(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-5712
(P2017-5712A)
(43)公開日　平成29年1月5日(2017.1.5)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/10	(2006.01)	H04L	9/00	621A	5J104
H04L	9/32	(2006.01)	H04L	9/00	675B	
G06F	21/44	(2013.01)	G06F	21/44		

審査請求 有　請求項の数 12　OL　外国語出願　（全 13 頁）

(21)出願番号　特願2016-115969 (P2016-115969)
(22)出願日　平成28年6月10日 (2016.6.10)
(31)優先権主張番号　15171811.1
(32)優先日　平成27年6月12日 (2015.6.12)
(33)優先権主張国　欧州特許庁 (EP)

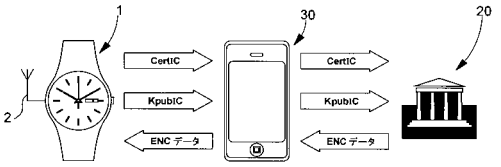
（特許庁注：以下のものは登録商標）
１．ブルートゥース
２．ＪＡＶＡ

(71)出願人　596162740
イーエム・ミクロエレクトロニク－マリン・エス　アー
スイス国・シイエイチ　２０７４・マリン・リュ　ドソル・３
(74)代理人　100098394
弁理士　山川　茂樹
(74)代理人　100064621
弁理士　山川　政樹
(72)発明者　ステファニー・サルガド
スイス国・２５２０・ラ　ヌーヴヴィル・レシール・４

Ｆターム(参考)　5J104 AA07 AA16 AA32 EA01 EA04 EA08 EA18 EA19 JA03 JA21 KA02 MA01 NA02 NA37 NA38 NA41 PA01 PA13

(54)【発明の名称】腕時計の集積回路に銀行データをプログラミングする方法

(57)【要約】　（修正有）
【課題】完全なプログラミングの安全性を保障し、腕時計の特定用途向け集積回路に銀行データなどの秘密または機密データをプログラミングする。
【解決手段】腕時計１（携帯品）の集積回路に銀行データを非対称暗号化および復号化アルゴリズムを用いてプログラミング可能とするため、集積回路の公開鍵および集積回路の公開鍵および認証局の秘密鍵に基づいて認証局によって生成されるデジタル証明書を、携帯品から銀行２０に送信するステップと、デジタル証明書を銀行において認証局の公開鍵によって検証するステップと、デジタル証明書が承認される場合は、携帯品の所有者に個別化される秘密または機密データを銀行から携帯品に送信するステップと、集積回路の秘密鍵によって、携帯品の所有者に個別化された復号化された秘密データを記憶するために、携帯品の特定用途向け集積回路によって受信された暗号化されたデータを復号化するステップと、で処理する。
【選択図】図３



【特許請求の範囲】
【請求項１】
銀行データなどの秘密または機密データを腕時計などの（１）携帯品の特定用途向け集積回路（３）にプログラミングする方法であって、データのプログラミングのために非対称暗号化／復号化アルゴリズムを用いる方法であって、
前記方法は、
－前記集積回路（３）の公開鍵（ＫｐｕｂＩＣ）と、前記集積回路の公開鍵および認証局の秘密鍵（ＫｐｒｉｖＡＣ）に基づいて前記認証局によって生成されるデジタル証明書（ＣｅｒｔＩＣ）とを、前記携帯品（１）から銀行（２０）または金融機関または銀行機関に送信するステップと、
－前記デジタル証明書（ＣｅｒｔＩＣ）を前記銀行（２０）または前記金融機関もしくは銀行機関で前記認証局の公開鍵（ＫｐｕｂＡＣ）によって検証するステップと、
－前記デジタル証明書が承認される場合は、前記携帯品（１）の所有者に個別化され、暗号化された秘密または機密データを前記銀行（２０）または前記金融機関もしくは銀行機関から前記携帯品（１）に送信するステップと、
－前記集積回路（３）の秘密鍵（ＫｐｒｉｖＩＣ）によって、前記携帯品（１）の前記所有者に個別化され、前記復号化された秘密または機密データを記憶するために、前記携帯品（１）の前記特定用途向け集積回路（３）によって受信された前記暗号化されたデータを復号化するステップと、
を含むことを特徴とする、方法。
【請求項２】
請求項１に記載のプログラミング方法であって、前記集積回路（３）は、前記携帯品所有者の銀行（２０）または金融機関もしくは銀行機関とデータ信号を送受信するために前記携帯品（１）のアンテナ（２）に接続し、前記集積回路（３）の前記公開鍵（ＫｐｕｂＩＣ）および前記デジタル証明書（ＣｅｒｔＩＣ）の前記送信は通信端末（３０）によって実現され、前記暗号化された秘密または機密データの前記銀行（２０）または前記金融銀行機関からの前記受信は、前記携帯品（１）の前記集積回路（３）に接続する前記アンテナ（２）によって前記通信端末（３０）経由で実現されることを特徴とする、方法。
【請求項３】
請求項２に記載のプログラミング方法であって、ＮＦＣプロトコルを用いる短距離通信は前記携帯品（１）と前記通信端末の間で確立され、前記通信端末は通信トンネルとして機能する携帯電話（３０）である、方法。
【請求項４】
請求項１に記載のプログラミング方法であって、前記集積回路の前記秘密鍵（ＫｐｒｉｖＩＣ）および公開鍵（ＫｐｕｂＩＣ）、ならびに前記デジタル証明書（ＣｅｒｔＩＣ）は、前記公開鍵（ＫｐｕｂＩＣ）および前記デジタル証明書（ＣｅｒｔＩＣ）を送信する前記ステップの前に、一時的に前記集積回路の不揮発性メモリ（３）に記憶され、受信された前記暗号化データが復号化されて前記集積回路メモリに記憶されると、前記集積回路の前記秘密鍵（ＫｐｒｉｖＩＣ）および公開鍵（ＫｐｕｂＩＣ）、ならびに前記デジタル証明書（ＣｅｒｔＩＣ）は前記メモリから削除されることを特徴とする、方法。
【請求項５】
請求項１に記載のプログラミング方法であって、前記デジタル証明書の検証後に、前記銀行（２０）または前記金融機関もしくは銀行機関は前記携帯品の前記所有者の銀行口座に関する銀行データを暗号化する、方法。
【請求項６】
請求項１に記載のプログラミング方法であって、前記方法は、
－前記集積回路（３）に特有の秘密鍵（ＫｐｒｉｖＩＣ）および公開鍵（ＫｐｕｂＩＣ）を前記集積回路の製造中または前記携帯品（１）の製造施設において生成する予備ステップと、
－前記集積回路（３）の公開鍵（ＫｐｕｂＩＣ）を前記認証局に送信して、前記デジタ

ル証明書（ＣｅｒｔＩＣ）を前記認証局の秘密鍵（ＫｐｒｉｖＡＣ）に基づいて算出する予備ステップと、
－前記デジタル証明書（ＣｅｒｔＩＣ）を前記集積回路（３）または前記携帯品（１）の前記製造者に送信し、前記特定用途向け集積回路を前記秘密および公開鍵ならびに前記デジタル証明書などの一時的なデータで個別化し、その後前記集積回路（３）の前記公開鍵（ＫｐｕｂＩＣ）および前記デジタル証明書（ＣｅｒｔＩＣ）を前記銀行（２０）または前記金融機関もしくは銀行機関に送信する予備ステップと、
を含む、方法。
【請求項７】
請求項１に記載のプログラミング方法であって、前記方法は、
－前記認証局の秘密鍵（ＫｐｒｉｖＡＣ）および公開鍵（ＫｐｕｂＡＣ）を生成する予備ステップと、
－前記認証局の前記公開鍵（ＫｐｕｂＡＣ）を銀行（２０）に送信する予備ステップと、
－前記認証局の前記秘密鍵（ＫｐｒｉｖＡＣ）および公開鍵（ＫｐｕｂＡＣ）を安全ユニットに記憶する予備ステップと、
を含む、方法。
【請求項８】
銀行データなどの秘密または機密データ用の特定用途向け集積回路（３）を備える携帯品（１）であって、請求項１～７のいずれか１つに記載のプログラミング方法にしたがって個別化およびプログラミングされる前記携帯品はまた、前記集積回路（３）に接続するアンテナ（２）を備え、前記アンテナ（２）は前記データ信号の送受信のための通信インタフェースを備え、前記集積回路（３）はプロセッサ演算装置と、オペレーティングシステムと、前記携帯品の前記所有者に特有の秘密および機密データを記憶するためのメモリとを備えることを特徴とする、携帯品。
【請求項９】
請求項８に記載の携帯品（１）であって、携帯品は腕時計ケース内部にアンテナを備える腕時計であり、前記アンテナは前記集積回路（３）の前記通信インタフェースに接続することを特徴とする、携帯品（１）。
【請求項１０】
請求項８に記載の携帯品（１）であって、前記集積回路（３）の前記通信インタフェースは、通信端末（３０）を通じ、銀行（２０）または金融機関もしくは銀行機関までの通信を確立するために、短距離通信インタフェース（ＮＦＣ）であることを特徴とする、携帯品（１）。
【請求項１１】
請求項８に記載の携帯品（１）であって、前記集積回路（３）はメモリに前記集積回路の前記秘密鍵（ＫｐｒｉｖＩＣ）および公開鍵（ＫｐｕｂＩＣ）と、前記集積回路のデジタル証明書（ＣｅｒｔＩＣ）とを一時的に記憶するように構成され、プログラミング後に、前記秘密または機密データは前記不揮発性メモリにロックされることを特徴とする、携帯品（１）。
【請求項１２】
請求項１０に記載の携帯品（１）であって、前記携帯品（１）は時間および日付の従来の設定用の少なくとも１つのプッシュボタン（４）、または短距離通信（ＮＦＣ）のための前記集積回路を起動するために用いられる少なくとも１つのプッシュボタン（４）を含むことを特徴とする、携帯品（１）。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、特に支払い取引を成立させるために、腕時計などの携帯品の特定用途向け集積回路において、銀行データなどの秘密または機密データをプログラミングする方法に関

連する。
【０００２】
本発明はまた、本プログラミング方法に従って個別化およびプログラミングされた銀行データなどの秘密または機密データのための特定用途向け集積回路を備える腕時計などの携帯品に関連する。
【背景技術】
【０００３】
複数の機能を実施可能な接続した携帯品が既知である。一般に、これらは通信モジュールを備える携帯電話であってもよい。携帯電話はＷｉｆｉプロトコル、ブルートゥースプロトコル、またはＮＦＣプロトコルなどの複数の通信プロトコルを使用することができる。これらの携帯電話を用いて、次に非接触型決済、電子チケットまたは非接触アクセスなどのいわゆる「接続した」機能を実施する。
【０００４】
物品またはサービスの支払いのために、個別化された安全なスマートカードもまた携帯品として使用されてもよい。スマートカードは、物品またはサービスを提供する場所の読み取り装置を備えるアンテナを通じたＮＦＣ短距離通信用の手段を備えていてもよい。ＮＦＣプロトコルを用いる短距離通信は、一般に前述のスマートカードに記憶された銀行データの検証操作を実施し、その後所望する物品またはサービスに対する支払いを実施するために用いられる。
【０００５】
図１に示すように、物品またはサービスの支払いのために用いられる各スマートカード１’は、製造時にスマートカード製造者１０によって個別化され、銀行機関２０によって認識され、認証されなければならない。このように認識されたカードの製造者は、たとえば、オベルチュール社、ジェムアルト社またはＧ＆Ｄ社である。本人証明または個人識別、銀行口座番号などの銀行データは、安全性の高い環境でスマートカードに搭載されなければならない。
【０００６】
この銀行データはカード製造者１０がカード保有者の銀行または金融機関もしくは銀行機関２０から受信する。スマートカードチップは一般に、たとえばＮＸＰまたはインフィニオンなどの、特定用途向けチップ製造者においてユーロカード、マスターカードまたはビザから認証を受けなければならない。カード保有者および銀行の両方は、カード製造者１０の製造施設でカードが製造されるときには既知である。銀行データはこのように、カード製造者の施設でカードが製造されるときにチップに搭載される。最終的に、製造されたカードは次に、カード１’のカード保有者に個人の銀行データすべての本人証明とともに送付される。
【０００７】
図２に例示するように、別の種類の接続した対象は腕時計１であってもよい。腕時計１もまた非接触型決済に用いてもよい。この腕時計１は支払い機能用のチップまたは特定用途向け集積回路を含む。支払いチップは銀行機関２０によって提供され、サポート上に配置されてもよく、その後サポートは製品内の特定のハウジング内に挿入される。またはブランクのチップを製品内部に直接配置して、その後銀行機関２０によってプログラミングしてもよい。
【０００８】
チップはＮＦＣ短距離通信手段を備えていてもよく、またはデータの送受信用のアンテナ２と併せてインタフェースを備えていてもよい。この腕時計１のブランクのチップをプログラミングするために、対称または非対称暗号化／復号化アルゴリズムを用いて、チップにプログラミングすべき口座を所有する口座所有者の銀行２０と通信することができる。
【０００９】
対称暗号化／復号化の事例では、チップメモリは、一式の秘密鍵を含んでいてもよい。

これらの秘密鍵は暗号化／復号化データ、整合性または身元検証データおよび外部ユーザを認証するためのデータである。外部ユーザは腕時計であってもよい。金融機関または銀行機関２０は腕時計チップに記憶された認証データに基づいて直ちに腕時計を認証する。腕時計が一度認証されると、金融機関または銀行機関２０は銀行データを暗号化し、身元照会および暗号化／復号化データを再び対称アルゴリズム（ＤＥＳ（データ暗号化標準）またはＡＥＳ（次世代暗号化標準））を用いて検証する。その後、暗号化データを腕時計チップに送信する。

【００１０】

ＮＦＣ短距離通信は腕時計によって行われるため、中長距離通信端末も使用しなければならない。この通信端末または手段は携帯電話３０であってもよく、ＮＦＣプロトコルを用いて通信するために腕時計の近くに配置される。銀行２０によって暗号化される銀行データＥＮＣはこのように通信電話３０を経由し、その後腕時計１によって受信される。最終的に、暗号化データＥＮＣを受信した腕時計１のチップは、データＥＮＣを復号化および記憶可能である。

【００１１】

チップを対称暗号化でプログラミングする際の問題の一つは、銀行および腕時計が秘密鍵を共有可能な方法を知ることである。製造時に、腕時計にとってまだ銀行は未知である。したがって、鍵をエンドユーザの銀行だけに送信することはできず、すべての銀行に配布するため、これが欠点となる。

【００１２】

非対称暗号化／復号化の事例では、腕時計１のチップメモリは一時的なデータを保存する。一時的なデータは公開鍵に関連する秘密鍵であり、すべての銀行２０に送信される。銀行から、たとえば（発明者のロナルド・リベスト（Ｒｏｎａｌｄ　Ｒｅｖｅｓｔ）、アディ・シャミア（Ａｄｉ　Ｓｈａｍｉｒ）およびレオナルド・エーデルマン（Ｌｅｏｎａｒｄ　Ａｌｄｅｌｍａｎ）の頭文字から由来する）ＲＳＡタイプの非対称暗号化および復号化アルゴリズムを用いることができる。銀行は銀行口座所有者に特有の銀行データを、腕時計１のチップの公開鍵で暗号化してから、この暗号化データＥＮＣを送信する。

【００１３】

前述したように、ＮＦＣ短距離通信は腕時計によって行われるため、携帯電話３０などの中長距離通信端末も使用しなければならない。銀行が暗号化する銀行データはしたがって、通信電話３０を経由してから腕時計１に受信される。最終的に、暗号化データＥＮＣを受信する腕時計１のチップはデータＥＮＣを秘密鍵によって復号化し、腕時計所有者に特有の銀行データを不揮発性メモリに記憶可能である。この銀行データもまたチップにロックされてもよい。

【００１４】

非対称暗号化を用いて銀行データを腕時計チップにプログラミングする方法を実施するときに、銀行は公開鍵のみを知っていることになり、それが有利であることに留意されたい。ただし、個別化すべきすべての腕時計チップの公開鍵を備えるデータベースを有することが必要である。このデータベースは、個別化すべき腕時計チップの数によっては非常に大きくなることもある。さらに、携帯電話などの通信端末を用いることを考慮すると、このような銀行データのプログラミングに必要な安全性のすべてが欠けており、これらが欠点である。

【００１５】

非対称暗号化の使用に関して類似しているものとして、特許文献１に言及する。同特許では、偽造から保護するために、腕時計などの対象物のデジタル証明書を認証する方法が記載されている。デジタル証明書は非対称暗号化のためにチップに記憶されている公開および秘密鍵を生成することによって得られる。証明および／または検証の権限も高級腕時計の信憑性を確認するために設けられる。ただし、物品またはサービスの非接触型決済で用いるための腕時計チップを安全にプログラミングする措置はない。

【先行技術文献】

【特許文献】
【００１６】
【特許文献１】スイス国特許第６９９０８３号
【発明の概要】
【００１７】
したがって本発明の目的は、ノンセキュアな環境において完全なプログラミングの安全性を保証しながら、腕時計の特定用途向け集積回路に銀行データなどの秘密または機密データをプログラミングする方法を提供することによって、前述の従来技術の欠点を克服することである。腕時計の特定用途向け集積回路をアンテナとともにプログラミングすることによって、具体的には、支払い取引を実施することが可能となる。
【００１８】
そのために、本発明は銀行データなどの秘密または機密データを腕時計の特定用途向け集積回路にプログラミングする方法に関連する。本方法は独立請求項１に規定する特徴を含む。
【００１９】
本プログラミング方法の具体的なステップを従属請求項２から７に規定する。
【００２０】
本プログラミング方法の１つの有利点は、集積回路に特有のデジタル証明書を検証し、腕時計から前述の集積回路の公開鍵を持つ機関に送信後に、暗号化データは金融機関または銀行機関から送信可能であるという事実にある。暗号化データの銀行機関から腕時計の集積回路またはチップへの送信は、集積回路の固有なプログラミングの安全性を損なうことなくノンセキュアな通信端末を経由することができる。集積回路はデータを記憶するために暗号化データを秘密鍵で復号化することができる。これは特定用途向け集積回路を備える腕時計を用いて、物品またはサービスの非接触型決済を短距離通信において特定用途向け読み取り装置を用いて行うことができることを意味する。
【００２１】
本プログラミング方法の有利点は、暗号化データを送信する企業を知る必要がないということである。なぜなら、このデータは、データ暗号化に用いた公開鍵と関連する腕時計所有者の秘密鍵によってのみ復号化することができるためである。さらに、デジタル証明書の検証は金融機関または銀行機関において認証局からの公開鍵を用いて実施される。認証局は、認証局の秘密鍵および腕時計集積回路の公開鍵に基づいて、腕時計集積回路のデジタル証明書を生成した。
【００２２】
本発明の目的は、本プログラミング方法により個別化およびプログラミングされた銀行データなどの秘密または機密データのための特定用途向け集積回路を備える腕時計などの携帯品を提供することでもある。
【００２３】
そのために、本発明は、本プログラミング方法によりプログラミングされた銀行データなどの秘密または機密データのための特定用途向け集積回路を備え、独立請求項８に規定する特徴を含む、携帯品に関連する。
【００２４】
本携帯品の特定の実施形態は従属請求項９から１２に規定される。
【図面の簡単な説明】
【００２５】
秘密または機密データを腕時計などの携帯品の特定用途向け集積回路にプログラミングする方法およびこの特定用途向け回路を備える携帯品の目的、有利点および特徴は、図に例示する少なくとも１つの非限定的な実施形態に基づいて以下の説明により明白に示されるであろう。
【００２６】
【図１】従来技術における、スマートカードを銀行データで個別化する前述の標準的な方

法を概略的に表す。
【図２】従来技術における、腕時計チップを銀行データで個別化する前述の標準的な方法を概略的に表す。
【図３】本発明による金融機関または銀行機関からの銀行データなどの秘密または機密データを個別化した様式で、腕時計などの携帯品の特定用途向け集積回路にプログラミングする方法を概略的に表す。
【図４ａ】本発明のプログラミング方法を用いて取得するプログラミング前後の支払い取引用の特定用途向けまたは専用集積回路を備える腕時計を表す。
【図４ｂ】本発明のプログラミング方法を用いて取得するプログラミング前後の支払い取引用の特定用途向けまたは専用集積回路を備える腕時計を表す。
【図５】本発明による腕時計の特定用途向け集積回路をプログラミングする方法の様々なステップを表す。
【発明を実施するための形態】
【００２７】
以下の説明では、当業者には周知である秘密または機密データを携帯品にプログラミングするために用いるすべての前述の手段は簡略化した様式でのみ記載する。強調する点は主に、秘密または機密データを携帯品のチップまたは集積回路に非対称暗号化および復号化技法を用いてプログラミングすることである。
【００２８】
図３は、秘密または機密データを腕時計１などの携帯品の特定用途向け集積回路にプログラミングするための様々な要素を概略的に表す。図４ａ、４ｂおよび５を参照して下記により詳細に説明するように、腕時計１のチップまたは特定用途向け集積回路は、少なくとも一時的に、秘密鍵ＫｐｒｉｖＩＣをプログラミングする前に、関連する公開鍵ＫｐｕｂＩＣおよび回路ＣｅｒｔＩＣのデジタル証明書を記憶することができる。このデジタル証明書は、デジタル署名と同様に、腕時計チップの公開鍵および認証局の秘密鍵ＫｐｒｉｖＡＣに基づいて認証局が生成することができる。認証局はたとえばスウォッチグループなどの携帯品、特に腕時計の製造会社であってもよい。
【００２９】
銀行データなどの秘密または機密データをプログラミングするために、腕時計１などの携帯品は、デジタル証明書ＣｅｒｔＩＣおよび集積回路ＫｐｕｂＩＣの公開鍵を、アンテナ２を経由して、ＮＦＣ短距離通信プロトコルを用いて送信する。アンテナは腕時計ベゼル下の腕時計ケースに配置されてもよく、ダイヤルの直径または腕時計ケース中間部の直径に近い直径の複数の同軸コイルを含んでいてもよい。
【００３０】
ＮＦＣ短距離通信は腕時計から行われるため、携帯電話３０などの長距離端末または手段を通過しなければならない。携帯電話３０は非依存性であり、通信トンネルとして機能する。携帯電話が備える機能によって、約３０ｃｍの距離までの腕時計との無線接触が自動的に確立されてもよい。通信はまた、携帯電話３０と携帯品所有者が少なくとも１つの銀行口座を持っている銀行機関２０との間にも確立される。
【００３１】
腕時計に特有のデジタル証明書ＣｅｒｔＩＣおよび集積回路公開鍵ＫｐｕｂＩＣを受信すると、金融機関または銀行機関２０はまず、デジタル証明書を認証局公開鍵ＫｐｕｂＡＣによって検証する。デジタル証明書の検証が認められると、腕時計１などの携帯品の公開鍵は承認される。特に銀行口座所有者の秘密または機密データは腕時計１の公開鍵ＫｐｕｂＩＣによって暗号化される。この暗号化データＥＮＣは金融機関または銀行機関２０から送信される。データＥＮＣはまず携帯電話３０によって受信され、腕時計１のアンテナ２を経由して腕時計の特定用途向け集積回路に送信される。
【００３２】
暗号化データＥＮＣを受信すると、腕時計１の特定用途向け集積回路はデータＥＮＣを少なくとも一時的にメモリに記憶された秘密鍵ＫｐｒｉｖＩＣによって復号化することが

できる。腕時計所有者の口座に関する銀行データなどの秘密または機密データはメモリ、好ましくは不揮発性メモリに記憶可能であり、おそらくメモリにロック可能である。

【００３３】

腕時計所有者の個人データが特定用途向け集積回路に記憶されると、腕時計アンテナ２に接続した集積回路を非接触型決済に用いることができる。非接触型決済はＮＦＣ短距離通信を用いて、特定の場所または物品もしくはサービスを販売する店舗の読み取り装置によって行われる。秘密データ検証は読み取り装置によって、腕時計１の所有者の銀行との通信を通じて実施される。

【００３４】

認証局、たとえばスウォッチ社の公開鍵は、スウォッチグループのパートナーである銀行または金融もしくは銀行機関にのみ配布することができることに留意されたい。このような事例では、個別化された銀行データを製造後に中間通信端末を通じて腕時計１に送付することができる。中間通信端末は通信トンネルとして機能する非依存性の携帯電話３０である。

【００３５】

集積回路識別コードなどの別のデータも認証することができる。集積回路識別コードはＥＭＶ認証（ユーロカード－マスターカード－ビザ）であってもよい。腕時計１の所有者の銀行データを保護することに加えて、これによって、腕時計の特定用途向け集積回路を特定することもでき、たとえば、この集積回路の製造者を認証することもできる。これらの特徴によって、腕時計が実際にオリジナルのスウォッチ腕時計であることが保証される。秘密データのみが腕時計の特定用途向け集積回路の安全なメモリにある。したがって、ハッキングされるデータベースはない。

【００３６】

携帯品１は図４ａおよび４ｂには簡略化した様式で表される。この携帯品は好ましくは腕時計１である。ただし、所有者特定集積回路がＮＦＣ短距離通信手段とともに挿入することができれば、ブレスレット、ネックレス、または指輪でさえも携帯品として考案可能である。

【００３７】

図４は腕時計１の簡略化した上面図を示す。腕時計１には、腕時計ケース内部にまだ腕時計所有者に個別化されていない集積回路３が配置される。この集積回路３はアンテナ２に周知のＮＦＣ通信インタフェースによって接続する。プッシュボタン４またはクラウンを設けて、従来の時間および日付を設定するために、またはＮＦＣ短距離通信の集積回路を起動するために用いてもよい。ただし、通信の開始も短距離に配置される携帯電話によって自動的に制御されてもよい。

【００３８】

集積回路は、ハードウェア部分に、ＮＦＣ通信インタフェース（ＲＦ）、プロセッサ演算装置および不揮発性メモリであってもよいメモリを備えていてもよい。集積回路はまた、ソフトウェア部分に、Ｊａｖａ仮想マシン、オペレーティングシステム、第１の銀行用アプリケーション、たとえばビザ、マスターカードまたはユーロカード、第２の銀行用アプリケーションおよびその他の可能性のあるアプリケーションを備えていてもよい。オペレーティングシステムは、すべての基本的なソフトウェア機能、ハードウェア部分とのインタフェース、周辺装置およびメモリの管理を実装することができる。

【００３９】

非対称アルゴリズムを開始するための集積回路に特有の秘密鍵ＫｐｕｂＩＣ、ＫｐｒｉｖＩＣ、ＣｅｒｔＩＣは不揮発性メモリに記憶されることに留意されたい。これらの鍵は一時的に記憶され、その後本発明によるプログラミング方法の最後に集積回路の恒久的なプログラミングまたは個別化を行う。

【００４０】

図４ｂは腕時計１の簡略化した上面図を示す。腕時計１には、腕時計ケース内部に、本発明によるプログラミング方法の最後に腕時計所有者に個別化される集積回路３が配置さ

れる。集積回路３がアンテナ２を経て、暗号化データＥＮＣのＲＦ信号を腕時計所有者の銀行から受信すると、データ復号化は記憶された秘密鍵ＫｐｒｉｖＩＣｐを用いて実施される。復号化された秘密または機密データは恒久的に不揮発性メモリに記憶可能である。この秘密データは腕時計所有者の氏名、秘密鍵および銀行口座番号であってもよい。秘密データをロックする前に、秘密および公開鍵ならびにデジタル証明書をメモリから削除することも考案可能である。銀行データを腕時計所有者に個別化すると、集積回路３を備え、アンテナ２に接続する腕時計１を用いて、特定の場所または店舗の読み取り装置と通信することによって、製品またはサービスに対して非接触型決済を行うことができる。

【００４１】

図５は、好ましくは腕時計１である携帯品の特定用途向け集積回路の秘密または機密データをプログラミングする方法の様々なステップを概略的に表す。下記のステップ１１０から１１８は本発明によるプログラミング方法の基本的なステップを構成し、これのみで本発明の範囲を画定するのに十分であってもよい。

【００４２】

特定用途向け集積回路を秘密または機密データでプログラミングする前に、認証局の秘密鍵ＫｐｒｉｖＡＣおよび公開鍵ＫｐｕｂＡＣを生成するステップ２００が設けられてもよい。この認証局は、たとえば、腕時計製造会社であってもよく、またはスウォッチグループなどの製造グループの企業であってもよい。ステップ２０６では、一度生成されると、認証局の秘密鍵ＫｐｒｉｖＡＣおよび公開鍵ＫｐｕｂＡＣはセイフティデポジットボックスなどの安全ユニットに記憶される。ステップ２０２では、認証局公開鍵ＫｐｕｂＡＣは銀行、特にスウォッチグループのパートナーである銀行または金融もしくは銀行機関に送信される。ステップ２０４では、銀行または金融もしくは銀行機関はメモリに記憶する公開鍵ＫｐｕｂＡＣを受信する。

【００４３】

本発明による秘密または機密データのプログラミングのために、ステップ１００では、集積回路の一式の秘密鍵ＫｐｒｉｖＩＣおよび公開鍵ＫｐｕｂＩＣが生成されてもよい。秘密および公開鍵は集積回路製造プロセスの最後または腕時計などの携帯品の製造施設で生成されてもよい。これらの秘密および公開鍵ＫｐｒｉｖＩＣおよびＫｐｕｂＩＣは、少なくとも一時的に不揮発性メモリなどの集積回路メモリに記憶される。これらの秘密および公開鍵は各製造された集積回路特有であり、腕時計の具体的な使用機能専用である。

【００４４】

ステップ１０２では、集積回路の秘密および公開鍵ＫｐｒｉｖＩＣおよびＫｐｕｂＩＣが記憶されると、集積回路公開鍵ＫｐｕｂＩＣはスウォッチグループの企業などの認証局に送信される。ステップ１０４で公開鍵ＫｐｕｂＩＣを受信すると、認証局秘密鍵ＫｐｒｉｖＡＣに基づいて集積回路のデジタル証明書の算出が行われる。デジタル証明書は一般式ＣｅｒｔＩＣ＝Ｆ（ＫｐｕｂＩＣ、ＫｐｒｉｖＡＣ）にしたがって取得される。ステップ１０６では、集積回路デジタル証明書が算出されると、証明書ＣｅｒｔＩＣは集積回路または腕時計の製造者に送信される。ステップ１０８では、特定用途向け集積回路は製造された腕時計に個別化される。個別化は、少なくとも一時的に、腕時計の公開鍵ＫｐｕｂＩＣ、秘密鍵ＫｐｒｉｖＩＣおよび集積回路デジタル証明書ＣｅｒｔＩＣを集積回路のメモリに記憶することからなる。

【００４５】

ステップ１１０では、秘密および公開鍵ＫｐｒｉｖＩＣおよびＫｐｕｂＩＣおよび証明書ＣｅｒｔＩＣが集積回路に記録されると、公開鍵ＫｐｕｂＩＣおよびデジタル証明書ＣｅｒｔＩＣは集積回路に関連する腕時計アンテナによって銀行または金融機関もしくは銀行機関に送信される。伝達は腕時計の近くにある携帯電話などの通信端末、または店舗、特にスウォッチ店舗のシステムを通じて行われる。スウォッチ店舗では、未来の腕時計所有者が腕時計を購入することができる。ステップ１１２では、デジタル証明書ＣｅｒｔＩＣは、購入した腕時計の所有者の銀行または金融機関もしくは銀行機関で、式Ｖ＝Ｇ（ＣｅｒｔＩＣ、ＫｐｕｂＡＣ）による認証局公開鍵ＫｐｕｂＡＣによって検証される。証明

書が承認されると、銀行または金融機関もしくは銀行機関は銀行データなどの秘密または機密データを生成し、腕時計を個別化する。このデータは集積回路から受信した公開鍵ＫｐｕｂＩＣで式暗号化データ＝Ｈ（銀行データ、ＫｐｕｂＩＣ）により暗号化される。

【００４６】

ステップ１１４では、銀行または金融機関もしくは銀行機関は暗号化データを腕時計集積回路に送信する。この暗号化データはまずトンネルとして機能する通信端末を通過してから、腕時計アンテナに受信される。ステップ１１６では、暗号化データが集積回路によって受信されると、暗号化データは集積回路秘密鍵ＫｐｒｉｖＩＣによって復号化される。腕時計所有者の秘密データに関連する暗号化データ、具体的には銀行データはステップ１１８で不揮発性集積回路のメモリに記憶される。この記憶されたデータをロックして、破壊されないようにすることができる。その後のステップ１２０では、集積回路メモリに記憶された一時的なデータはメモリ空間を空けるために削除されえる。

【００４７】

秘密または機密データのプログラミングは、時計からの公開鍵および証明書、ならびに銀行から受信する暗号化データの一回のみの送受信につき一回だけ実施されてもよい。復号化後に、記憶される秘密データを一回のみロックしてもよい。これは、その後物品またはサービスを非接触型決済するために腕時計を個別化する間に、所有者が腕時計購入後に非常に迅速に行うことができる。

【００４８】

ここまで前述した記載から、秘密または機密データを腕時計および本発明にしたがってプログラミングされた集積回路を備える携帯品などの携帯品の特定用途向け集積回路にプログラミングする本方法の複数の変形は、請求項が規定する本発明の範囲から逸脱せずに当業者には考案可能であろう。携帯品はまた、集積回路を挿入可能であり、短距離通信を確立可能であれば、たとえばブレスレット、指輪またはネックレスであってもよい。秘密または機密データを携帯品の集積回路にプログラミングすることはまた、銀行または金融機関もしくは銀行機関で通信端末を用いずに直接実施されてもよい。秘密または機密データは銀行データ以外のデータであってもよく、それによって携帯品は電子チケット、ある場所への非接触アクセス、自動車などの装置のレンタル、またはその他の機能のためにプログラミングされた特定用途向け集積回路とともに用いることができる。

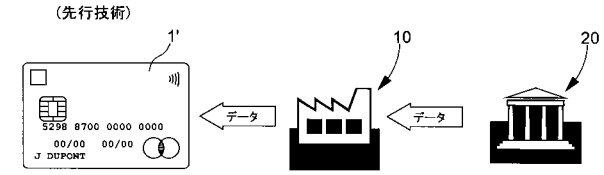
【符号の説明】

【００４９】

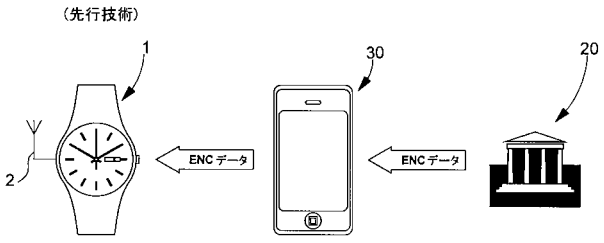
１　携帯品
１’　カード
２　アンテナ
３　集積回路
４　プッシュボタン
１０　カード製造者
２０　銀行
３０　携帯電話
１００　ステップ
１０２　ステップ
１０４　ステップ
１０６　ステップ
１０８　ステップ
１１０　ステップ
１１２　ステップ
１１４　ステップ
１１６　ステップ
１１８　ステップ
１２０　ステップ

２００　ステップ
２０２　ステップ
２０４　ステップ
２０６　ステップ

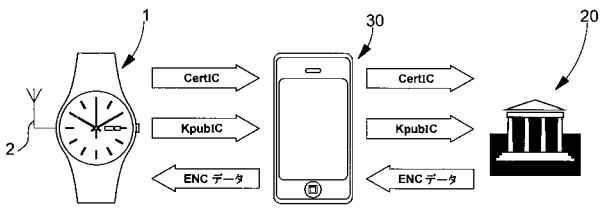
【図１】



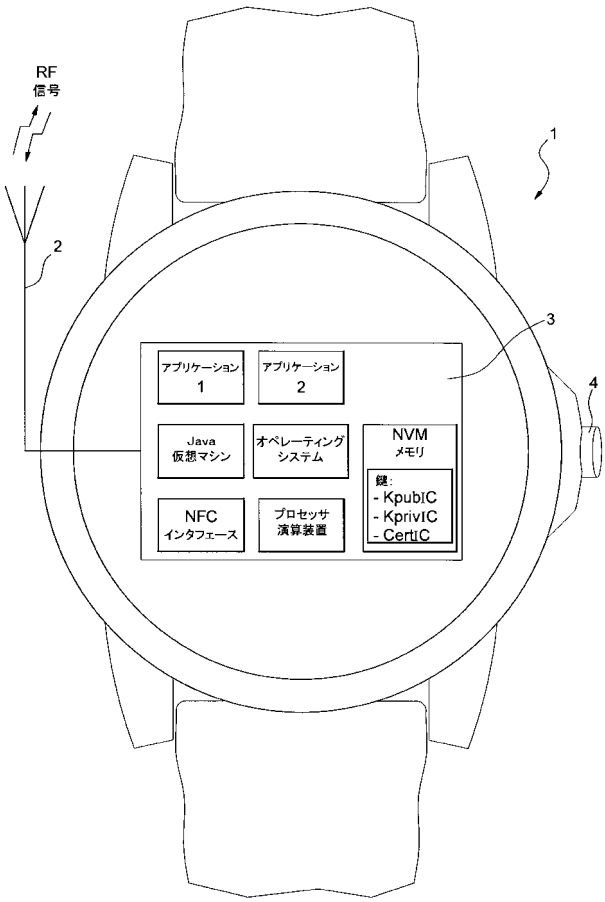
【図２】



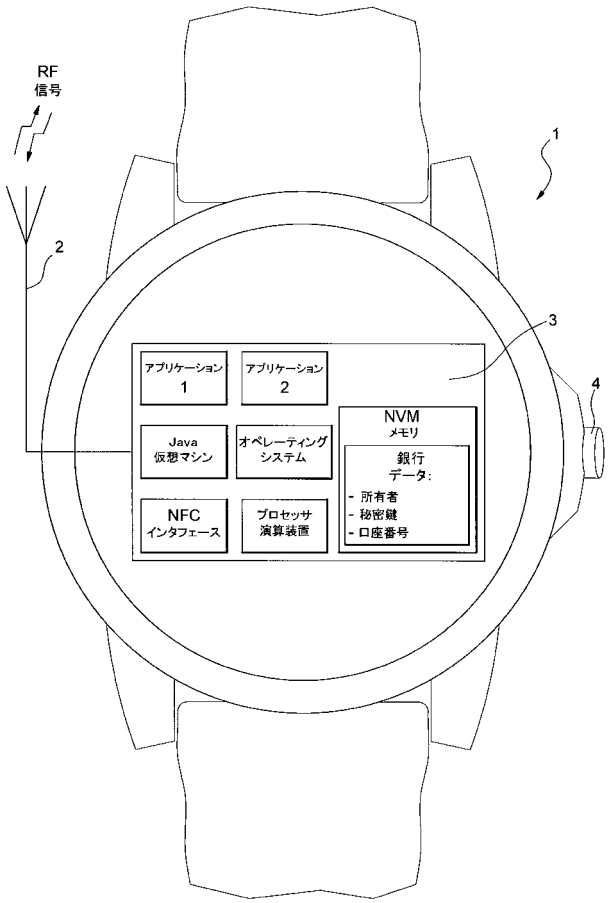
【図３】



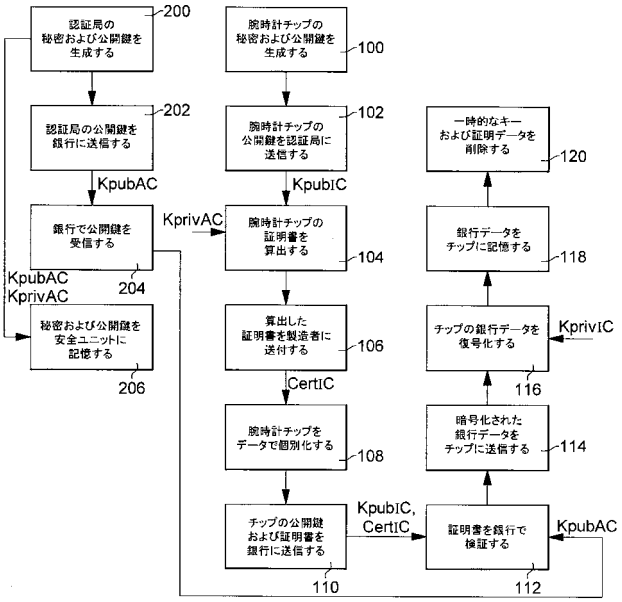
【図４ａ】



【図４ｂ】


RF
信号
1
2
3
4
アプリケーション
1
アプリケーション
2
Java
仮想マシン
オペレーティング
システム
NVM
メモリ
銀行
データ:
- 所有者
- 秘密鍵
- 口座番号
NFC
インタフェース
プロセッサ
演算装置

【図５】


認証局の
秘密および公開鍵を
生成する
200
腕時計チップの
秘密および公開鍵を
生成する
100
認証局の公開鍵を
銀行に送信する
202
腕時計チップの
公開鍵を認証局に
送信する
102
一時的なキー
および証明データを
削除する
120
KpubAC
KpubIC
銀行で公開鍵を
受信する
KprivAC
腕時計チップの
証明書を
算出する
104
銀行データを
チップに記憶する
118
KpubAC
KprivAC
204
秘密および公開鍵を
安全ユニットに
記憶する
206
算出した
証明書を製造者に
送付する
106
チップの銀行データを
復号化する
KprivIC
116
CertIC
腕時計チップを
データで個別化する
108
暗号化された
銀行データを
チップに送信する
114
チップの公開鍵
および証明書を
銀行に送信する
110
KpubIC,
CertIC
証明書を銀行で
検証する
112
KpubAC

【外国語明細書】
2017005712000001.pdf