(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2009-503665
(P2009-503665A)
(43)公表日　平成21年1月29日(2009.1.29)

(51)Int.Cl.		F I			テーマコード（参考）
G06K 19/073	(2006.01)	G06K	19/00	P	5B035
G09C 1/00	(2006.01)	G09C	1/00	660A	5B058
G06K 19/07	(2006.01)	G06K	19/00	H	5B285
G06K 17/00	(2006.01)	G06K	17/00	F	5J104
G06F 21/20	(2006.01)	G06K	17/00	E	

審査請求 未請求　予備審査請求 未請求　（全 20 頁）　最終頁に続く

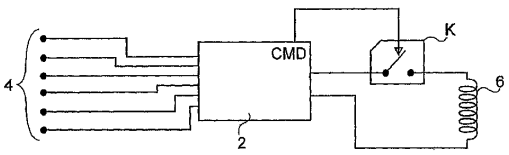
(21)出願番号　特願2008-523404 (P2008-523404)
(86)(22)出願日　平成18年7月24日 (2006.7.24)
(85)翻訳文提出日　平成20年3月24日 (2008.3.24)
(86)国際出願番号　PCT/FR2006/001797
(87)国際公開番号　WO2007/012738
(87)国際公開日　平成19年2月1日 (2007.2.1)
(31)優先権主張番号　0507887
(32)優先日　平成17年7月25日 (2005.7.25)
(33)優先権主張国　フランス(FR)

(71)出願人　501094410
オベルトゥル　カード　システムズ　ソシエテ　アノニム
フランス国，エフ－７５０１７　パリ，ブールバール　マルシェルブ　１０２
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100102819
弁理士　島田　哲郎
(74)代理人　100108383
弁理士　下道　晶久
(74)代理人　100114018
弁理士　南山　知広

最終頁に続く

(54)【発明の名称】接触通信手段およびリモート通信手段を有する電子エンティティ

(57)【要約】
本発明は、接触通信手段（４）と、リモート通信手段（６）と、を備える電子エンティティに関する。接触通信手段を介する事前の指示の受信に応じて、少なくともリモート通信手段を介する一定のデータの交換を認証する手段（２、Ｋ）も提供される。本発明は、電子エンティティと通信する接触通信手段や、電子エンティティを制御しカスタマイズする方法にも関する。



【特許請求の範囲】
【請求項１】
接触通信手段（４；１４）と、
リモート通信手段（６；１６）と、を備え、
前記接触通信手段を介する指示の事前の受信に応じて、少なくとも前記リモート通信手段を介する一定のデータの交換を認証する手段（２、Ｋ；１２）を特徴とする、電子エンティティ。
【請求項２】
前記指示によって制御される活性化情報を格納する手段（１８）と、
前記活性化情報が存在する場合、前記リモート通信手段を介する前記データの交換を認証する手段（１２）と、
を特徴とする、請求項１に記載の電子エンティティ。
【請求項３】
前記活性化情報が存在しない場合、前記リモート通信手段を介する前記データの交換を禁止する手段を特徴とする、請求項２に記載の電子エンティティ。
【請求項４】
前記リモート通信手段が、アンテナ（６）を備え、
前記交換を認証する手段が、前記指示に基づいてマイクロ回路（２）に前記アンテナの接続（Ｋ）を指示する手段（２、ＣＭＤ）を備える、ことを特徴とする請求項１に記載の電子エンティティ。
【請求項５】
マイクロ回路カードであることを特徴とする、請求項１～４のいずれか１項に記載の電子エンティティ。
【請求項６】
リモート通信手段を備える電子エンティティと通信する接触通信手段を備える端末であって、
前記接触通信手段を介して、少なくとも前記リモート通信手段を介する一定のデータの交換を条件設定するための指示を送信する手段を特徴とする端末。
【請求項７】
請求項６に記載の携帯端末。
【請求項８】
接触通信手段と非接触通信手段とを備える電子エンティティを制御する方法であって、
前記接触通信手段を介して活性化指示を受信するステップ（Ｅ６；Ｅ２０）と、
前記活性化指示を受信したとき、少なくとも前記リモート通信手段を介する一定のデータの交換を認証するステップ（Ｅ８；Ｅ２４）と、を特徴とする方法。
【請求項９】
前記認証するステップによって条件設定される、前記リモート通信手段を介して前記データを交換するステップ（Ｅ１０，Ｅ１２；Ｅ３８，Ｅ４２）を特徴とする、請求項８に記載の方法。
【請求項１０】
活性化情報に予め定められた値を設定する（Ｅ２４）ことによって前記認証するステップを実行し、前記条件設定された交換するステップは、
－前記活性化情報の値が前記予め定められた値に等しいことを確認するステップ（Ｅ３４）と、
－前記確認が肯定である場合のみ、前記リモート通信手段を介して前記データを交換するステップ（Ｅ３８，Ｅ４２）と、を備えることを特徴とする、請求項９に記載の方法。
【請求項１１】
特定の時間において、前記活性化情報に前記予め定められた値の補数値を設定するステップ（Ｅ４０）を特徴とする、請求項１０に記載の方法。
【請求項１２】

特定の時間において、前記データの交換を禁止するステップ（Ｅ１６）を特徴とする、請求項８または９に記載の方法。
【請求項１３】
前記特定の時間は、前記リモート通信手段による通信コマンドの終了の受信（Ｅ１４）に対応することを特徴とする、請求項１１または１２のいずれか１項に記載の方法。
【請求項１４】
前記特定の時間は、タイムディレイによって決定されることを特徴とする、請求項１１または１２のいずれか１項に記載の方法。
【請求項１５】
前記リモート通信手段を介して予め定められた数のコマンドを受信した後に前記特定の時間に達することを特徴とする、請求項１１または１２のいずれか１項に記載の方法。
【請求項１６】
前記特定の時間は、通信初期化ステップ（Ｅ３８）の完了に対応することを特徴とする、請求項１１または１２のいずれか１項に記載の方法。
【請求項１７】
接触通信手段を備える電子エンティティをカスタマイズする方法であって、
少なくともリモート通信手段を介する一定のデータの交換を条件設定するための活性化情報を書き込むステップを特徴とする方法。
【請求項１８】
前記電子エンティティは、接触通信手段を備え、
前記接触通信手段を介して指示を受信したとき前記活性化情報を変更することができることを特徴とする、請求項１７に記載の方法。
【請求項１９】
前記活性化情報を変更する条件を示す設定情報を書き込むステップを特徴とする、請求項１７または１８に記載の方法。
【請求項２０】
非接触通信手段を備える電子エンティティをカスタマイズする方法であって、
少なくとも前記リモート通信手段を介する一定のデータの交換を条件設定するための活性化情報を変更する条件を示す設定情報を書き込むステップを特徴とする方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、接触通信手段およびリモート通信手段を有する電子エンティティと、この電子エンティティを有する通信端末装置と、この電子エンティティを制御しカスタマイズする方法と、に関する。
【背景技術】
【０００２】
例えば、一般に、情報を格納するのに適応した電子回路を含むマイクロ回路カードなどの電子エンティティは、外界と通信するための手段を有する。これによって、特に、読取装置または端末のタイプに関して、電子エンティティが保持する情報を外部の装置と交換する。
【０００３】
一般に使用される通信手段の中でも、通信を設定するのに電子エンティティと端末との間の物理的接触が必要条件となる接触通信手段と、２つの素子間に物理的接触がなくても一般に数センチメートルのオーダの範囲内で電子エンティティと読取装置との間の通信が可能であるリモート通信手段と、は区別される。
【０００４】
また、ある電子エンティティは、前述の２つのタイプの通信手段を組み合わせる。この場合、「接触」モードおよび「非接触」モードの各通信モードのため装置に必要な機能に従って、これらの動作モードが構成される場合がある。これについては、例えば、米国特

許第５，２０６，４９５号明細書および米国特許第５，９９９，７１３明細書中に説明されている。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

非接触通信手段の使用は、実用的である（情報を交換するために電子エンティティを正確に配置する必要がない）ことで知られている。それにもかかわらず、例えば、読取装置の近傍を通過したとき、ユーザが望まない通信を設定することによって意図しない情報交換を行ってしまうリスクがあるという欠点がある。例えば、電子パスポートの場合のように、電子エンティティが機密情報を有する場合、この問題は特に重大である。

【０００６】

したがって、当分野では、望まないデータ交換を回避するための試みがすでに行われており、「スキミング防止」法として知られる。

【０００７】

この考え方の線上において、国際特許出願９９／１６０１９号明細書では、マイクロ回路カードの上面にスイッチを配置することによって、スイッチを活性化した後だけカードがデータを受信することができるようにする提案がされている。しかしながら、電子エンティティにこのスイッチを追加すると、（例えば、ＩＳＯ標準７８１６で規定される電子エンティティを繰り返し曲げる場合など）生産および信頼性のいろいろな問題が発生し、製造コストが上がる。

【０００８】

おそらく、このため、米国特許第６，４２４，０２９号明細書において、特にマイクロ回路カードの場合、情報を持つ電子エンティティの一般的構成によりよく適応した静電容量型スイッチの使用が提案されている。この解決法は、ここで言及した問題を低減するが、これらの問題を完全に回避することに成功していない。

【０００９】

また、ここで概説した解決法は、柔軟性に欠ける。特に、例えば、パスワードによる非接触通信モードのアクセスの制限を想定することができない。

【課題を解決するための手段】

【００１０】

この状況において、本発明によって、接触通信手段を介して、事前の指示の受信機能として、少なくともリモート通信手段を介する一定のデータの交換を認証する手段を特徴とする、接触通信手段およびリモート通信手段を備える電子エンティティが提案される。

【００１１】

したがって、例えば端末による接触接続によって、リモート通信手段を介するデータの交換が可能か否かを管理することができる。

【００１２】

この認証に関係するデータの交換とは、例えば、少なくとも一定のデータの送信および／または少なくとも一定のデータの受信である。

【００１３】

また、想定可能な第１の実施例において、電子エンティティは、前記指示によって制御される活性化情報を格納する手段と、前記活性化情報が存在する場合、前記リモート通信手段を介する前記データの交換（送信および／または受信）を認証する手段と、を備える。

【００１４】

したがって、指示の受信は、例えば時間平面において、データの交換（例えば、送信）から分離することができる。

【００１５】

また、補足的方法として、電子エンティティは、前記活性化情報が存在しない場合、前記リモート通信手段を介する前記データの交換を禁止する手段を備えてもよい。

【００１６】
前記リモート通信手段がアンテナを備える場合、想定可能な第２の実施例によれば、前記交換を認証する手段は、前記指示に基づいてマイクロ回路にアンテナの接続を指示する手段を備える。この場合、データ交換（例えば、送信および／または受信）の認証および禁止は、特に効果的である。
【００１７】
電子エンティティは、例えば、ＩＳＯ標準１４４４３および／またはＩＳＯ標準７８１６に準拠するマイクロ回路カードである。
【００１８】
また、本発明によれば、リモート通信手段を備える電子エンティティと通信する接触通信手段を備える端末であって、前記接触通信手段を介して、少なくとも前記リモート通信手段を介する一定のデータの交換を条件設定するための指示を送信する手段を特徴とする端末が提案される。
【００１９】
この端末によって、電子エンティティのリモート通信手段による交換の認証を管理することができる。この認証に関係する交換は、データの送信および／または受信の場合がある。
【００２０】
この端末は、携帯用であってもよい。特に、電子エンティティのリモート通信手段による交換の認証を管理するアドホック携帯端末である場合がある。
【００２１】
本発明は、接触通信手段および非接触通信手段を備える電子エンティティを制御する方法をさらに提案するが、この方法は、以下のステップを特徴とする。
－前記接触通信手段を介して活性化指示を受信するステップ。
－前記活性化指示を受信したとき、少なくとも前記リモート通信手段を介する一定のデータの交換を認証するステップ。
【００２２】
このように、リモート通信手段を介するデータの交換が可能か否かを活性化指示によって指示するため、既に述べた利点を有する。
【００２３】
この方法では、前記リモート通信手段を介して前記データを交換（送信および／または受信）するステップは、例えば、前記認証するステップによって条件設定される。
【００２４】
実行可能な一実施例において、活性化情報に予め定められた値を設定することによって前記認証するステップを実行し、前記条件設定された送信するステップは、以下のステップを備える。
－前記活性化情報の値が前記予め定められた値と等しいことを確認するステップ。
－前記確認が肯定である場合のみ、前記リモート通信手段を介して前記データを交換（例えば、送信）するステップ。
【００２５】
本方法は、実装するのに実用的であり、認証するステップと交換するステップとを分離する点において既に述べた利点を有する。
【００２６】
本方法は、同様に、特定の時間に、前記活性化情報に前記予め定められた値の補数値を設定するステップを備えることができる。
【００２７】
実行可能な他の実施例において、本方法は、特定の時間に前記データの交換を禁止するステップを含む。
【００２８】
前記特定の時間を前記リモート通信手段による通信コマンドの終了の受信に対応させ、

指示によって通信を１回だけ認証できるようにすることができる。
【００２９】
前記特定の時間をタイムディレイによって決定し、前記認証の期間を制限することができる。
【００３０】
前記リモート通信手段を介して予め定められた数のコマンドを受信した後、前記特定の時間に達することができ、前記認証の使用可能性を制限することができる。
【００３１】
前記特定の時間を、通信を初期化するステップの完了に対応させることができる。
【００３２】
最後に、本発明によれば、非接触通信手段を備える電子エンティティをカスタマイズする方法であって、少なくとも前記リモート通信手段を介する一定のデータの交換を条件設定するための活性化情報を書き込むステップを特徴とする方法が提案される。
【００３３】
したがって、電子エンティティをカスタマイズする間に、デフォルトで非接触通信手段の使用が認証されるか否かを決定することができる。
【００３４】
前記活性化情報は、前記電子エンティティの接触通信手段を介して指示を受信したとき、変更することができる。これは、例えば、安全な指示を指す。
【００３５】
本方法は、前記活性化情報の変更のための条件を示す設定情報を書き込むステップをさらに備えることがある。こうして、使用する回路を変更せずに、カスタマイズ中に後続の使用に従ってリモート通信手段の使用が可能か否かに関して電子エンティティを設定することができる。
【発明を実施するための最良の形態】
【００３６】
本発明の他の特徴や利点に関しては、添付の図面を参照しながら行われる以下の説明を鑑みれば明確になるであろう。
【実施例】
【００３７】
一例として図１に示す電子エンティティは、各々がマイクロ回路の端子に接続されるコンタクト４によって、および、例えば、複数の巻き数を備える巻き線で構成される磁気アンテナ６によって、他の電子装置と通信するのに適応したマイクロ回路２（例えば、通常スマートカードで使用される安全なマイクロコントローラ）を備える。
【００３８】
磁気アンテナ６は、マイクロ回路２の制御端子ＣＭＤを介して制御されるスイッチＫを介して、マイクロ回路の２個の端子に接続される。したがって、マイクロ回路は、端子ＣＭＤで生成される信号コマンドによって、マイクロ回路２にアンテナ６との接続を命じ、これによって、アンテナ６が一部を形成するリモート通信手段の使用を認証したり禁止したりすることができる。
【００３９】
次に、図２を参照しながら、本装置の概略動作について説明する。
【００４０】
まず、本実施例において、電子エンティティは、接触通信手段（１セットのコンタクト４）によって、端末タイプの外部装置に接続されたときだけ、電力が供給されることに留意されたい。この外部装置は、コンタクト４の各々と電気的に接続され、こうして、特に電子エンティティに電力を供給する。
【００４１】
電気スイッチＫは、例えば、電力が供給されない場合（および、特に、例えば端子ＣＭＤに信号が存在しない場合）、開いている。したがって、アンテナ６を備えるリモート通

信手段は、電子エンティティが、（コンタクト４によって）電力を電子エンティティに供給する端末に接続されていない場合、使用することができなくなる。本実施例において、電子エンティティは、アンテナ６によって提供されるリモート電力供給に基づいてのみ動作するよう適応するものでない。

【００４２】

したがって、図１の電子エンティティの作用の概略図において、電子エンティティは、最初に、（コンタクト４を介して）端末に接続される。これによって、図２のステップＥ２に示すように、電子エンティティ（すなわち、マイクロ回路２）と端末（例えば、端末におけるマイクロ回路タイプの手段）との間の通信の初期化が行われる。

【００４３】

初期化ステップの間、スイッチＫは開いており、上記で説明したように非接触通信は禁止される。マイクロ回路２が、例えば、論理レベル０を示す電位などスイッチＫを開くための電位を端子ＣＭＤに印加することによって、スイッチＫは開く。

【００４４】

このとき、電子エンティティは、「接触」モードにおいて正常に動作することができる。このモードの間、例えば、電子エンティティと電子エンティティが接続されている端末との間でデータの交換が行われる（ステップＥ４）。

【００４５】

ステップＥ６に示すように、これらのデータ交換の間、電子エンティティは、特に非接触モード通信を認証する指示を受信する場合がある。

【００４６】

例えば、電子エンティティのマイクロ回路２の動作が端末から受信したオペレーションコードによって制御される場合、上記の指示は、特定のオペレーションコードとして受信される。代替方法として、この指示は、マイクロ回路２が、データが正当であれば「非接触」モード通信を認証する指示として解釈されるデータアイテム（例えば、端末上のユーザによって入力された秘密コードなど）でもよい。

【００４７】

ステップＥ６の間にこの指示を受信すると、ステップＥ８において、マイクロ回路は、（例えば、端子ＣＭＤを論理レベル１に対応する電位にすることによって）スイッチＫを閉じるよう命じる。こうして、アンテナ６は、マイクロ回路２に両端で接続される。これによって、電子エンティティは、アンテナ６を介して、すなわち非接触通信手段を介して、外部装置と通信することができる。

【００４８】

本実施例では、以下に記載するように、スイッチＫは、非接触通信手段を介する通信が終了するまで閉じた状態を維持する。代替方法として、（終了時に端子ＣＭＤの電位が論理レベル０に戻るタイムディレイによって）予め定められた時間だけ非接触通信を認証することができる。第２の実施例を参照して説明したように、他の変形も想定することができる。

【００４９】

ステップＥ１０で示すように、一旦スイッチＫが閉じられると、電子エンティティは、（接触通信端末に関連するかしないかに関わらず）その目的のために設計された読取装置との非接触通信をセットアップすることができる。こうして、図２のステップＥ１２に示すように、電子エンティティと読取装置との間の「非接触」モードにおけるデータ交換が可能になる。

【００５０】

ステップＥ１４で示すように、電子エンティティと読取装置との間の非接触モードの対話が終了した時、すなわち、これら２台の装置が目的のデータ交換を実行し終わった時、電子エンティティは、例えば、ＩＳＯ標準１４４３－４において規定される「ＤＥＳＥＬＥＣＴ」指示などの「トランザクション終了」指示を受信する。

【００５１】

ステップＥ１６で示すように、マイクロ回路２は、この指示を受信すると、（ここで説明する一例では端子ＣＭＤ上に論理レベル０を印加することによって）スイッチＫを開くように命じ、アンテナ６がもはやマイクロ回路２に接続されていないという事実によって、非接触通信を禁止する。

【００５２】

既に示したが、以下に述べるように、代わって、電子エンティティが読取装置の範囲から離れるか、通信の認証後の一定の時間などの他の条件に従って、（ここでは、スイッチＫを開くことによって）非接触通信を禁止することができる。

【００５３】

ステップＥ４おいて、動作は、「接触」モードの管理で再開される。

【００５４】

また、電子エンティティが接触端末にも接続されているにも関わらず、リモート読取装置が電子エンティティと通信しなければならないとき、これまでに説明した本実施例が特に優位であることに留意されたい。それは、例えば、リモート読取装置を搭載するガントリの下を車両が通過するとき、マイクロ回路カードがこの車両の適切な端末に挿入されている場合の問題である。したがって、（例えば、バリアを開いたり通行料金を払ったりするための）電子エンティティとリモート読取装置との間のデータ交換は、例えば端末上のユーザによる秘密コードの入力やハンドル上の制御スイッチの操作など、車両に配置される接触端末が管理する特定の条件に左右される場合がある。

【００５５】

次に、図３～６を参照して、本発明の第２の実施例について説明する。

【００５６】

図３に、電子エンティティの第２の実施例の主要な要素を示す。この電子エンティティは、マイクロ回路１２（例えば、マイクロプロセッサ）を備える。マイクロ回路１２をコンタクト１４によって端末タイプの外部装置に接続することによって、電子エンティティと端末との間の「接触」通信をセットアップすることができる。

【００５７】

また、電子エンティティは、各終端でマイクロ回路１２の対応する端子に接続されるアンテナ１６を含む（上記の第１の実施例とは対照的に、アンテナ１６とマイクロ回路１２との間の接続の遮断は想定されない）。

【００５８】

アンテナ１６は、電子エンティティのリモート通信手段の一部である。

【００５９】

また、書き換え可能なメモリ１８（例えば，電気的消去可能プログラム可能タイプ（ＥＥＰＲＯＭ）の不揮発性メモリ）は、マイクロ回路１２に接続される。

【００６０】

本実施例において、マイクロ回路１２は、接触接続によって（コンタクト１４の少なくとも１つを介して）電力を供給できたり、または、この電力供給が可能であるか否かに関係なく、（第１の実施例とは対照的に、）磁気アンテナ１６を使用するリモート電力供給によって電力を供給できたりすることに留意されたい。このため、ここでは、（コンタクト１４を介する）接触接続を同時に使用することを条件としないで、「非接触」通信モードを使用することができる。

【００６１】

したがって、接触接続またはリモート電力供給によって電力を電子エンティティに供給することができる。その結果、図５および図６を参照してそれぞれ説明する２つの主要な動作モードになる。上記の２つのモードの動作原理を検討しなくても、接触接続やリモート電力供給によって同時に電力を供給することは、当然、実行可能である。

【００６２】

電子エンティティがコンタクト１４を介して端末と通信しているとき、図５に示す方法が、マイクロ回路１２の（例えば、メモリに格納された指示によってプログラミングされ

た）制御の下で行われる。
【００６３】
事前に、例えば、電子エンティティに格納されたデータを初期化するステップ（例えば、販売前にマイクロ回路カードの製造において従来実行されるカスタマイズステップ）の間に、書き換え可能メモリ１８に格納される活性化ビットは、例えば、０に設定される。これは、（以下でさらに詳細に説明するように、）デフォルトでリモート通信が禁止されることを示す。
【００６４】
同様に、カスタマイズステップの間、どの程度、電子エンティティのリモート通信手段の使用を接触接続を介して認証することができるかを（例えば、活性化ビットが格納されるファイルへアクセスする権利の形式で）示す設定情報を書き込むための規定条件をカスタマイズしてもよい。例えば、以下が挙げられる。
－常時。例えば、活性化ビットを含むファイルに自由にアクセスすることができる（しかしながら、後で説明するように、この場合、電子エンティティの制御プログラムによって秘密コードの入力に基づいて送信の条件を設定することができる）。
－読取装置（または、適用可能な場合、読取装置にコードを入力するカードホルダ）の認証の後。本実施例の変形例として後で説明するが、認証されたユーザにのみリモート通信手段の使用を認証する。
－全く認証しない。例えば、適切であれば、活性化ビットを含むファイルへのアクセスを禁止することによって、活性化ビットを変更して非接触通信手段の使用を認証することができないようにする。
【００６５】
以下に説明する状況では、電子エンティティの制御プログラムは、活性化ビットに自由にアクセスすることができる。
【００６６】
図６を参照して説明したように、「接触」モードにおける動作のある時点で（この場合、マイクロ回路１２は、端末から電力が供給され、コンタクト１４を介して端末とデータを交換する）、マイクロ回路は、端末から指示を受信して非接触通信を活性化することができる。この指示とは、すなわち、アンテナ１６を介する「非接触」モードでの動作の認証を指示するためのデータアイテム（または、より一般的には情報アイテム）である（ステップＥ２０）。
【００６７】
ここで説明する一例では、ユーザによって（例えば、キーパッドによって）端末に供給されたコードを活性化の指示と関連付けて送信し、正しいコードがユーザによって供給された場合のみ、「非接触」モードでの動作の認証が有効になるようにする。すなわち、この正しいコードとは、マイクロ回路１２に関連付けられた書き換え可能なメモリ１８（または読取り専用メモリタイプであって、マイクロ回路１２に関連付けられた他のメモリ）に（適用可能であれば保護された形式で）保存されている予め定められたコードである。
【００６８】
ユーザによって供給されたコードと共に活性化の指示を受信すると、マイクロ回路１２は、供給されたコードが正しいことを確認するステップＥ２２に進む。すなわち、このステップとは、供給されたコードと既に述べたように電子エンティティに格納されたコードとを比較するステップである。
【００６９】
供給されたコードが、電子エンティティに格納された秘密コードに対応している場合、ステップＥ２４において、電子エンティティが非接触通信の活性化に関する正しい情報を実際に受信したことを意味するよう上記の活性化ビットに１を設定することによって、非接触通信の認証が有効になる。
【００７０】
一方、ステップＥ２０において、ユーザによって供給され活性化の指示と共に電子エン

ティティに送信されたコードが、電子エンティティに格納されたコードと一致しない場合、次に、ステップＥ２６において、書換え可能メモリ１８中の活性化ビットに０を設定する。すなわち、この段階では、正しい活性化情報が受信されていないと考えられることを意味する。

【００７１】

どちらの場合も、活性化ビットは、「ＳＥＬＥＣＴ」タイプのコマンドによって活性化ビットを含むファイルを選択した後、（ＩＳＯ標準７８１６－４で定義される）「ＵＰＤＡＴＥ　ＢＩＮＡＲＹ」タイプの指示によって変更される。

【００７２】

活性化ビットが初期化ステップの間に０に設定される上記の状況においては、先験的に活性化ビットの値を変更しないので、ステップＥ２６は必要でないことに留意されたい。しかしながら、このステップを使用して、例えば、前のフェーズ中に正しいコードが与えられた場合でさえ、不正確なコードを使用した場合はいつでも確実に活性化ビットを０に設定するようにしなければならない場合がある。また、ステップＥ２６が存在するか否かに関わらず、不正確なコードを受信したとき、例えば、カードから端末にコンタクト１４を介してエラーメッセージを送信するなど、他の結果になる場合もある。

【００７３】

さらに、簡潔さのために、コードが正しいことを確認するステップを繰り返し実行することが可能か否かを特定せずに、１回のステップについて説明した。しかしながら、もちろん、ユーザが制限された回数だけ正しい秘密コードの入力を試行できるようにすることが可能であると想定できる。この場合、例えば、制限された回数の試行を行ったがそれでもなおコードが間違っているとき、電子エンティティをロックする結果となる。

【００７４】

次に、図６を参照して、動作の「非接触」モードについて説明する。以下で示すように、この動作モードは、リモート読取装置の範囲内に入った電子エンティティがトリガとなって開始される。これは、図５の各ステップを実行することによって事前に非接触接続を活性化したか否かに関わらず、開始される。

【００７５】

電子エンティティが読取装置のフィールドに入ったとき（ステップＥ３０）、リモート電力供給によって電子エンティティに電力が供給され（電子エンティティによる読取装置の検出と考えることができる）、マイクロ回路１２は、「非接触」モードで動作を開始する。

【００７６】

動作の開始時（好ましくは、例えば、ＩＳＯ標準１４４４３－３で定義されるように、初期化プログラムおよびコリジョン防止プログラムの実行中など、マイクロ回路１３によって実行されるプログラムの最初のステップ中）に、マイクロ回路１２は、書換え可能メモリ１８において活性化ビットを読み取りにいく（ステップＥ３２）。

【００７７】

次に進み、ステップＥ３４において、（既に示したように、非接触通信の活性化に関する情報を示す）活性化ビットの値を確認する。

【００７８】

（電子エンティティの初期化中に値が書き込まれ、正しい活性化指示の受信によって変更されなかったため、あるいは、間違ったコードが入力された後、または、新たな権限を与えられずに事前に認証されたデータを交換した後、このビットが０にリセットされたため）活性化ビットが０である場合、非接触通信は、ステップＥ３６で終了する。この場合、最初のステップだけ実行され、データの交換は行われない。

【００７９】

一方、マイクロ回路１２が、書換え可能メモリ１８に格納された活性化ビットが１の値である（すなわち活性化情報が存在する）ことを確認した場合、非接触通信は、継続される。すなわち、最初にステップＥ３８において（例えば、ＩＳＯ標準１４４４３－４に従

って、「Half-Duplex Block Transmission Protocol」の実行レベルに達するため）非接触接続プロトコルの初期化を行うことを意味する。

【００８０】

いったん非接触通信が確立されると（例えば、ステップＥ３８の後）、次に、図６のステップＥ４０で示すように、書換え可能メモリ１８中の活性化ビットに０を設定する。プロトコルの初期化後ステップＥ４０を実行することによって、確実に、電子エンティティが読取装置のフィールドから離れた後、（接触接続によって新たに活性化指示を受信しなければ）非接触通信を再度確立することを認証しないようにする。

【００８１】

しかしながら、既に示したように、他の条件下で、活性化ビットに０を設定（すなわち、非接触通信の再度の確立を禁止）する場合もある。例えば、活性化指示の受信時間（又は、適用可能であれば非接触接続の設定）に対するタイムディレイ、マイクロ回路１２による予め定められた数の指示（すなわち、「Application Protocol Data Unit（ＡＰＤＵ）」コマンド）の実行、またはトランザクションメッセージ終了の受信（第１実施例の場合）などの条件である。

【００８２】

他の変形例として、非接触モードにおける動作中ではなく、むしろ「接触」モードにおいて非活性化指示を受信したとき、活性化ビットを０にリセットすることを想定できる。（例えば，図６を参照して説明するように）非接触動作中に活性化ビットが０にリセットされる場合でも、非活性化指示が与えられることがある。

【００８３】

上述の例において、ステップＥ３８でいったんプロトコルが初期化されると、ステップＥ４０で活性化ビットが０にリセットされる。それにもかかわらず、次に、ステップＥ４２で非接触プロトコルに従ってデータの交換が行われる。しかしながら、次のことに留意されたい。例えば、電子エンティティが読取装置のフィールドから離れたり、または代替方法として、非接触通信終了コマンドを受信したりして、ステップＥ４２のデータ交換を終了した場合、ステップＥ４０で活性化ビットが０にリセットされているため、電子エンティティが読取装置のフィールドに戻って新たにステップＥ３０～Ｅ３４を反復すると、非接触通信に失敗しステップＥ３６に行く。

【００８４】

ここまで説明した本実施例では、活性化ビット（正しい活性化指示を前に受信したことを示すインジケータとして使用される）によって、非接触モードにおけるすべてのデータ交換を条件設定する。代替方法として、電子エンティティのある特定のデータの交換のみを活性化ビットで条件設定するよう規定してもよい。一方、非接触接続を介して特定の指示を事前に受信していない場合でも、電子エンティティがリモート読取装置の近くを通過するとき、電子エンティティによって他のデータを自由に通信することができるようにしてもよい。

【００８５】

したがって、電子エンティティが電子身分証明書である場合、この書類上に存在するデータ（対象者の名前など）を通信するのに、必ずしも特定の認証を事前に活性化しない場合がある。一方、他のデータ（例えば，バイオメトリックデータタイプの秘密情報－指紋、虹彩、または顔の画像）の送信は、電子エンティティがこの意味において有効な活性化指示を事前に接触接続を介して受け取ったという条件を満たす場合のみ、電子エンティティによって非接触接続を介して行われてもよい。

【００８６】

この場合、活性化情報が存在しても（すなわち、活性化ビットの値が１であっても）、非接触接続の設定を条件設定するものでなく、秘密データを送信するステップを条件設定するものである。

【００８７】

例えば、このデータを一回のみ送信するため認証に対応する活性化指示の規定があって

もよい。すなわち、活性化ビットは秘密データを送信した直後０にリセットされる。

【００８８】

変形例（適用可能な場合、ここまで説明した本実施例と組み合わせ可能）では、活性化情報によって非接触接続を介するデータ受信を条件設定するよう規定することもできる。例えば、これによって、悪意のある第三者が、電子エンティティの権限を与えられた所有者に知られずに、非接触接続を介して電子エンティティに識別コードを示さないよう防止することができる。例えば、第三者が間違ったコードを何回も示した後は電子エンティティをロックしてしまうというリスクを侵して、防止することができる。

【００８９】

また、交換の認証が関連するデータは、電子エンティティのアプリケーションデータ（すなわち、特に、電子エンティティによってその情報媒体機能で運ばれるデータ）に限定する必要はなく、通信プロトコルを設定するためのデータなど、他のタイプのデータを同様に含んでもよい。

【００９０】

以上、想定される変形例と共に説明した本実施例は、本発明の実現の実行可能な例にすぎず、これらに限定されるものではない。

【図面の簡単な説明】

【００９１】

【図１】本発明の教示による電子エンティティの第１の例を示す図である。

【図２】図１の電子エンティティの一般的作用を示すフローチャートである。

【図３】本発明の教示による電子エンティティの第２の例を示す図である。

【図４】図３の電子エンティティの実施可能な物理構成の一例を示す図である。

【図５】図３の電子エンティティの作用の前半を規定するフローチャートである。

【図６】図３の電子エンティティの作用の後半を規定するフローチャートである。

【図１】

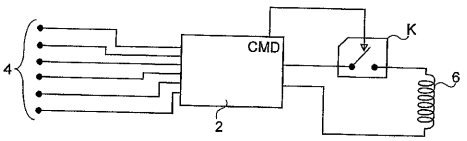


Fig. 1

【図２】

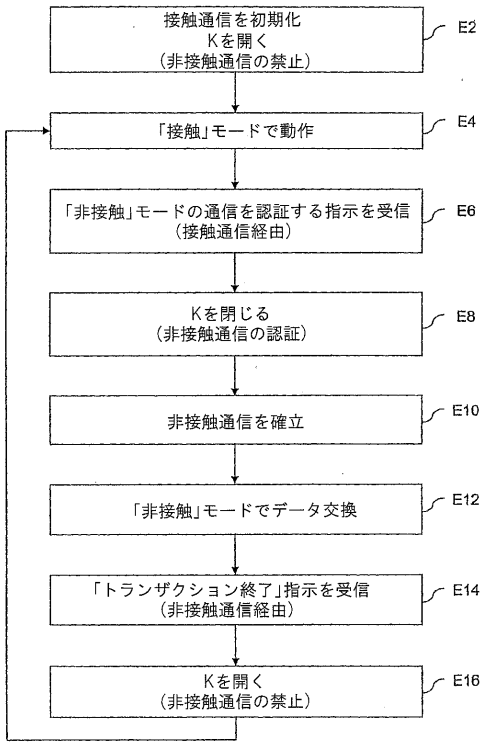


Fig.2

【図３】

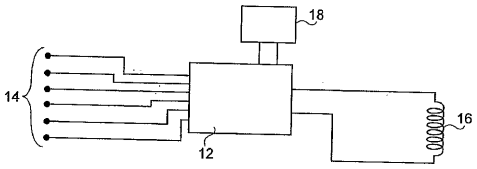


Fig. 3

【図４】

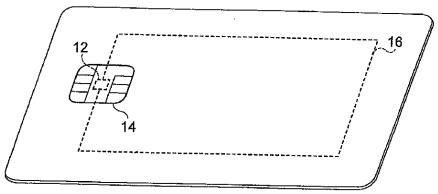


Fig. 4

【図５】

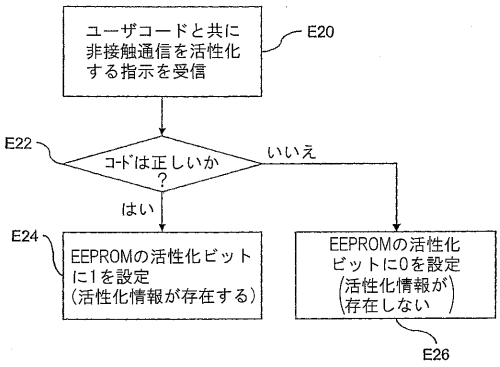


Fig.5

【図６】

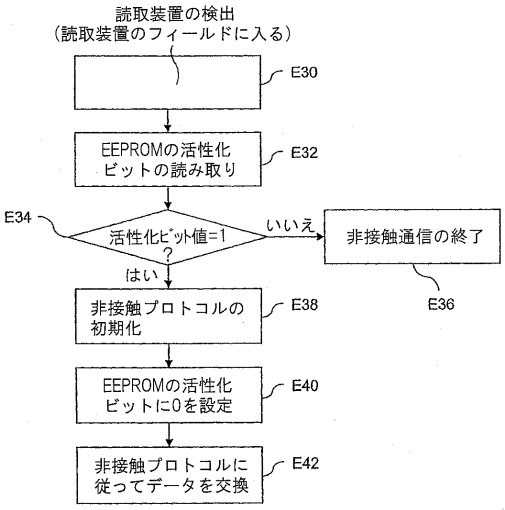


Fig.6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/001797

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K19/07 G06K19/073

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)
G06K

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)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 1 258 831 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD) 20 November 2002 (2002-11-20) paragraph [0001] paragraph [0019] - paragraph [0036] paragraph [0043] - paragraph [0088] paragraph [0120] - paragraph [0126] paragraph [0132]	1-3,5-20 4
Y A	EP 0 945 828 A (KABUSHIKI KAISHA TOSHIBA) 29 September 1999 (1999-09-29) paragraph [0052] - paragraph [0072]	4 1-3,5-20

-/--

[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 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
15 November 2006	23/11/2006

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Geiger, Hans-Walter

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/001797

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 206 495 A (KREFT ET AL) 27 April 1993 (1993-04-27) column 2, line 3 - line 26 column 2, line 59 - column 4, line 21	1-20
A	FR 2 809 516 A (INNOVATRON ELECTRONIQUE) 30 November 2001 (2001-11-30) page 1, line 1 - page 4, line 30	1-20
A	US 6 138 918 A (TARBOURIECH ET AL) 31 October 2000 (2000-10-31) column 2, line 21 - column 3, line 54	1-20
A	DE 100 28 821 A1 (MIDITEC DATENSYSTEME GMBH) 20 December 2001 (2001-12-20) paragraph [0001] - paragraph [0012] paragraph [0019] - paragraph [0027]	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2006/001797

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1258831	A	20-11-2002	US	2002170975 A1	21-11-2002
EP 0945828	A	29-09-1999	CN	1231459 A	13-10-1999
			TW	569143 B	01-01-2004
			US	6375082 B1	23-04-2002
US 5206495	A	27-04-1993	DE	3935364 C1	23-08-1990
			EP	0424726 A1	02-05-1991
			JP	2755809 B2	25-05-1998
			JP	3209592 A	12-09-1991
FR 2809516	A	30-11-2001	NONE		
US 6138918	A	31-10-2000	GB	2321744 A	05-08-1998
DE 10028821	A1	20-12-2001	NONE		

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/001797

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06K19/07 G06K19/073

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 258 831 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD) 20 novembre 2002 (2002-11-20)	1-3,5-20
Y	alinéa [0001] alinéa [0019] - alinéa [0036] alinéa [0043] - alinéa [0088] alinéa [0120] - alinéa [0126] alinéa [0132]	4
Y	EP 0 945 828 A (KABUSHIKI KAISHA TOSHIBA) 29 septembre 1999 (1999-09-29)	4
A	alinéa [0052] - alinéa [0072]	1-3,5-20

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 novembre 2006	23/11/2006

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Geiger, Hans-Walter

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/001797

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 206 495 A (KREFT ET AL) 27 avril 1993 (1993-04-27) colonne 2, ligne 3 - ligne 26 colonne 2, ligne 59 - colonne 4, ligne 21	1-20
A	FR 2 809 516 A (INNOVATRON ELECTRONIQUE) 30 novembre 2001 (2001-11-30) page 1, ligne 1 - page 4, ligne 30	1-20
A	US 6 138 918 A (TARBOURIECH ET AL) 31 octobre 2000 (2000-10-31) colonne 2, ligne 21 - colonne 3, ligne 54	1-20
A	DE 100 28 821 A1 (MIDITEC DATENSYSTEME GMBH) 20 décembre 2001 (2001-12-20) alinéa [0001] - alinéa [0012] alinéa [0019] - alinéa [0027]	1-20

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2006/001797

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1258831	A	20-11-2002	US	2002170975 A1	21-11-2002
EP 0945828	A	29-09-1999	CN	1231459 A	13-10-1999
			TW	569143 B	01-01-2004
			US	6375082 B1	23-04-2002
US 5206495	A	27-04-1993	DE	3935364 C1	23-08-1990
			EP	0424726 A1	02-05-1991
			JP	2755809 B2	25-05-1998
			JP	3209592 A	12-09-1991
FR 2809516	A	30-11-2001	AUCUN		
US 6138918	A	31-10-2000	GB	2321744 A	05-08-1998
DE 10028821	A1	20-12-2001	AUCUN		

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	G06F 15/00 330C	

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

(74)代理人 100122965
弁理士 水谷 好男
(72)発明者 ゴエ，クリストフ
フランス国，エフ－６９００４ リヨン，リュ アンリ シェバリエ，３３

Ｆターム(参考) 5B035 BB09 CA25 CA38
5B058 CA13 CA15 CA27 KA31
5B285 AA01 BA05 CA04 CB01 CB75
5J104 AA07 AA16 EA03 KA02 NA40