2を発生させる工程、

前記第１の通信者が、第２のチャレンジを発生させ、該第２のチャレンジを、前記第２の証明書C_2と共に、前記第２の通信者に送信する工程、

前記第２の通信者が、前記第１の署名スキームに従って、前記証明書C_2を検証する工程、

前記第２の通信者が、前記第２の署名スキームに従って、前記第２のチャレンジＲ２に署名し、この署名を前記第１の通信者に送信する工程、及び、

前記第１の通信者が、前記第２の署名スキームに従って、前記署名を検証し、前記各証明書又は署名が検証されなかったときは、前記各通信者が前記電子取引を拒絶する工程、を有するメッセージの正当性の検証方法。

６．通信先との電子取引において使用するための、スマートカードであって、メモリを有し、該メモリは、

前記通信先によって第１署名発生アルゴリズムにより行われた署名の検証を実行するための第１署名スキームによる検証アルゴリズムと、

第２署名発生アルゴリズムに従って署名を実行するための、楕円曲線暗号を利用し前記第１署名スキームとは異なる第２署名スキームによる署名アルゴリズムと、

前記各アルゴリズムを呼出すためのプログラムと、

前記検証アルゴリズムを作動させ、前記通信先によって署名された第１のメッセージを検証し、更に、前記署名アルゴリズムを作動させ、第２のメッセージに署名し、前記通信先に送信する演算手段と、

を含む、スマートカード。

７．前記検証アルゴリズムがＲＳＡ署名を検証する請求の範囲第６項記載のスマートカード。

８．前記検証アルゴリズムがＤＳＳ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ｓｔａｎｄａｒｄｓ）署名を検証する請求の範囲第６項記載のスマートカード。

９．第１の署名スキームと楕円曲線暗号を利用し前記第１の署名スキームとは異なる第２の署名スキームとを有し、データ伝送システムを介して行われる電子取引の第１の通信者から第２の通信者に送信されるデータストリームであって、

ａ）前記第２の署名スキームに従って、前記第１の通信者によって署名された第１の値と、

ｂ）前記第１の署名スキームに従って、認証オーソリティによって署名された証明書と、を含み、

前記第２の通信者が、前記証明書になされた署名を検証することによって、前記第１の値になされた署名を検証するデータストリーム。

１０．前記第１の署名スキームは、検証の場合よりも署名の場合が計算上より困難であり、前記第２の署名スキームは、署名の場合よりも検証の場合の方が計算上より困難であり、それにより、前記取引のセキュリティを保ちながら一方の前記第１の通信者が比較的低い計算力を持って参加することを可能とする請求の範囲第９項記載のデータストリーム。

１１．前記第１の署名スキームがＲＳＡ型スキームである請求の範囲第９項記載のデータストリーム。

１２．請求の範囲第９項記載のデータストリームから、公共キー暗号システム（パブリックキー暗号システム）の証明書を生成する方法であって、

ａ）楕円曲線暗号方式で通信者によって使用される公共情報を取得する工程、

ｂ）前記通信者によって使用される公共情報にＲＳＡ暗号方式を用いて署名する工程、を含む、証明書生成方法。

１３．前記通信者によって使用される情報は、楕円曲線暗号方式の公共キー（パブリックキー）を含む請求の範囲第１２項記載の証明書生成方法。

１４．請求の範囲第９項記載のデータストリームを包含する公共キーシステム（パブリックキーシステム）の証明書であって、

ａ）楕円曲線暗号方式で署名を生成するために用いられる公共情報と、

ｂ）ＲＳＡ暗号方式によって前記ａ）の公共情報になされる署名と、を含む、証明書。

１５．前記ａ）の情報は、楕円曲線暗号方式の公共キー（パブリックキー）を含む請求の範囲第１４項記載の証明書。