(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2017-509042
(P2017-509042A)
(43)公表日　平成29年3月30日(2017.3.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/31		5J104
H04L 9/32	(2006.01)	H04L	9/00	675A	5K102
G06K 19/077	(2006.01)	G06K	19/077	112	
G06K 19/07	(2006.01)	G06K	19/07	280	
G06F 21/46	(2013.01)	G06K	19/07	030	

審査請求 未請求　予備審査請求 未請求　（全 15 頁）　最終頁に続く

(21)出願番号　特願2016-543599 (P2016-543599)
(86)(22)出願日　平成26年12月3日 (2014.12.3)
(85)翻訳文提出日　平成28年8月22日 (2016.8.22)
(86)国際出願番号　PCT/EP2014/076348
(87)国際公開番号　WO2015/101457
(87)国際公開日　平成27年7月9日 (2015.7.9)
(31)優先権主張番号　13306894.0
(32)優先日　平成25年12月30日 (2013.12.30)
(33)優先権主張国　欧州特許庁 (EP)
(31)優先権主張番号　14151152.7
(32)優先日　平成26年1月14日 (2014.1.14)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　504326572
ジエマルト・エス・アー
フランス国、９２１２０・ムドン、リユ・ドウ・ラ・ベレリー・６
(74)代理人　110001173
特許業務法人川口國際特許事務所
(72)発明者　トゥベ，ステファン
フランス国、９２１９０・ムドン、リュ・ドゥ・ラ・ベルリ・６、ジェマルト・エス・アー、インテレクチュアル・プロパティ・デパートメント

最終頁に続く

(54)【発明の名称】光アクティブ化センサを備える通信デバイス

(57)【要約】
通信デバイス１は、数字鍵および多様化アルゴリズムを記憶するメモリＭと、少なくとも数字鍵および多様化アルゴリズムから識別コードを生成する演算部Ｄと、演算部によって生成された識別コード１０１、１０２、１０３を表示するディスプレイと、を備える。通信デバイスは、光信号３０を受信する光センサ１１をさらに備える。

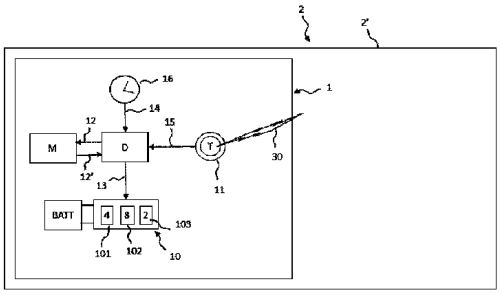

FIG.1

【特許請求の範囲】
【請求項１】
通信デバイス（１）であって、
－　数字鍵および多様化アルゴリズムを記憶するメモリ（Ｍ）と、
－　少なくとも数字鍵および多様化アルゴリズムから、識別コードを生成する演算部（Ｄ）と、
－　演算部によって生成された識別コード（１０１、１０２、１０３）を表示するディスプレイ（１０）とを備える通信デバイス（１）であって、
光を受光および／または検出する光センサ（１１）を備えることを特徴とする、通信デバイス（１）。
【請求項２】
光センサ（１１）が、光信号（３０）を受信するように意図されており、通信デバイスが、デバイス初期化機能を提供し、初期化機能が、
－　光センサによって受信された光信号を変調する一連のデータを復号することと、
－　復号された数列に含まれた数字鍵を記憶することと
を含む、請求項１に記載の通信デバイス（１）。
【請求項３】
演算部（Ｄ）が、
－　所定時間の間に光センサ（１１）によって受光された光強度（３０）の取得後、ディスプレイ（１０）をアクティブ化させる機能
を提供することを可能にする、請求項１に記載の通信デバイス（１）。
【請求項４】
前記デバイスが、ディスプレイ（１０）および演算部（Ｄ）に電力供給することができるバッテリ（ＢＡＴＴ）を備える、請求項１に記載の通信デバイス（１）。
【請求項５】
演算部（Ｄ）が、メモリ（Ｍ）に記憶された数字鍵およびデータの公開部分から、識別コードを生成する、請求項１に記載の通信デバイス。
【請求項６】
前記通信デバイスが、日付を提供する時計（１６）を備え、前記日付が、データの公開部分を定義する、請求項５に記載の通信デバイス。
【請求項７】
時間間隔を決定する時計を備え、その時間間隔でディスプレイ（１０）が演算部によって生成された識別コード（１０１、１０２、１０３）の表示を可能とし、光の検出後に所定のセキュリティ時間の経過した後、前記識別コードが表示される、請求項１に記載の通信デバイス。
【請求項８】
新たな識別コードが、定期的に生成される、請求項３に記載の通信デバイス（１）。
【請求項９】
識別コードの表示が、表示時間中、ディスプレイで維持される、請求項３に記載の通信デバイス（１）。
【請求項１０】
請求項１から９のいずれか一項に記載の通信デバイスを備える、スマートカード（２）。
【請求項１１】
ディスプレイが、光センサと同じカード面に配置される、請求項１０に記載のスマートカード（２）。
【請求項１２】
デバイスを含むスマートカード（２）から取引を行う方法であって、デバイスが、
－　数字鍵および多様化アルゴリズムを記憶するメモリ（Ｍ）と、
－　少なくとも数字鍵から識別コードを生成する演算部（Ｄ）であって、数字鍵が、プ

ライベートデータを定義する、演算部（Ｄ）と、
－　演算部によって生成された識別コード（１０１、１０２、１０３）を表示するディスプレイ（１０）と、
－　光を受光および／または検出する光センサ（１１）と
を備える、方法において、
－　光センサ（１１）が、最小限の時間で光源に晒されるように、スマートカード（２）を配置することと、
－　最小限の時間で露光された後に、ディスプレイ（１０）に識別コードを表示することと
を含むことを特徴とする、方法。
【請求項１３】
カード番号を含むスマートカード（２）をパーソナル化する方法であって、
－　請求項１から９のいずれか一項に記載の通信デバイスを、カード番号に割り当てることであって、前記通信デバイスの識別子が遠隔サーバに格納され、かつ前記カード番号に関連付けられる、割り当てることと、
－　前記スマートカードに、通信デバイスを組み立てることと、
－　カード番号に関連付けられた通信デバイスに、数字鍵を割り当てることと、
－　スマートカードの最終パーソナル化中に一連のデータによって変調された光信号を光センサ（１１）で受信することによって、数字鍵を転送することと
を含むことを特徴とする、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の分野は、特にセキュリティコードの生成によって、取引を安全にするデバイスに関する。より正確には、本発明の分野は、ディスプレイが取引を安全にするためのコードを生成するモジュールを備える、バンクカードの領域に適用する。
【背景技術】
【０００２】
現在、電話によって、またはインターネットを介して、カードの番号、有効期限日、および所持者で、そのカードを簡単に識別することによって、取引を安全にすることができるバンクカードを製造するソリューションがすでに存在する。
【０００３】
取引を安全にする簡単な手段は、３桁セキュリティコードであり、ＣＳＣ、ＣＶＶ、ＣＶＣもしくはＶ－コード、またはＣＣＶとも呼ばれる。本願の出願人は、当業者に知られている、広く行き渡った頭字語、ＣＶＶを使用し、これはＣａｒｄ　Ｖｅｒｉｆｉｃａｔｉｏｎ　Ｖａｌｕｅ（カード確認番号）の略である。
【０００４】
この安全にする手段の問題の１つは、コードがカードの片面に静的に表示されることである。その結果、このコードは、第三者によって簡単に読み取られ、カードに収集されたその他の情報と併せて使用される可能性がある。
【０００５】
バンクカードを使用するこのような取引のセキュリティを高めるために、ＣＶＶを動的にすることが知られている。動的ＣＶＶは、時間とともに変わるコードで、このコードはカードに表示される。可変コードは、取引の日付および時間に応じてコードの真正性を確認することを可能にするサーバに、同期化擬似ランダムタイプの生成装置によって提供される。
【０００６】
しかし、動的ＣＶＶの使用は、いくつかの問題を引き起こす。第１の問題はパーソナル化から生じ、パーソナル化は、ディスプレイモジュールがスマートカードに組み込まれる前に、ディスプレイモジュールのメモリに数字暗号鍵を導入することを必要とする。

【０００７】
ＣＶＶコードを生成して表示するモジュールを、関連付けられたカード番号で追跡する作業を増やす必要があるため、このソリューションは、構成的な面では複雑である。カード番号は、この時点では、すなわちモジュールにおける数字鍵の定義中は、必ずしも知られていないので、モジュールの追跡および割り当ては、その実施が複雑になる。
【０００８】
一代替方法では、ＣＶＶコードを生成するモジュールをパーソナル化する外部コンタクタを有することが可能である。カードが製造されると、モジュールにおいて暗号鍵をパーソナル化することを可能にする外部デバイスで、パーソナル化が行われる。しかし、コンタクタは、ユーザにとって便利ではない場合があるため、このソリューションは、カード使用の面では欠点がある。また、コンタクタは、カードの美的外観に悪影響を及ぼす。
【０００９】
別の代替方法では、ＣＶＶコードを生成するモジュールは、カードが製造された後のパーソナル化を可能にする外部デバイスとのリンクを確立することを可能にするＲＦモジュールに関連付けられてもよい。しかし、このソリューションは、特に、そのモジュールの１つがその他のモジュールとの干渉を起こす可能性のある、非接触型バンクカードでは、その実施は費用がかかり、また困難である。
【００１０】
別の代替方法では、ＣＶＶコードを生成するモジュールは、すでにＩＳＯコンタクトを介してカードに組み込まれたマイクロチップに接続されることができる。しかし、このソリューションは、組み込みの面では困難である。さらに、このソリューションは、カードの２つの構成要素を分離して、それらを独立させることを可能にしない。２つの構成要素の独立は、カードの環境を安全にすることに役立ち、よりハックされにくくする。
【００１１】
第２の問題は、動的ＣＶＶコードの場合でも、スマートカードに表示された情報の盗用を排除することができないことである。例えば、カードが第三者によって見られることができる場合、その第三者は、動的に表示されたＣＶＶコードを含む情報を収集して、コードの有効期限内に、その情報を使用することができる。
【００１２】
このため、既存のソリューションは、このような情報の盗用を制限する手段を提案する。例えば、必要とされる場合のみ、ディスプレイ上にＣＶＶコードの表示を生成するボタンを設けることが可能である。このソリューションは、スマートカードに組み込むことが難しいという欠点があり、またボタンは、ユーザには不便である可能性がある。また、ボタンは、間違って、または一時的にカードを所持する、悪意ある人によって押される可能性がある。
【００１３】
別のソリューションは、表示を定期的にトリガすることにあり、このソリューションは、電力消費に関して費用がかかる可能性がある。また、このソリューションは、コードが表示されるまでの時間待たなければならず、取引の間、悪影響を及ぼす可能性がある。支払いを確認する際の待ち時間が長すぎるとなると、このソリューションは実行可能ではない。
【００１４】
本発明は、上述の欠点を克服することを可能にする。
【発明の概要】
【課題を解決するための手段】
【００１５】
本発明の一対象は、通信デバイスに関し、通信デバイスは：
－　数字鍵および多様化アルゴリズムを記憶するメモリと、
－　少なくとも数字鍵および多様化アルゴリズムから識別コードを生成する演算部と、
－　演算部によって生成された識別コードを表示するディスプレイと、

を備える。
【００１６】
さらに、本発明による通信デバイスは、光を受光および／または検出することができる光センサを備える。
【００１７】
光センサは、光信号を受信するように意図されるのが有利であり、通信デバイスは、デバイス初期化機能を行い、初期化機能は：
－　光センサによって受信された光信号を変調する一連のデータを復号することと、
－　復号された数列に含まれた数字鍵を記憶することと
を含む。
【００１８】
一利点は、スマートカードなどのデバイスのパーソナル化を、光学式エミッタを使用して、安全で簡単な方法で可能にすることである。
【００１９】
一利点は、前記通信デバイスが、カードの製造時にそのカードに組み込まれる場合、スマートカードとの通信に対するデバイスのトレーサビリティを容易にすることである。数字鍵は、カードの製造後、カードの最終パーソナル化の時点で、カード番号に関連付けられてもよい。このように、通信デバイスは、それの数字鍵が多様化アルゴリズムの初期化シードを構成する、ＣＶＶ式コードなどの識別コードを生成するモジュールであることが有利である。
【００２０】
本発明の一実施形態では、演算部は、所定時間の間に光センサによって受光された光強度の取得後、ディスプレイをアクティブ化させる機能を実行させる。
【００２１】
この機能の一利点は、遅延されたコード表示を得ることを可能にすることである。この表示遅延は、最小限のアクティブ化時間として理解されてもよく、したがって、コードが第三者によってコピーされることからの保護を提供できる。
【００２２】
受光された光量は、受光された光強度であってもよい。この光強度が時間スケールにわたって積分される場合、光強度は、受け取られたエネルギー量を定義できる。
【００２３】
所定時間にわたって受光される光量は、直接光センサによって、または演算部によって、またはそれら２つの構成要素によって共同で、実施形態に応じて測定されてもよい。このために、通信デバイスは、時計を含んでもよく、演算部は、所定の時間の間で光束を測定するためにタイムカウンタをトリガすることができる。
【００２４】
通信デバイスは、取得時間中の各瞬間で、または別の実施形態で受光された光強度を比較することができ、また通信デバイスは、取得時間中に受け取られた総エネルギーを、エネルギー限界値と比較することができる。
【００２５】
通信デバイスは、ディスプレイおよび演算部に電力供給するバッテリを備えるのが有利である。このことは、通信デバイスを独立させることを可能にする。その低電力消費は、一般的に有効期限のあるスマートカードによる寿命を超える最低寿命を提供することを可能にする。
【００２６】
演算部は、メモリに記憶された数字鍵およびデータの公開部分から識別コードを生成することができるのが有利である。
【００２７】
このような生成は、表示されたコードのセキュリティとその有効性を高めることを可能にする。

【００２８】
データの公開部分は、日付データであることが有利である。この場合、通信デバイスは、日付を伝達することができる時計を備える。
【００２９】
一実施形態では、本発明による通信デバイスは、時間間隔を決定する時計を備え、その時間間隔で、ディスプレイが演算部によって生成された識別コードの表示を可能にする。光の検出後に所定のセキュリティ時間が経過した後、識別コードの表示が有利に表示される。
【００３０】
新たな識別コードが定期的に生成されるのが有利である。
【００３１】
識別コードの表示が、表示時間中、表示され続けるのが有利である。
【００３２】
このソリューションが選択される場合、サーバも、ＣＶＶコードなどの識別コードと、動的ＣＶＶコードを生成することを可能にした日付データに対応するデータとのその一致をチェックする時計を備える。サーバは、特に、通信デバイスで使用される時計の時間ドリフトに対して、ある程度の許容誤差を容認するように構成されてもよい。
【００３３】
ディスプレイは、電気泳動表示を可能にするのが有利である。このソリューションは、特に表示されたデータの不揮発性状態のおかげで、電力消費を低減することを可能にする。
【００３４】
第１の所定時間は、１０分－２日で、第２の所定時間は、１－１０分であるのが有利である。
【００３５】
本発明の別の対象は、本発明による通信デバイスを備えるスマートカードに関する。
【００３６】
本発明の一実施形態では、通信デバイスのディスプレイは、光センサと同じカード面に置かれる。
【００３７】
本発明の別の対象は、デバイスを含むスマートカードから取引を行う方法に関し、デバイスは：
－　数字鍵および多様化アルゴリズムを記憶するメモリと、
－　数字鍵から識別コードを生成する演算部と、
－　演算部によって生成された識別コードを表示するディスプレイと、
－　光を受光および／または検出する光センサと、
を備える。前記方法は：
－　光センサが最小限の時間で光源に晒されるように、スマートカードを配置するステップと、
－　最小限の時間で露光された後に、ディスプレイにコードが表示されるステップと
を含む。
【００３８】
このような方法の一利点は、識別コードが第三者に晒される可能性のある時間を短くすることによって、識別コードの確認作業を安全にすることである。
【００３９】
本発明の別の対象は、カード番号を含むスマートカードをパーソナル化する方法に関し、前記方法は：
－　本発明による通信デバイスを、カード番号に割り当てることであって、前記通信デバイスの識別子が遠隔サーバに格納され、かつ前記カード番号に関連付けられる、割り当てることと、

－　前記スマートカードに、通信デバイスを組み立てることと、
－　カード番号に関連付けられた通信デバイスに、数字鍵を割り当てることと、
－　スマートカードの最終パーソナル化中に一連のデータによって変調された光信号を光センサで受信することによって、数字鍵を転送することと
を含む。

【００４０】

このような方法の利益は、識別コードを生成するモジュールを、カードが製造される時点から、カードに関連付けることによって、それらのカードで追跡する必要がもうなくなるということである。このような場合、本発明による通信デバイスは、ＣＶＶコードを生成するモジュールであることが理解される。ＣＶＶ生成モジュールは、最終パーソナル化中にパーソナル化され、初期化シードは、同じ時点で、カードに入力されるアカウント番号に簡単に適合される。

【００４１】

数字鍵の転送は、通信デバイスの光センサにおける、一連のデータによって変調された光信号の放出を含むことが有利である。

【００４２】

本発明の他の特徴および利益は、以下の添付図面を参照することによって、以下の発明を実施するための形態において明らかになるであろう。

【図面の簡単な説明】

【００４３】

【図１】本発明による、通信デバイスを備えるスマートカードの裏面の図である。
【図２】本発明による、通信デバイスを備えるスマートカードの表面の図である。

【発明を実施するための形態】

【００４４】

以下の発明を実施するための形態において、「光アクティブ化センサ」は、一般的に「光センサ」と呼ばれる。

【００４５】

本出願において、「暗号鍵」は、「数字暗号鍵」または「数字鍵」と呼ばれてもよい。

【００４６】

この発明を実施するための形態は、通信デバイスが動的ＣＶＶコード生成装置である実施形態を説明する。より一般には、本発明では、例えばＣＶＶ式であってもよい数字鍵から生成されたコードは、識別コードと呼ばれる。

【００４７】

図１は、通常裏面２’とされるその片面で提示されたスマートカード２を表す。この裏面は、本発明による通信デバイス１を含む。

【００４８】

本発明によるデバイスは、光束３０を受光することができる光センサ１１を備える。

【００４９】

光センサは、フォトトランジスタ、フォトダイオードまたはフォトエレクトリックセルなどの受光素子であってもよい。通信デバイスがスマートカードに組み込まれる場合、光センサ１１は、ディスプレイ１０と同じカード面に置かれるのが好ましい。

【００５０】

通信デバイスがスマートカードに組み込まれる場合、光センサは、スマートカードの表面との表面の同質性を可能にするため、半透明部の下に置かれてもよい。一実施形態では、半透明部は、カードの表面の一部を形成する。半透明部は、このように、カードがポケットや財布に入れられた場合に生じる可能性のある、手や擦れによる接触から光センサを保護する。

【００５１】

光センサ１１は、演算部Ｄに接続される。ディスプレイ１０は、動的ＣＶＶコード式の識別コードを表示することを可能にする。メモリＭは、数字暗号鍵Ｋおよび多様化アルゴ

リズムを記憶するために使用される。また、時計１６は、時間データを提供することを可能にする。本発明の一実施形態では、数字鍵と時間データは、演算部Ｄを使用して、識別コードを生成することを可能にする。識別コードの生成は、例えば、日付に応じて一意の識別コードを関連付ける、または所定の日付で新たなコードを生成する、知られている多様化アルゴリズムに従ってもよい。この識別コードは、２つの識別コードの生成間の時間間隔に対応する所定の時間の間有効である。数字鍵と時間によって構成された、秘密情報から識別コードを多様化するアルゴリズムは、演算部Ｄによって実行される。生成された各識別コードは、このように、時間データのおかげで以前のコードとは異なる。

【００５２】

暗号鍵と公開データから識別コードを生成する別の代替方法がある。この公開データは、例えば、例えばカード所持者が、アクションをとることによって、イベントカウンタをインクリメントする場合のイベントの数であってもよい。このアクションは、カード利用が検出される毎にとられてもよい。カウンタは、また、例えば取引の回数をカウントすることによって、サーバによって評価される。この場合、許容誤差がサーバによって容認される必要がある。このように、取引が終了すると、コードが有効にされてもよい。

【００５３】

この意味では、本発明の通信デバイスは、識別コード、例えば、動的ＣＶＶコードの生成装置である。光センサは、シードを定義して、それを識別コード生成装置のメモリに記憶することによって、通信デバイスが初期化されるようにする。この最後の段階は、スマートカードがパーソナル化される段階であると理解されてもよく、原則として１回のみ行われる。さらに、光センサは、カードが使用される時に生成されるコードの表示をアクティブ化させるために、またはアクティブ化させないために、所定時間の間の光強度の受光をテストすることを可能にする。

【００５４】

ディスプレイおよび演算部は、識別コードを表示する際、バッテリＢＡＴＴによって電力供給されることができる。このコードが、図１に表されたように、３つの数字、１０１、１０２、１０３を含む場合、図示された数列は、３桁のコード「４８２」を表す。

【００５５】

本発明による通信デバイスの第１の実施形態では、第１の機能は、光列を復号することにある。第１の信号を変調する数値データを含む信号は、「第１の光信号」と呼ばれる。この第１の機能は、カードのパーソナル化の最中、初期化で使用され、数字暗号鍵を定義し、送信し、メモリＭに記憶することを可能にする。原則として、第１の機能は、１回のみ行われる。

【００５６】

暗号鍵は、識別コードを可変にすることを可能にするシードを定義する。シードは、必要であれば、識別子などのその他の情報を含む可能性がある。一代替実施形態では、暗号鍵の受信は、画面上の表示によって、またはＬＥＤによって、返報で確認されることができる。

【００５７】

本発明による通信デバイスの第２の実施形態では、第２の機能は、センサ１１が所定時間で光に晒された後、ディスプレイ１０をアクティブ化させることにある。一利点は、スマートカードの寿命における異なる時点で、２つの機能から利益を得ることである。２つの機能は、このような本発明による識別コード生成装置によってサポートされる。

【００５８】

使用段階では、受光素子の第２の機能は、識別コードの表示を認可するために、カードのディスプレイが、所定時間の間、光に晒されたことを検出することである。

【００５９】

第２の光信号は、表示をアクティブ化させることを可能にする信号であり、すなわち、一定の時間の間受光された光強度で、演算部Ｄは、ディスプレイ１０上に、コードの表示をアクティブ化させることができる。この第２の機能は、ユーザが識別コードを必要とす

る時はいつでも使用される。この場合、ユーザは、スマートカード２のセンサを含む面を、光１１に一定の時間晒す。図１の場合、センサがある面は、スマートカードの裏面である。

【００６０】

２つの実施形態は、本発明の通信デバイスによってサポートされる。これらの実施形態は、異なる時点でアクティブ化させられる。第１の機能に関して、この機能は、カードがパーソナル化され、このようにカードが製造され、構成される時に、アクティブ化させられる。第２の機能に関して、この機能は、カード所持者によって新しく使用される度に、新たな識別コードを提供するためにアクティブ化させられる。

【００６１】

第１の機能の働きを詳しく述べることとする。一代替実施形態では、光センサは、光信号を復調して、それから数列を抽出することを可能にする、構成要素を備える。第２の代替実施形態では、演算部は、アナログ信号を受信し、その信号を数値信号に変換するように構成されたインタフェースを備える。本発明による通信デバイスは、このように、光センサ１１または演算部Ｄに組み込まれてもよい、アナログ－デジタル信号コンバータを備える。あるいは、コンバータは、光センサ１１と演算部Ｄとの間の受信チェーンに位置する独自の構成要素であってもよい。

【００６２】

代替実施形態では、受信された信号を数量化する、または正規化することのできる構成要素は、本発明による通信デバイスで使用されてもよい。

【００６３】

コンバータがセンサ１１に組み込まれる場合、数値データは、接続１５を介して、演算部Ｄに転送される。

【００６４】

演算部Ｄは、数字暗号鍵などの、受信された数列から情報を抽出することを可能にする。この鍵は、その後、接続１２を介して、メモリＭに記憶される。図１の例は、可能性のある実装の実施形態を表す。

【００６５】

パーソナル化段階の最中、光信号を変調する一連の情報を送信することができる適切なエミッタは、特にこの段階中に使用されてもよい。エミッタは、光センサに対向して配置される。

【００６６】

第２の機能の働きを詳しく述べることとする。

【００６７】

ユーザが、動的識別コード、例えば、取引を安全にする３桁コードを生成したいと思う場合、ユーザは、スマートカード２を２’の面にして、センサ１１が、所定時間の間、光に晒されるようにする。この時間は、２、３秒であってもよい。

【００６８】

光センサは、光束３０を取得し、所定の時間にわたって集積された、受光された光強度を測定する。この光強度が、所定時間中に所定の限度値を超えると、信号は、直接ディスプレイ１０に、または演算部Ｄに送信されてもよい。この最後のソリューションは、図１で説明されるモードである。

【００６９】

演算部Ｄは、その後、識別コードの表示をアクティブ化させる。このようなアクティブ化は、「表示認可」として理解されてもよい。

【００７０】

第２の機能を行うために、第１の機能とは違って、受信された光信号は、データ列を必ずしも変調しない。光エネルギーの持続時間またはレベルのみが、識別コードの表示をアクティブ化させるのに必要である。

【００７１】

一実施形態では、時計は、時間間隔を決定し、時間にわたって規則的に、または擬似ランダムに、新たなコードを生成することを可能にする。

【００７２】

このソリューションは、例えば、スマートバンクカードの使用セキュリティを高めることを可能にする。表示された各識別コードは、そのため使い捨てのコードである。

【００７３】

使い捨ての識別コードは、識別コードが第三者に即座に晒されないようにするために、所定のセキュリティ時間の終了後に表示される。

【００７４】

さらに、識別コードが表示された時点で、一定の延長時間の間、コードを表示し続けるために、オプション機能が実施されてもよい。「フリーズ」機能として知られているこの機能は、前の識別コードが読み取られている間、新たな識別コードの表示をフリーズする。

【００７５】

一実施形態では、識別コードは、暗号鍵と時間データから生成される。暗号鍵は、メモリＭに記憶され、演算部が識別コードを表示するために呼び出されると、その演算部Ｄによって読み取られることができる。接続１４を介して送信された鍵および時間データは、有効な識別コードを生成することができる、アルゴリズムの入力データであってもよい。

【００７６】

他の実施形態では、識別コードは、Ｎ個の数字を含み、３桁に限定されない。

【００７７】

図２では、スマートカード２の裏面２”を表す情報が図示される。スマートカード２は、マイクロチップＰ１と、ＩＳＯ７８１６規格で規定されるように、コンタクトを備えるインタフェース２０を備える。例えば関連するメモリなどのマイクロチップに関連したいくつかの要素は、表されていない。

【００７８】

本発明のスマートカード２は、このように、本発明の通信デバイスを裏面に、すなわち、従来表面に置かれているマイクロチップを含む、カードのもう一方の面に、置くことを可能にする。

【００７９】

本発明は：

－　ＣＶＶコード生成モジュールにおける情報の読み込みを、ソリューションおよび使用の複雑さの観点から、最適に解決することと、

－　カードの製造を容易にし、その費用を低減することと、

－　ＣＶＶに追加のセキュリティをよい安い費用で提供することと

を可能にする。

【図１】

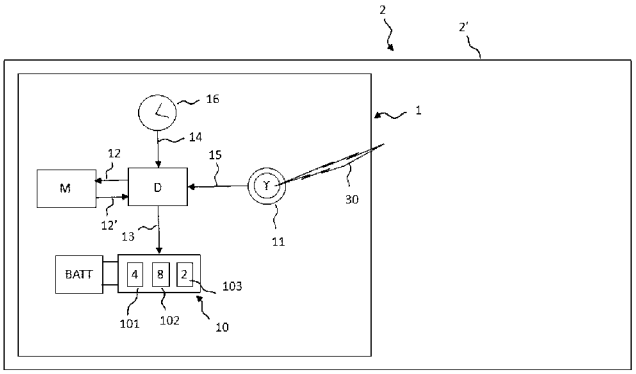

FIG.1

【図２】

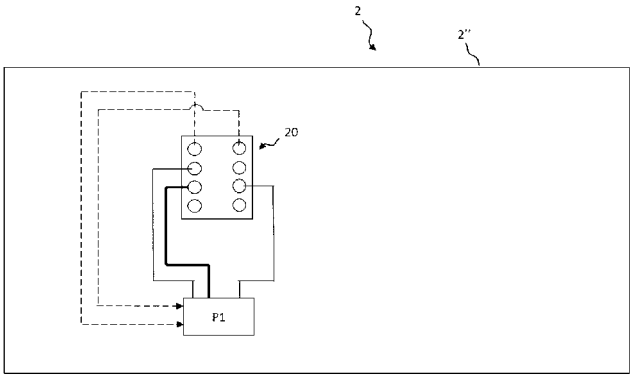

FIG.2

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/076348

A. CLASSIFICATION OF SUBJECT MATTER
INV. G09C1/00 H04L9/08
ADD.

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)
G09C H04L

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 practicable, search terms used)
EPO-Internal, PAJ, WPI Data, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2009/056897 A1 (TELECOM ITALIA SPA [IT]; GHIRARDI MAURIZIO [IT]) 7 May 2009 (2009-05-07) figures 1,2 page 10, line 23 - page 12, line 26 -----	1-13
Y	US 2012/153028 A1 (POZNANSKY AMIR [IL] ET AL) 21 June 2012 (2012-06-21) abstract figures 3,5 paragraph [0014] - paragraph [0032] paragraph [0050] - paragraph [0056] ----- -/--	1-13

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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 application or patent 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
12 February 2015	20/02/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bec, Thierry

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/076348

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Pepijn Pinkse: "Quantum Credit card", , 31 January 2013 (2013-01-31), XP055168636, Retrieved from the Internet: URL:http://www.utwente.nl/mesaplus/archive/2013/1/272924/vici-quantum-credit-card [retrieved on 2015-02-10] page 1	1-13
A	Sebastianus A Goorden ET AL: "Quantum-Secure Authentication with a Classical Key", , 1 March 2013 (2013-03-01), XP055168644, DOI: 10.1364/OPTICA.1.000421 Retrieved from the Internet: URL:http://arxiv.org/abs/1303.0142 page 1 - page 3	1-13
T	SKORIC B: "Security analysis of Quantum-Readout PUFs in the case of generic challenge-estimation attacks", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20130814:143926, 7 August 2013 (2013-08-07), pages 1-10, XP061007989, [retrieved on 2013-08-07] paragraph [01.2] - paragraph [01.3]	

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/076348

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009056897 A1	07-05-2009	BR PI0722174 A2	01-04-2014
		CN 101897165 A	24-11-2010
		EP 2220840 A1	25-08-2010
		ES 2456815 T3	23-04-2014
		US 2010275010 A1	28-10-2010
		WO 2009056897 A1	07-05-2009
US 2012153028 A1	21-06-2012	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)Int.Cl.			FI			テーマコード（参考）
Ｈ０４Ｂ	*10/80*	*(2013.01)*	Ｇ０６Ｋ	19/077	１８８	
Ｈ０４Ｂ	*10/114*	*(2013.01)*	Ｇ０６Ｆ	21/46		
			Ｈ０４Ｂ	10/80		
			Ｈ０４Ｂ	10/114		

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 ティル，ミシェル
フランス国、９２１９０・ムドン、リュ・ドゥ・ラ・ベルリ・６、ジェマルト・エス・アー、インテレクチュアル・プロパティ・デパートメント
(72)発明者 スピロプーロス，エバンゲロス
フランス国、９２１９０・ムドン、リュ・ドゥ・ラ・ベルリ・６、ジェマルト・エス・アー、インテレクチュアル・プロパティ・デパートメント
(72)発明者 カマス，ギヨーム
フランス国、９２１９０・ムドン、リュ・ドゥ・ラ・ベルリ、６、ジェマルト・エス・アー、インテレクチュアル・プロパティ・デパートメント

Ｆターム(参考) 5J104 AA07 GA03 GA04 GA05 KA01 KA03 KA21 NA04 NA35 NA40
PA10
5K102 AB15 AL23 AL28 AM02 AM06 PH31 RD28