(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2019-194858
(P2019-194858A)
(43)公開日　令和1年11月7日(2019.11.7)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 20/38	(2012.01)	G06Q	20/38	310	5L055

審査請求 未請求　請求項の数 26　ＯＬ　外国語出願　（全 34 頁）

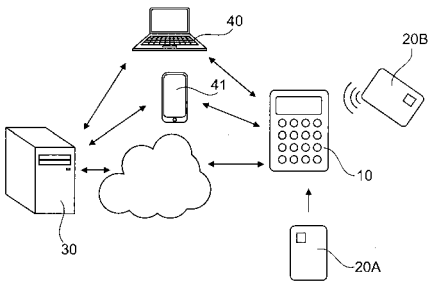
(21)出願番号　特願2019-87763(P2019-87763)
(22)出願日　令和1年5月7日(2019.5.7)
(31)優先権主張番号　1853789
(32)優先日　平成30年5月2日(2018.5.2)
(33)優先権主張国・地域又は機関
フランス(FR)
(31)優先権主張番号　16/171,427
(32)優先日　平成30年10月26日(2018.10.26)
(33)優先権主張国・地域又は機関
米国(US)

(71)出願人　519163212
マルブフ・コンセイユ・エ・ルシェルシュ
フランス・７５００９・パリ・リュ・ドゥ・モーボウジュ・４２
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉
(74)代理人　100133400
弁理士　阿部　達彦
(72)発明者　ブリュノ・サングレ・フェリエール
フランス・７５０１６・パリ・ブールバール・ボーセジュール・４７

Ｆターム(参考)　5L055 AA71

(54)【発明の名称】安全なデータ交換を実行するための方法およびシステム

(57)【要約】　（修正有）
【課題】安全なデータ交換を実行するための方法およびシステムを提供する。
【解決手段】システムは、第１及び第２の電子デバイス２０Ａ，２０Ｂと、電子デバイスのそれぞれの接続のための手段を含むデュアルリーダ１０と、ヒューマンマシンインタフェース及び安全な交換に関する情報を伝達するサーバ３０とを含む。デュアルリーダのインタフェース又はそれに接続される外部装置を使用して、第１および第２の電子デバイスの間で実行される交換に関する情報の項目をデュアルリーダに入力するステップと、デュアルリーダを用いて第１の電子デバイスに、交換に関する情報の項目を登録するステップと、デュアルリーダを用いて第２の電子デバイスに、交換に関する情報の項目を登録し、そうでなければ交換をキャンセルするステップと、トランザクションに関するデータをサーバに送信するステップとを含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
システム内で少なくとも1つの安全な交換を実行するための方法であって、前記システムが、第1および第2の電子デバイス(20A、20B)および前記デバイスのそれぞれとの接続のための手段を含むデュアルリーダ(10)、および前記交換に関する情報が伝達されることが可能である少なくとも1つのサーバ(30)を含み、前記方法が、
a) 前記リーダ(10)のインタフェースまたは前記リーダ(10)に接続される外部装置を使用して、前記第1および第2のデバイス(20A、20B)の間で実行される交換に関する情報の項目を前記リーダ(10)に入力するステップと、
b) 前記リーダ(10)を用いて前記第1のデバイス(20A)に、前記交換に関する情報の項目を登録するステップと、
c) 前記第2のデバイス(20B)に、前記交換に関する情報の項目を登録するか、そうでなければ前記交換をキャンセルするステップと、
d) トランザクションに関するデータを前記サーバ(30)に送信するステップと
を含み、
前記デュアルリーダは、トランザクションが2つの電子デバイスの間で実行される間、またはこのようなトランザクション外で、外部サーバに接続するように構成される、
方法。
【請求項２】
前記第1のデバイス(20A)における前記登録の有効性が、前記第2のデバイス(20B)における前記交換に関する情報の前記項目の前記登録に対して条件付きであり、前記第1のデバイス(20A)における前記登録の前記有効性は、前記第2のデバイス(20B)における前記登録の後、前記デュアルリーダによって、または、その後に前記サーバおよび別のデュアルリーダによって、前記第1のデバイス(20A)に伝達される、請求項1に記載の方法。
【請求項３】
前記交換に関する情報の前記項目が同じ一つのレジスタまたは同じ一つのファイルに関する以前の交換に関する情報を含む、請求項1に記載の方法。
【請求項４】
前記サーバ(30)は、このトランザクションのいずれかのトランザクションへのチェイニングが、トランザクションと関連した、サーバでパラメータ化された少なくとも1つのルールに従っていないことを生じさせる場合、前記電子デバイスにおいて記録されたトランザクションをキャンセルする、請求項3に記載の方法。
【請求項５】
前記電子デバイス、前記サーバおよび前記デュアルリーダから選択される前記システムの2つの要素は、それらが他の要素に配置されている秘密鍵に対応する公開鍵を各々有し、この秘密鍵がユニークで前記要素だけに配置されているかもしくは前記システムの他の要素によって共有されている場合、または、前記2つの要素がそれらの間で、もしくはそれらと前記システムの他の要素との間で共有される同じ一つの秘密鍵をそれぞれ知っている場合、互いに通信することが認可される、請求項1から4のいずれか一項に記載の方法。
【請求項６】
前記デュアルリーダ(10)がクロックを含み、前記第1および第2のデバイスにおいて登録される前記情報が前記交換の時間でタイムスタンプされる、請求項1から5のいずれか一項に記載の方法。
【請求項７】
前記デュアルリーダは他の電子デバイスのレジスタから、または前記レジスタに、第1の電子デバイスのレジスタにおいて登録された数量の転送を実行し、各転送の終了において、受領される前記数量だけインクリメントされ、送られた数量がその値から差し引かれている前記レジスタの各初期値が、転送時に前記デュアルリーダに存在する特定のルールに従っていることを確実にする、請求項1から6のいずれか一項に記載の方法。
【請求項８】

第1の安全な接続および第2の安全な接続が時間的に重複している、請求項1から7のいずれか一項に記載の方法。

【請求項９】

ステップa)は、前記第1のデバイスおよび／または前記第2のデバイスが前記リーダに情報を伝達するステップの後にある、請求項1から8のいずれか一項に記載の方法。

【請求項１０】

前記情報が前記デバイスにおいて記録される文書の目録に関連し、その結果、前記リーダが前記文書をメニューに組み込むことが可能である、請求項9に記載の方法。

【請求項１１】

第1の接続が接触を基にしたものであり、第2の接続が非接触である、請求項1から10のいずれか一項に記載の方法。

【請求項１２】

前記デュアルリーダのヒューマンマシンインタフェースが、前記交換に関する情報の前記項目を入力するためのキーパッドを含む、請求項1から11のいずれか一項に記載の方法。

【請求項１３】

前記デュアルリーダのヒューマンマシンインタフェースがスクリーンを含み、前記システムが、前記第1および第2のデバイスのベアラをそれぞれ対象とする2つのメッセージを表示するように構成される、請求項1から12のいずれか一項に記載の方法。

【請求項１４】

前記電子デバイスがクレジットカードまたはSIMカード形式である、請求項1から13のいずれか一項に記載の方法。

【請求項１５】

前記電子デバイスとの安全な交換が、コンピュータ接続によってリンクされる2つのデュアルリーダを通して異なる位置において行われる、請求項1から14のいずれか一項に記載の方法。

【請求項１６】

前記電子デバイスの1つが所有者を有し、前記所有者の識別情報は、前記第2の電子デバイスが前記トランザクションを行う前に前記第2の電子デバイスの保有者に示される、請求項15に記載の方法。

【請求項１７】

前記デュアルリーダが前記サーバに知らせるための中継器としての役割を果たし、前記サーバは電子デバイスから生じるトランザクションを列挙し、前記電子デバイスは、前記サーバと通信しているが必ずしも前記トランザクションを生成していない、請求項1から16のいずれか一項に記載の方法。

【請求項１８】

前記ステップd)が、前記トランザクションの後に行われる、請求項1から17のいずれか一項に記載の方法。

【請求項１９】

請求項1から18のいずれか一項に記載の方法を実施するシステムであって、

- 少なくとも1つのデュアルリーダ(10)と、
- 少なくとも2つの電子デバイス(20A、20B)と、
- 少なくとも1つのコンピュータサーバ(30)と

を含み、

前記デュアルリーダは、前記第1のデバイス(20A)への第1の安全な接続を確立し、前記第2のデバイス(20B)への第2の安全な接続を確立し、前記第1と第2の電子デバイス(20A、20B)の間で実行される交換に関する情報の項目が、前記リーダのインタフェースまたは前記リーダに接続される外部装置を使用して前記リーダに入力されることを可能にし、前記第1のデバイス(20A)において前記交換に関する情報の項目を登録し、前記第2のデバイス(20B)において前記交換に関連する情報の項目を登録し、前記交換をキャンセルしない場合

には前記サーバ(30)に前記交換に関する前記情報を伝達するように構成され、
前記デュアルリーダ(10)は、トランザクションが前記2つの電子デバイスの間で実行される間、またはこのようなトランザクション外で、外部サーバに接続するように構成される、
システム。
【請求項２０】
前記サーバはデータネットワークへの接続によってアクセス可能であり、コンピュータまたは電話を介して前記電子デバイスの少なくとも1つのデータ同期を可能とする、請求項19に記載のシステム。
【請求項２１】
前記デュアルリーダが、前記電子デバイスの1つとの接触を基にした通信および他の電子デバイスとの非接触通信を同時に可能にするように構成される、請求項19または20に記載のシステム。
【請求項２２】
前記デュアルリーダまたは前記電子デバイスが、ユーザを識別するための生体認証手段を含む、請求項19から21のいずれか一項に記載のシステム。
【請求項２３】
前記サーバは口座にリンクされるトランザクションの全てを記録し、これらのトランザクションはトランザクション時にまたはその後に前記サーバに報告される、請求項19から22のいずれか一項に記載のシステム。
【請求項２４】
前記サーバは口座にリンクされるトランザクションの全てだけではなく、前記電子デバイスのレジスタに登録されるファイルおよび数量も記録する、請求項19から23のいずれか一項に記載のシステム。
【請求項２５】
前記デュアルリーダが、前記デュアルリーダの秘密鍵を含む物理的に保護されているメモリを含む、請求項19から24のいずれか一項に記載のシステム。
【請求項２６】
前記メモリの物理アクセスは、前記メモリが含む情報がそこからコピーできる前にその破壊に導く、請求項25に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、安全なデータ交換を実行するための方法およびシステムに関する。
【背景技術】
【０００２】
支払カードは、安全な支払をするために、今日では、極めて広く使われている。カードが挿入されるかまたは非接触通信の場合には近くにカードが持ってこられるリーダを用いて、カードと関連付けられた銀行口座をデビット処理するかまたはクレジット処理することができる。大抵の場合、このリーダはトランザクションの間、リモートサーバと通信しなければならず、このことにより、利用可能なネットワークがない場合、時にはリモートサーバをブロックする。
【０００３】
さらに、現在、特定の金銭の総計が別の人の口座への支払のために支払カードと関連した口座からデビット処理されなければならないときには、上記別の人は、自分の支払カードで受領される総計を使用することが可能となるためには、対応する総計が有効に転送されるのを待たなければならないことが多い。
【０００４】
したがって、キャッシュ支払は、ネットワークが存在せず、そして、人々が受領した金銭をすぐに再利用することができるのを望む多くの場合に好まれるが、現金を運搬するこ

とに関連した欠点があり、特に紛失または偽札の危険を伴う。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
これらの欠点の全部または一部を正し、さらに一般的に言えば金融トランザクションを促進するための新規の手段を見つけ、さらに一般的に言えば、任意のコンピュータファイルまたはそのようなファイルにリンクされているかまたはそれとは独立した少なくとも1つのレジスタにおいて登録された任意の数量を、安全に送信するという必要性がある。
【課題を解決するための手段】
【０００６】
本発明はこの必要を満たすことを目的としており、その態様の1つに従って、第1および第2の電子デバイスおよびそのデバイスのそれぞれとの接続のための手段を含むデュアルリーダ、ならびに好ましくはヒューマンマシンインタフェースおよび少なくとも1つの安全な交換に関する情報が伝達されることが可能な少なくとも1つのサーバを含むシステムにおいて、上記交換を実行する方法によってこの目的を達成するものであり、この方法は次のステップを含む。
a) おそらく、リーダを用いて第1のデバイスに対する第1の安全接続を確立するステップ。
b) おそらく、リーダを用いて第2のデバイスに対する第2の安全接続を確立するステップ。
c) リーダのインタフェースまたはリーダに接続される外部装置を使用して、第1および第2のデバイスの間で実行される交換に関する情報の項目をリーダに入力するステップ。
d) リーダを用いて第1のデバイスに、交換に関する情報の項目を登録するステップ。
e) 特にリーダを用いて第2のデバイスに、交換に関する情報の項目を登録するか、そうでなければ交換をキャンセルするステップ。
f) おそらく、特にリーダを用いて第1のデバイスにおいて、交換に関する情報の項目を確認するステップ。
g) 上記トランザクションに関するデータを前記サーバに送信するステップ。
【０００７】
「交換」は、2つのデバイスの間の、コンピュータファイルの、あるいは、上記デバイスの1つまたは複数のレジスタにおいて登録された1つまたは複数の数量の、転送またはコピーを意味すると理解すべきであり、この転送は部分的であるか全体であることが可能である。この交換は、文書の交換または転送に対応することができるが、また支払または他のいかなる金融もしくは非金融トランザクションにも対応することができる。
【０００８】
好ましくは複数のサーバがある。以下では、1つのサーバについて説明されることは、複数のサーバがあるときにも適用できる。
【０００９】
方法は、好ましくはステップa)および／またはb)を含む。第1および／または第2のデバイスはリーダに、情報を、特に、デバイスにおいて記録される文書の目録に関する情報を伝達することができて、そのためリーダは文書をメニューに組み込むことが可能である。
【００１０】
ステップa)およびb)は、特に、転送可能なファイルおよび数量のリストが電子デバイスと独立してリーダに公知である場合、例えばシステムが特定のタイプのファイルまたは数量の転送に制限される場合に、または、ユーザは上記ファイルまたは数量が電子デバイスに存在すると仮定することが可能である場合に、省略することができる。
【００１１】
ステップe)において、登録が行われることができない場合、デュアルリーダは、例えば、システムでパラメータ化されたある時間、例えば1分間などの時間の間、第2の電子デバ

イスで示されることなしに待機したことでこれを検出する。それからそのデュアルリーダは、第1の電子デバイスに送信されるステップのトランザクションを、第2の電子デバイスが、デュアルリーダに接続しているか、または再びデュアルリーダの近くに持ってこられるか、そうでなければその後に、別のデュアルリーダおよびサーバにより、第1のデュアルリーダが直接または間接的に、キャンセル情報の項目をサーバに送信した後に、第2の電子デバイスがサーバと同期するときに第2の電子デバイスに送信されるか、または第1の電子デバイスがサーバと同期するときに第1の電子デバイスに送信される場合に、キャンセルする。デュアルリーダは、他の電子デバイスに関するキャンセル情報の項目を、それらが情報ベクトルとして使われるということに関する以外の影響を他の電子デバイスに与えることなく登録することもでき、このキャンセル情報の項目は、それらが後で使われるときにサーバに渡すことが可能である。したがって、第1のデバイスにおける登録の有効性は、第2のデバイスにおける、交換に関する情報の項目の登録に対して条件付きであり、第1のデバイスにおける登録の有効性は、第2のデバイスにおける登録の後、デュアルリーダによって、または、その後にサーバおよび次に別のデュアルリーダによって、第1のデバイスに伝達されてもよい。

【００１２】

方法は、好ましくはステップf)を含む。

【００１３】

第1のデバイスが、ファイルの、または、レジスタに登録されている数量の一部または全部を表している特定の総計の受信者であるときにステップf)が省略される場合、上記第1のデバイスは、同じデュアルリーダへの次の接続の際に、または、サーバへの接続、そして、同じであるか他のデュアルリーダによって、上記ファイルで、または、上記総計でクレジット処理される。最後に、第1のデバイスがデュアルリーダに挿入される場合、ステップa)、d)およびf)は、手動介入を必要とすることなく、自動的に実行することができる。

【００１４】

ステップg)が、トランザクションの直後に、例えば5分未満で行われてもよく、またはより長い時間の後でもよい。

【００１５】

ステップg)がトランザクションの直後に行われない場合、交換に関する情報はサーバにデュアルリーダを通して伝達されてもよく、それはその後に、第2の電子デバイスと、または、ステップf)が行われた場合は第1または第2の電子デバイスと、または、ファイルもしくは第1のデバイスからデビット処理される数量からの結果の別の総計がその後に転送される電子デバイスと、通信に入る。

【００１６】

「デュアルリーダ」は、本発明を実施することができ、したがって、本発明により2つの電子デバイスと同時におよび／または連続して交換することができるリーダを意味するものと理解される。

【００１７】

安全な交換が金融トランザクションであっても単純なファイルの送信であっても、デュアルリーダによって、そして、本発明によれば、トランザクション時にリモートサーバに接続することが必要ではなく、それにより、トランザクションをより容易にして、同時に安全なトランザクションを可能にする。

【００１８】

トランザクション

「トランザクション」は、電子ファイルの送信、または、上記ファイルにリンクしているかまたは独立したレジスタに登録された数量の結果の1つまたは複数の総計の送信を意味するものと理解すべきである。

【００１９】

トランザクションは、ファイルの削除もしくは転送された総計のソースである電子デバ

イスから転送される数量の精算を伴う、1つの電子デバイスから他方への転送、または単に、デュアルリーダによるか、サーバによるかまたは、リーダに接続された別の電子デバイスによる参照のための、ファイルの、もしくはファイルにリンクされているか独立した数量の通信から成るものであり得、この場合、ファイルまたは数量はそれから最初の時点に存在している電子デバイス上に残ったままであり、第2の電子デバイスへのその通信はおそらく第2の電子デバイスが対応する情報を得ることを可能にするのが唯一の目的である。

【００２０】

ファイルまたは数量は、ポイント数、または識別情報もしくは割引カードまたは交通パスなどの検証が生じた場合に特定の状況で示される文書を表すことができる。この場合、ファイルは、別の検証のためにトランザクション終了後に、電子デバイスに保持されても保持されなくてもよい。それは、割引クーポンなどの有効期限を有しているかまたは有していない文書、スキーリフトか他の器材または施設へのアクセスパス、音声またはビデオ記録、例えば借りられるか、貸し出されるかまたは、購入される、本または他の物でもよい。

【００２１】

それは秘密情報の項目、例えばウェブサイトに関連するログインおよびパスワードか、単一ファイルの解読のために必要なPINまたは鍵を必要とするかまたは必要としなくてもよいユーザライセンスか、または指紋スキャンなどの生体認証ファイルでもよくて、物理的計測の読み取りが、リーダに関連しており人体の内部または外側に配置される医用センサによってなされ、物理的計測の読み取りが、電気、水またはガスなどの何らかの必需使用のリーダに関連するセンサによりなされ、物理的計測の読み取りが、そのサイズ、位置、速度などの車両の状態のリーダに関連するセンサによりなされ、安全に別の車両、例えば解読されるかまたは転送されるために生体認証またはパスワードなどのコードの入力を必要としている電子鍵またはメモに伝達される。リーダは、いくつかの暗号鍵を含んでいるファイルを使用するいくつかの機能性を含むことができて、いくつかの電子署名を検証するかまたは、このような暗号鍵で文書を解読するかもしくは暗号化することができる。PCのスクリーンに接続しているこのようなリーダは、電子デバイス上に文書として置かれる暗号鍵に基づいて、このようなスクリーンによって表示されるいくつかのファイルの署名を解読するかまたは検証することができ、リーダはキーボードに接続されて、その上でタイプされるいくつかのテキストを、スクリーンに、そしてその後にインターネットを通して送信する前に、暗号化するかまたは署名することができる。それは金銭でもよいが、しかし、本発明は、CO_2排出の権利のベアラに対するストックの、または、例えばゲームの間の試験で与えられるポイントなどの任意のタイプのボーナスまたはペナルティの、または運転免許ポイントなどの公文書の特定の属性の交換もカバーする。

【００２２】

ファイルは、制限されるか、リーダによって表示されないかまたはリーダに接続しているいかなるデバイスにもコピーされないか、あるいはこのような動作が時間または量において限定されるようにマークされ、したがって、例えばユーザ情報の安全な格納を可能とし、システムは法律によって要求されるように情報を格納するが、このような情報が外部に転送されるかまたは大量に外部に転送されるのを許容しない。

【００２３】

ファイルは、おそらく許容コピーの数を設定され、そしてコピーのコピーおよびそのようなコピーの深さが許容されるかとともに「コピー許容」としてマークすることができる。コピーとは、システムの範囲内で行われるファイルのコピーのことを意味する。このようなコピーは、コピーまたは潜在的に一定の深さまでのコピーのコピーとしてマークされ、コピーの深さが一緒に記録されてもよい。これは、例えば、コピーされるIDカードおよび別の安全なデバイスへ転送されるそのコピーなどの公文書を考慮に入れる。

【００２４】

ファイルは、それらがこのようにマークされると編集可能とすることができ、それらに

付加される量はファイルに許容される最大量に等しい。例えば、この機能は、受領物、すなわち、例えば、ファイルがシステムの中で二重作成可能でない、またはシステム外部に表示されないといった、システムのセキュリティ能力の恩恵をその後に受けることができる、ファイルのためのプレーンな記憶容量の自動作成を考慮している。

【００２５】

ファイルは1つのグループに一緒に関連付けることができ、そのため、1つのファイルの転送は、それが関連付けられている他のファイルの転送とともにしか処理され得ない。このような場合、他のデバイスのリーダは、グループのファイルメンバーのデバイスからの転送を、このような転送が、このようなファイルがメンバーである全てのファイルのグループにとって小さすぎるようなファイルに関連する量を転送可能にする場合には、可能にすることができない。例えばこの機能性は、ファイルのグループがユーザによって準備されるのを可能とするため、その後にユーザがすぐにそれらを別のデバイスへと外に転送できる。ファイルの、グループへの連結は「強い」ものとしてマークすることもできて、その結果、特定のデバイスにおけるグループに強く連結されたファイルは、ファイルが除去することができるとマークされ、かつファイルがグループに連結した同じデバイス上で除去が行われる場合にしか、このようなグループから除去することができない。グループに連結している第1のファイルは、そのグループから離れることができないようにすることもできて、その結果、このファイルから始まるグループに連結しているいかなるファイルもこの第1のファイルにリンクされ、特に後でグループに連結することができた他のいかなるファイルにもリンクされないことになる。例えばこの機能性は、例えばユーザが自身のIDのコピーを、他のユーザが自身のIDの同様のコピーを除去する可能性を残すことなく、裏書署名することをユーザが望む文書を含んでいるファイルのグループに追加する、いくつかの文書の署名を可能にする。

【００２６】

さらなる機能性は、このようなファイルのグループを封印するのを可能とすることができ、それらがグループに連結したデバイス上でさえファイルのグループがその要素のいくつかを除去することによって撤去される能力を除去する。この機能性は、例えば、グループに連結している第1のファイルを「封印可能」としてマークすることによって、そして、このファイルが封印可能であるとマークされたデバイスのユーザに、それがその一部となったファイルのグループを封印するのを可能とすることによって、実装することができて、このようなファイルのグループがそのメンバーの一部を失うか、または最終的に任意の新たなメンバーを得ることができるという可能性を許さない。例えばこの機能性は、文書を含んでいるファイルのグループに自分のIDのコピーを与えることに潜在的に不可逆的に同意したであろう個人によって裏書署名される文書の裏書署名の安全な保管を考慮に入れる。いくつかのファイルは、決してグループに封印できないか、またはグループに何かが起きた場合に、例えば、金銭を表すファイルが永久にグループに添付されることがあっても、そのファイルが自由に交換されないようにして、そのグループから離れられるよう、マークされてもよい。封印されたグループに添付されたファイルはまた、封印されたグループに含まれるテンプレートに由来するファイルまたは封印されたグループ内に置かれる文書のコピーのオリジナルが、それが転送されることを意図されたデバイスに存在しない場合、そのようなファイルのグループの転送を防止するために用いることができる。これは、例えば有効な会員カードを有するデバイスへのいくつかの文書の移動または配布を例えば制限するのを許す。

【００２７】

同様に、ファイルは、リーダと一体化されるかまたは周辺機器としてリーダに接続される中継器を起動させる能力、または、ファイルがIDカードのコピーに、もしくは文書テンプレートにグループ化され、そしてIDカードのオリジナルまたは上記テンプレートからの有効な文書が、上記リーダに接近している第2の電子デバイスに存在する場合、デバイスのピン上に電圧を印加する能力を有することができる。この機能性は、例えば機器またはドアロックを制御するために用いることができる。その場合、リーダは、それが制御する

ことになっている機器またはロックに好ましくは一体化されて、必要に応じて、リーダが配置されるドアの両側に接近している第2の電子デバイスとともに動作するように構成されることさえできる。

【００２８】

各電子デバイスは、デュアルリーダの外部の1つまたは複数のサーバによって管理される口座と関連付けられる。

【００２９】

サーバは口座にリンクされたトランザクションの全てとともに、電子デバイスのレジスタにおいて登録されたファイルおよび数量も記録する。これらのトランザクションは、トランザクション時にまたはその後にサーバに報告される。ファイルまたは数量に影響を及ぼす動作は、「最初の」ファイルまたは数量を含んだ電子デバイスへ転送されるファイルまたは数量をリンクするトランザクションの全てをサーバが知るとすぐに、サーバによって確認され、サーバ上にそのように登録されるが、これら「最初の」ファイルまたは数量それ自体は、他のトランザクションに続いてサーバによって前もって登録されて確認されているか、またはそうする許可を与えられた外部アプリケーションによって修正されているものであり、これによって確実にすることが可能になるのは、第1に、各トランザクションはただ1回だけ口座のデビット処理またはクレジット処理を行うということであり、そして、第2に、ある数量による口座のあらゆるクレジット処理は、トランザクションが転送に対応するものであり参照に対応するものではない場合、そのような数量による別の口座のデビット処理によって補償される、ということである。例えば、電子デバイスAがファイルまたは数量を、それを電子デバイスCに送信する電子デバイスBに送信する場合、電子デバイスCに登録されているファイルまたは数量の値の存在は、上記サーバが、AからBへ、そして、BからCへ(チェイニング)という2つのトランザクションについて知らされる前にはサーバによって確認されない。この情報プロセスは、最後のトランザクションを有する電子デバイスが同期されると、実施することができ、中間トランザクションがその最後のトランザクションの間にそれに登録される。ファイルおよび数量は、システムの外部のコンピュータシステムの介入を通して更新されることもできて、この動作を実行する許可を与えられることもできる。例えば、割引カードを発行する会社のコンピュータシステムは、サーバに接続して、電子デバイスの口座上にその割引カードの1つに対応するファイルを置くことができる。サーバは、サーバにそれ自体接続しているデュアルリーダを通してサーバが電子デバイスに接続するときに、該当の電子デバイスにこのファイルを伝達する。

【００３０】

トランザクションは特定の制約に従ってもよく、例えば、転送されるものの性質に依存し、したがって、数量は、該当する場合には定義済みインクリメントによって変化する可能性を有する定義済み値域の範囲内で変化するように拘束され得る。通常、通貨口座には、最低0で設定された最大の、単位の1/100の倍数であるインクリメントによって変化する残高がある。したがって、デュアルリーダは他の電子デバイスのレジスタから、またはレジスタに、第1の電子デバイスのレジスタにおいて登録された数量の転送を実行することができ、各転送の終了において、受領される数量だけインクリメントされるか、または、送られた数量がその値から差し引かれている、上記レジスタの各初期値が、転送時にデュアルリーダに存在する特定のルールに従っていることを確実にし、これらのルールは、特に、ゼロ以上で最大値以下の残存のものであってもよい。システムは、数量を、それ以外ではいかなる数量とも関係し得ないいかなるファイルとも関連付けて、1のインクリメント、最小でゼロ、最大で1をそれに割り当てるように設計されていてもよく、したがって、システムによってファイルを送信することができると同時に、数量の転送のために設計された確認手順を用いて、上記ファイルが、いつでもシステムの電子デバイスのただ1つに存在するだけであることを確実にすることができる。

【００３１】

トランザクションの対象を形成しているファイルの、または、数量の電子デバイスにお

ける真正性は、上記ファイルまたは数量が別の電子デバイスへ転送されるとすぐに、または、トランザクションが一部分である場合はそれが第2の電子デバイスのレジスタに登録される数量に追加される前かそれと同時に、第1の電子デバイスからの数量から第2の電子デバイスへ転送される総計が第1のデバイスの数量から減算されるとすぐに、このファイルまたはこの数量が電子デバイス上で利用できないようにされ得るという事実によって、好ましくは確実にされ、加えて、この転送された総計が最初に第1の電子デバイスのレジスタにおいて登録された数量より大きくないように、検証をインストールすることができる。

【００３２】

例えば、転送の対象が値を有する仮想手形から形成されることを確実にすることができ、それについて、システムを通る数量の合計は銀行口座の残高に対応する。ファイルは仮想通貨を表すことができて、数量は手形の値を表すことができる。トランザクションは、これらの仮想手形について実行することができる。これらの仮想手形を出している銀行口座の保有者は、その人の外部アプリケーションを通して、システムが電子デバイスの保有者によって同じ総計だが実際は上記銀行口座の実際の通貨のクレジットに対して特定の総計によって電子デバイスのファイルと関連付けられた数量を増加させるのを認可することができ、そして、対照的に、第三者によって保持される電子デバイス上に登録された上記仮想手形と関連付けられた数量をデビット処理することに対して、第三者の銀行口座をクレジット処理する。第1の電子デバイスから第2の電子デバイスへ金銭の総計を転送するために、ユーザは、第2のデバイスに対するこの仮想手形(それがすでにそこにない場合)と関連したコンピュータファイルとともに、ユーザの電子デバイスに存在するこの仮想手形と関連した数量の全部または一部を転送することができる。好ましくは、仮想手形の発行者は、デビット処理される数量がサーバによって確認されている場合だけ、第三者の銀行口座をクレジット処理する。

【００３３】

同じ1つの電子デバイスは、異なるファイルおよび数量に対して同時にかつ条件付きで関連するトランザクションを実行するように構成することができる。例えば、電子デバイスのファイルおよび数量はデバイスに利用可能な多くの交通チケットを格納するが、別のファイルおよび別の数量はデバイスに利用可能な総計を格納する。

【００３４】

ファイルおよび数量(電子ファイルおよび／またはレジスタに登録された関連する数量)は、例えば、交通パス販売者または銀行などの、ファイルまたは登録された数量を発行している会社に所属する外部サードパーティアプリケーションから生じて、それにより、サーバを通して更新されてもよい。

【００３５】

発行者は、それが発行するファイルまたは数量に、他の銀行発行の仮想手形との特定の代替可能性を許容する情報を割り当てることができ、それから、デュアルリーダは、同じ通貨と関連した数量の合計額を表示してこの通貨に関する全体の転送命令を受信する許可を与えられ、そのためユーザは仮想手形にリンクされる発行銀行に言及する必要はなく、デュアルリーダが、デビット処理される電子デバイスに存在する種々の仮想手形に対応する転送に全体の転送のそれぞれを分解することに対する責任をとる。

【００３６】

デュアルリーダを経た2つの電子デバイス間のトランザクションは、リモートサーバへの接続なしで行うことができる。しかしながら、実行される動作のサーバとの即時の同期および／またはトランザクションの間、デュアルリーダをサーバに接続するための検証を確実にすることが特にできる。この場合、デュアルリーダは、3G、4G、5Gなどのセルラデータネットワーク、メッシュネットワークもしくはインターネットに接続しているローカルエリアネットワーク(LAN)、または、インターネットに接続している外部装置、例えばマイクロコンピュータ、電話もしくは専用端末装置に接続することができる。外部サードパーティアプリケーションとのトランザクションを実行するために、したがって、ユーザ

は、デュアルリーダに接続している外部装置を使用することができて、それによってユーザは、自分が対話したいデュアルリーダにリンクした2つの電子デバイスの1つを選択することができ、さらに自分が送るかまたは受領することを望むファイルおよび／または可能な数量を選択することができる。

【００３７】

各トランザクションの前に、記録された数量にクレジットトランザクションを加えて、そして、以前のデビットトランザクションを引いたものに等しい、「利用できる」数量を算出することができて、この利用できる残高を越えてこの口座のデビット処理をすることを目的とするいかなるトランザクションも拒否され得る。「確定して利用できる」数量を算出することもでき、それはこの同一数量から以前のデビットトランザクションを引いた数量に対応する。この算出数量は、サーバによってまだ確認されていないクレジットトランザクションを考慮しない限り、確定している、と呼ぶことができる。

【００３８】

デュアルリーダは、デビット処理されるかまたはクレジット処理される各電子デバイス上にトランザクションを記録することによって、そして、該当する場合、クレジット処理されるデバイスへの転送の対象であるファイルを、それがすでにそこになければ、コピーすることによって、トランザクションを生成することができる。

【００３９】

デュアルリーダは、数量の転送を実行するために、この転送を、

● 電子デバイスに存在する数量、

● または電子デバイスへ書き込まれて以前のトランザクションから生じるクレジット、

に関連するサブ転送に分割することができ、

一方で同時に、各デビット処理された部分要素については、デビット処理された総計が確定して利用できる数量を超えない数量または以前のトランザクションを検証し、または、以前のトランザクションについては、最初のクレジットトランザクションの総計から、過去にそれと関連したことのあり得るデビットトランザクションの総計を引いたものを検証する。

【００４０】

トランザクションを制限することを目的とする機能性を提供することができ、例えば、数量に、または、転送される数量に最大限度を課す。

【００４１】

電子デバイスに登録されるトランザクション、ファイルおよび数量は、インターネットを介してそのそれぞれの十分に長い接続に際して、サーバに伝達することができる。

【００４２】

デュアルリーダはサーバに知らせるための中継器としての役割を果たすことができ、サーバは電子デバイスから生じるトランザクションを列挙し、電子デバイスは、サーバと通信しているが必ずしも上記トランザクションを生成していない。

【００４３】

サーバに対する電子デバイスの接続の間か後に、サーバは、1回限りの方法で、トランザクションを確認することができて、デバイス用の新規のファイルおよび数量を算出することができ、以下を伴う。

- この接続の間か、または、デバイスの次の接続の際に削除されてもよいトランザクションのリスト。

- 残高が更新されるときにそれに追加されなければならないか、または削除されなければならないトランザクションのリスト。

- 他の電子デバイスおよびリーダによってサーバに報告されるトランザクションであるが、特に、トランザクションが電子デバイスにおけるデビットを作成したにもかかわらず対応するクレジットトランザクションがクレジット処理されるデバイスに伝達されていない場合、例えば、操作の間の最後の時間にそのユーザがリーダの隣に自分のカードを配

置することを怠った場合か、またはカードに示される未知の相手とのデビットトランザクションが同じトランザクションと置き換えられることはできないが相手の識別子を含んでいる場合に、該当の電子デバイスにまだ存在しないものである、トランザクションのリスト。

【００４４】

デバイスの新規の接続の際に、または、これが十分に長く持続する場合、同じ接続の間に、前述のこれらのリストのそれぞれにリンクされた動作、およびまた、ファイルおよび数量のあり得る更新処理が実行されてもよい。

【００４５】

必要に応じて、特定のトランザクションに対する、そして、ある数量およびファイルに対する更新が、同時であるように、システムは構成することができる。例えば、更新が、数量への1の追加を表すトランザクションの組み入れを含む場合、このトランザクションは数量を含んでいるレジスタが1だけインクリメントされるのと同時にデバイスから削除される。

【００４６】

電子デバイス

本発明による電子デバイスは、好ましくは既存の支払端末と互換性がある。

【００４７】

好ましくは、電子デバイスは、標準ISO7810によって定義されるような、クレジットカードの標準化されたフォーマットである。変形として、それは、携帯電話または携帯電話に挿入することが可能なSIMカードでもよい。

【００４８】

それがカードの形であるときには、デバイスはデュアルリーダに挿入されて、それと通信することができるコネクタを備えたチップを都合よく有する。

【００４９】

電子デバイスは、非接触のリンクを介してデュアルリーダと通信するシステム、例えばRFIDシステムを備えることもできる。

【００５０】

電子デバイスは、保護された対称形のまたは秘密鍵およびメモリ、例えばデバイスの鍵を用いて暗号化されるフラッシュメモリおよびおそらくプロセッサを含むことができる。鍵を含んでいるメモリは、メモリが含む情報がそこから抽出される前にそれに物理的にアクセスすることがその破壊に導くように、好ましくは物理的に保護されている。デバイスの保有者は、もはやそれを使用することができないで、中央サーバのオペレータに連絡しなければならず、オペレータは、その電子デバイスを識別することが可能で、システムを使用するのに適している適切な手順がある場合、おそらく、サーバから、電子デバイスに存在するファイルおよび数量を回復することができて、新規の電子デバイス上にそれらを置くことができる。

【００５１】

電子デバイスは電源、例えばバッテリ、電磁誘導システムまたは、コンデンサ、スーパーキャパシタまたは蓄電池を含むことができ、それはリーダまたはその他への接続の際に再充電される。デバイスは、例えば温度、圧力、位置などのいくつかのセンサを含むこともできて、これらのセンサを使用するいくつかの文書を作成するかまたは更新する能力を有することができる。

【００５２】

電子デバイスは、例えばBLE(Bluetooth(登録商標) Low Energy)、Sigfox、Lora、4GのLTEなどのような低エネルギー消費ワイヤレスネットワークを用いることにより、リモートサーバとの直接の一方向または両方向通信を可能にするインタフェースをおそらく備えることができる。サーバとのこの通信が、利用可能なときには使われることができて、電子デバイスとサーバの間のデータの同期の速度を上げる。

【００５３】

電子デバイスはスクリーンだけでなく、ミニキーボードも備えることができ、スクリーンは、例えば、文書または残高を表示することを可能にし、ミニキーボードは、例えば、任意選択的に、表示されるものを選ぶこと、または、例えばトランザクションを承認する能力などの、デュアルリーダのキーボードの特定の機能をデバイスに移すことさえも可能にする。

【００５４】

電子デバイスは、以下の動作の全部または一部を実行するように構成することができる。

- リーダとのいかなる通信の前にも、上記リーダが認可されたリーダの一部をなすことを検証する。
- それが指定受信者である暗号化された情報だけを受け入れる。
- リーダのために、または、サーバのために意図される情報のいかなる送出項目も暗号化して、署名する。

【００５５】

電子デバイスに記録される情報は、以下の情報の全部または一部でもよい。

・ コンピュータファイルのコピー、および数量のコピー。
・ サーバによってまだ認証されてない最新のトランザクションのログ。
・ デバイスによって実行される他の電子デバイスとのトランザクションであって、リモートサーバにまだ記録されておらず、これらのトランザクションがさらにサーバに伝達されていなかった場合であっても、サーバがデバイスにおける各トランザクションを別の電子デバイスの数量またはファイルにチェイニングすることができる、トランザクションのリスト。
・ 電子デバイスがデュアルリーダに挿入されるかまたは別の方法でそれと通信するトランザクションをおそらく許可するためのPINコード。
・ 電子デバイスの識別子番号。
・ 上記デバイスの外部では利用できない電子デバイスの秘密鍵。
・ デュアルリーダの、そして、サーバの公開鍵および、それが通信することができるいずれのサーバまたはデュアルリーダにも関連しており、このようなサーバまたはデュアルリーダによりそれ自体を識別するために用いられる潜在的に固有の秘密鍵のリスト。

【００５６】

電子デバイスの中で、各ファイルおよび数量またはファイルのタイプおよび数量のタイプごとに、最小、最大および認可されたインクリメント、さらにはその転送を拘束することに対する可能性があるルールを記録することが可能である。

【００５７】

デュアルリーダ

「リーダ」と呼ぶこともできるデュアルリーダは、トランザクションを実行するために本発明によって電子デバイスへの安全な接続を確立するように構成される。したがって、それは、これらの電子デバイスで通信するための手段を備えている。

【００５８】

この接続は、各電子デバイスとデュアルリーダの間の物理的接触を含むことができる。変形として、この接続は、特にNFCタイプの無線リンクを介して、無接触でなされ得る。デュアルリーダは、コンピュータ接続によってリンクされる2つのデュアルリーダを通して異なる位置の電子デバイスとの安全な交換を許容することが可能であるように構成することができる。それから、電子デバイスの1つが所有者を有し、その所有者の識別情報が、第2の電子デバイスがトランザクションを行う前に第2の電子デバイスの保有者に示されるケースに、このタイプの使用を制限することもできる。

【００５９】

デュアルリーダは、この目的のために設計されるコンピュータ、電話または電子システムによって制御されるオプションを有することができる。コンピュータまたは電話が、例えば、キャッシュレジスタ、ATM、または、列車チケット販売者の機能を実行する場合、

これは特に役立ち得る。デュアルリーダは、その読み取り値が文書の作成または更新で使用されるいくつかのセンサを含むことができる。デュアルリーダは例えば、その読み取り値が文書を作成するときに使用され得るセンサ、またはその読み取り値がリーダ用の生体認証を行うために使用され得る生体認証デバイスでもよいいくつかの周辺機器にも接続することができる。デュアルリーダは、自動的に文書を生成し、それが接続している電子デバイスの1つに、それらを配置するいくつかの能力を含むことができ、このような自動的に生成された文書は、例えば物理的測定値、例えば液体の中の分子の位置または温度または濃度などの測定値であり得る。デュアルリーダは電子デバイスの1つを組み込むこともでき、組み込まれた電子デバイスの機能性は「デュアルリーダ」機能性がオフにされるときに、動作中のままとすることが可能である。デュアルリーダは電子デバイスの1つまたは複数を統合してもよく、機能性「デュアルリーダ」がオフであるときに、統合された電子デバイスの機能性は潜在的に、有効なままとすることが可能である。デュアルリーダは、他のオブジェクトが電子デバイスとのトランザクションの間、ネットワークに必然的に接続していることを必ずしも必要とすることなく別のオブジェクト、例えば電話、コンピュータ、財布またはその他に、統合されることもできる。

【００６０】

本発明の1つの例示的な実装において、電子デバイスの1つは、デュアルリーダに対応するカードリーダに挿入されるカードであり、他の電子デバイスへの、またカードへのものであってもよい接続は非接触でなされ得るが、第1のカードはリーダで保持される。したがって、この例では、第1の接続は接触を基にしたものであり、第2の接続は非接触である。

【００６１】

デュアルリーダは、2つの電子デバイスがそこに接続されているときに、接触を通して、または、非接触で、2つの電子デバイスとの情報の同時交換を可能にするように構成することができる。

【００６２】

変形として、情報の交換は非同期であり、デュアルリーダは一度に情報をただ単一の電子デバイスと交換するように構成され、この場合、トランザクションを実行するために次に続く接続は電子デバイスになされる。

【００６３】

デュアルリーダは、トランザクションが2つの電子デバイスの間で実行される間、またはこのようなトランザクション外で、外部サーバに接続するように構成することができる。

【００６４】

デュアルリーダは支払端末の形、例えば今日では店で銀行カードを用いて支払をするために用いる支払端末という形をとることができるかまたは他に、バンキングインタフェースへの接続を認可するために用いるが交換に関する情報の入力を可能としている、個人カードリーダと類似のキーパッドを有するリーダという形をとることができる。デュアルリーダは、接触型のカードリーダおよび非接触型の、特にNFCタイプのカードリーダの両方を備えることができる。

【００６５】

デュアルリーダは、以降さらに説明するように、電子デバイスの複数対間の転送が直接「多重デュアルリーダ」に、または、リモートデュアルリーダへの接続を通して接続されるのを可能にしている「多重デュアルリーダ」を形成している1つのデバイスにグループ化することができる。例えば、多重デュアルリーダは、それ自身多重デュアルリーダにインターネットまたはコンピュータネットワーク経由で接続される他のリモートデュアルリーダに、他のデバイスに対するトランザクションが接続されるのを可能にする、多くの内部デバイスのためのスロットを有することができる。これは、例えば単一の「多重デュアルリーダ」を用いてそれらの支払を管理することができるオンラインショッピングウェブサイトに役立つものであり得る。

【００６６】
複数の電子デバイスは、1つの単一デバイスにグループ化することもできる。このようなグループ化によって、多重デュアルリーダが多重デュアルリーダのオペレータを必要とせずにこのような複数の電子デバイスを用いてトランザクションを処理して複数の電子デバイスを管理することができる。
【００６７】
デュアルリーダは、それがコンピュータネットワーク、例えばインターネットに、3G、4G、5GもしくはWi-Fiネットワーク、メッシュネットワークまたは該当する場合コンピュータまたは電話を介してインターネットに接続しているLANを介して接続していることを可能にするインタフェースを備えていることができる。デュアルリーダのヒューマンマシンインタフェースは、キーパッドで好ましくはボタンを有するもの、および少なくとも1つのスクリーンを含むことができて、それから、システムは、第1および第2のデバイスのペアラをそれぞれ対象とする2つのメッセージを表示することを可能にする。
【００６８】
変形として、デュアルリーダのヒューマンマシンインタフェースは、音声インタフェースを含む。デュアルリーダのインタフェースは電子デバイスの保有者を識別するための手段、例えばPINコードを入力するオプションまたは生体測定システムを含むこともでき、それは、上記保有者を識別して上記電子デバイスによって運ばれる文書を考慮した後に、電子デバイスの、そしてその保有者の、証明書を確認することができる。
【００６９】
デュアルリーダのヒューマンマシンインタフェースは、以下のことを可能にすることができる。
- リーダに挿入されるか、または、別の方法でそれに接続される、電子デバイスへの接続を確認する。
- おそらく、転送されるファイルまたは数量を選択する。
- おそらく、トランザクション、例えば転送される総計に関する数量を入力して、これが対応する電子デバイス用の送信または受信を含むかどうかを示す。
- 、2つの電子デバイスのそれぞれのユーザに対しておそらく連続のメッセージを表示する。
- ユーザが、それらの電子デバイスの、ファイルと関連するかまたは関連していない残高および／または、1つまたは複数の数量を表示することができるようにする。
- PINコードが変更できるようにする。
- おそらく、このファイルに対して許可される場合、ファイルの内容が変更できるようにする。
- おそらく、ファイルの、そして、関連する数量の作成を可能にする。
【００７０】
ヒューマンマシンインタフェースは、トランザクションの確認の前に転送と関連した1つまたは複数の数量を表示することを可能にすることができ、トランザクションに関するファイルはまた、特にそれがオーディオまたはビデオファイルである場合、表示するかまたは読み取ることができ、ユーザに対する命令も、表示するかまたは読み取ることができる。
【００７１】
該当する場合、ヒューマンマシンインタフェースは、デュアルリーダが有線であるか無線リンク、例えばコンピュータ、キャッシュレジスタ、電子ロックまたは携帯電話を介して通信する別の装置に移される。
【００７２】
デュアルリーダは好ましくは、上記のトランザクションを実行するために必要で、したがって、それを識別するコンピュータの鍵、つまり利用できる数量、特に確定して利用できる数量を算出する能力を有するメッセージに署名するために必要で、例えば電子デバイスに登録されるトランザクションまたは命令を表すメッセージを作成するために必要な手

段、ならびに、サーバに、レジスタに登録された数量、トランザクションおよび、認可されたリーダのリストを電子デバイスとの間で自由に書き込み、読み出しおよび削除を可能とする手段を備えている。

【００７３】

デュアルリーダは、好ましくは以下の要素の全部または一部を備えている。

マイクロコンピュータまたは他の端末に対する有線リンク用の例えばUSBタイプの接続、

マイクロコンピュータまたは電話に対する例えばBluetooth(登録商標)タイプの無線接続、

本発明による電子デバイスへのリンクを確立するための、例えばBluetooth(登録商標)またはRFIDタイプの無線接続、

電子デバイスがリーダに挿入される場合、本発明による電子デバイスと通信するための接触型のコネクタ、

サーバへの接続ごとに同期され、そしてトランザクションおよび残高がタイムスタンプされ、このクロックが好ましくは、1ヵ月につき+/-5秒の範囲内の精密さである内部クロック、

デュアルリーダの秘密鍵を含む物理的に保護されたメモリであって、その物理アクセスが、好ましくは、メモリが含む情報がそこからコピーできる前にその破壊に導く、メモリ、

少なくとも1つのメモリであって、その内容がそれ自身の秘密鍵によって暗号化されて、以下の情報の全部または一部が格納され得る少なくとも1つのメモリ:

デュアルリーダを識別するコード、

デュアルリーダを介して実行される最新のトランザクションの、そして、対応するファイルのリスト、

他のリーダによって実行される、サーバが電子デバイスへ伝達することを望む、または、電子デバイスがサーバへ伝達することを望む不正なトランザクションまたは残高または他のあらゆるデータの項目のトランザクションのバッファリスト、

サーバまたは電子デバイスに関連付けられ、そしてこのようなサーバまたは電子デバイスと通信して、それ自体を識別するために用いられる、サーバおよび電子デバイスの共通または公開鍵の、また、おそらく秘密鍵の、リスト。

【００７４】

デュアルリーダは、以下の動作の全部または一部を実行するように構成することができる。

PINコードおよび接続される電子デバイスの識別子を読み込む、

利用できる数量を算出する、

トランザクションを削除するか、書き込むかまたは、保持する、

それに接続されている電子デバイスにメッセージの署名を行わせる、

電子デバイス上で、採用されるセキュリティシステムに応じて、認可されたリーダおよびサーバのリストを更新する。

【００７５】

本発明の別の主題は、そのようなものとして考慮されるデュアルリーダである。

【００７６】

サーバ

これらは、各電子デバイスと関連した口座、および、関連する電子デバイスによって実行されるトランザクションを基礎とした、または、ファイルを追加することができるかまたは除去することができて、数量を修正することができる認可された外部アプリケーションから生じる命令を基礎としたデュアルリーダを含む、リモートコンピュータシステムである。

【００７７】

サーバは、以下の情報の全部または一部が格納され得る少なくとも1つのメモリを含む

。
1.各電子デバイスに対するもの:
このデバイス上で、数量の、または、トランザクションが関連するファイルの変化をまだ引き起こしていないトランザクションのコピー、および対応する電子デバイスに別のコピーが記録されているそれらの関連ファイルであり、サーバによってその後に確認される各トランザクションは、以下のようにマークされる。
・ 電子デバイスに記録される数量およびファイル。
・ 電子デバイスに存在する鍵のリストを識別するための情報。
2.各デュアルリーダに対するもの:
・ デュアルリーダに存在する鍵のリストを識別するための情報。
3.好ましくは物理的に保護されているサーバの秘密鍵、または、好ましくは物理的に保護されている秘密鍵のリストであり、これらの鍵のそれぞれは、いくつかの個々のデバイスまたは個々のデュアルリーダ、またはこのようなもののグループによってそれらの関連する公開鍵とともに、それ自体を識別するために用いられる。
4.デュアルリーダの公開鍵のリスト。
5.電子デバイスの公開鍵のリスト。
6.他のサーバの公開鍵のリスト。

【００７８】
サーバ同士は、互いに通信して、例えば電子デバイスによって、そしてデュアルリーダによって情報をサーバ間で分配することができ、これにより、特定のデュアルリーダに、または特定のサーバにおける特定の電子デバイスに関連する情報を保持することを可能にすることができ、また、いずれかのデュアルリーダが接続しているサーバが、必要に応じて、この情報を読み取り、変更または修正を行うこともできる。システムは1つだけしかサーバを含まなくてもよく、したがって、システムの複雑さを減らす。

【００７９】
サーバは、数量を、上記数量より大きい総計によってデビット処理することを目的とするいかなるトランザクションも拒否して、このようなトランザクションを不正であるとマークするように構成することができ、情報のこの項目は、次の接続の際に電子デバイスに伝達することができる。不正であるとマークされたトランザクションは、その後もはや考慮されない。不正なトランザクションに依存するトランザクションもまた、キャンセルされるかまたは、不正であるとマークすることができる。

【００８０】
サーバは特に、以下の検証がなされるとすぐに、トランザクションを有効であるとマークすることができる。
● それらが、上記トランザクションの間有効である電子デバイスおよびデュアルリーダと関連しているということ。
● それらが、この検証の前にサーバによってそれ自体確認されたトランザクションから生じる数量をデビット処理するということ、または、それらが、電子デバイスにおけるサーバによって前もって登録される数量またはファイルをデビット処理するということ、または、それらが、デュアルリーダを用いて何もないところから作成されてかつまだ送信されていないファイルをデビット処理するということのいずれか。
● それらが、例えば、このトランザクション時にこのようなトランザクションに課される、例えば以下のようなルールに従っているということ:
○ このルールがこの数量に適用できる場合、レジスタに登録された数量を、上記数量より大きい総計によってデビット処理することを不可能とする。
○ 検証されたトランザクションの前に他のトランザクションの総計によって調整される電子デバイスのレジスタに登録されて、そしてこの総計からデビット処理されることになる数量より大きい総計を、このルールがこの数量に適用できる場合、デビット処理することを不可能とする。
○ 他のリンクされたトランザクションが同時に実行されず、そしてこれらのトランザ

クションの全てが実行されたわけではなく、これらのリンクされたトランザクションの1つは、例えば生体測定検証を要求することが可能な場合、トランザクションを作ることを不可能とする。

【００８１】

トランザクションに関する情報は、クレジット処理される電子デバイスに存在する数量に関する情報を含むことができ、その情報はサーバがトランザクションを確認するために必要となることがあり得る。

【００８２】

サーバは、それらが、デバイスごとに確認されているとマークされておりそして各クレジットをすでに確認された数量のデビットにリンクするトランザクションの、全てについての知識を有している場合だけ、数量を算出して、更新するように構成することができる。このようにして、リーダから、または、サーバに登録されていない電子デバイスから生じているトランザクションは、数量における変化を引き起こすことが可能でない。さらにこれは、他の電子デバイスにおけるデビットにリンクされる同じトランザクションを基礎として数量を電子デバイスにクレジット処理することをサーバができるようにするので、確認されてはいるが、電子デバイス上に登録される数量によってまだ考慮されていないトランザクションの全てによって調整された数量の合計値の、全ての電子デバイスにわたる一貫性を確実にする。サーバは、同時に同じ一つのトランザクションによってデビット処理されてクレジット処理される数量を算出して、更新するように構成することもできる。それから、サーバは、第1に、電子デバイスに登録された数量を、第2に、サーバによって更新されたが、上記電子デバイスにまだ登録されていない数量を、メモリに保持し、その数量にリンクされるのは、更新のために使われて、そして、新しく算出された数量が上記デバイスへコピーされるときに上記電子デバイスから削除されなければならないトランザクションである。

【００８３】

このチェイニングを容易にするために、電子デバイスは、数量の、または、ファイルのデビットの前に実行された他のトランザクションのコピーを含むことができ、これらのトランザクションは、これらのトランザクションが別の方法でサーバに報告されていない限り、このデビットを、サーバによってすでに確認されている初期ファイルまたは数量にリンクすることを可能にする。

【００８４】

外部エンティティとのトランザクションの間、サーバは該当の数量を算出することから始めることができ、デバイスに存在する上記数量に適用されるトランザクションの全てを考慮する。

【００８５】

電子デバイスのレジスタに登録されたファイルまたは数量によって表される文書を修正するために、電子デバイスがサーバによってまだ確認されていないこの文書に関するトランザクションを含む場合、デュアルリーダは、外部エンティティとのトランザクションのために提供されて、したがって、サーバとの同期を要求している以下の手順に従うことができて、それから、電子デバイスにおける上記ファイルの、または、数量の修正を許可して実施することができる。デバイスは、ファイル変更を、数量を登録可能で、この数量が0または1にだけ限定されるただ1つのレジスタを有するファイルに制限することもできる。

【００８６】

サーバは、データネットワークへの接続によってアクセス可能なので、それらは、コンピュータまたは電話を介して、電子デバイスの少なくとも1つの、上記サーバとのデータ同期を可能とすることができる。例示的な同期プロセスは、図4を参照してさらに説明される。

【００８７】

本発明を実施するシステムはサーバ当たりいくつかの電子鍵を含むことができて、これ

は必要である場合、無差別に使われ、そのため各サーバは短時間でデュアルリーダに、そして、電子デバイスに応答することが可能である。

【００８８】

本発明の1つの例示的な実装では、電子デバイスがSIMチップカードおよびRFID接続を含み、システムは、トランザクションが互いとかけ離れている2つのデュアルリーダを含んでいることができるように構成される。それから、システムは、トランザクションの記録で、2つのリーダのそれぞれの識別子に注目することができる。2つのリーダのペアリングのための機構を構成することができる。この機構は、リモート電子デバイスの保有者の識別情報を表示するための手段を含むことができて、関係する電子デバイスの少なくとも1つが識別可能な保有者を備えているトランザクションに、トランザクションを制限することもできる。ペアリング機構は、2つのペアとなったリーダの1つのための、または、それぞれのための、他方のリーダが置かれている位置を示す手段を含むこともできる。

【００８９】

ファイルおよび数量のセキュリティ

「安全な」とは、情報がそこに特有の手順の範囲外のシステムに流れること、またはそのシステムで修正することが可能でなく、システムの手順に従ってユーザから認可なしにそれを置いておくこと、またはそれを入力することができないことを意味するように意図しており、それは各文書のタイプに依存し得る。

【００９０】

本発明による電子デバイスおよびリーダまたはサーバに存在するデータは、好ましくは安全である。メモリに登録されるこれらのデータは、電子デバイスまたはそれらを運ぶデュアルリーダが存在する場合にだけ、例えばこの電子デバイスまたはデュアルリーダにある鍵を使用した暗号化を通して、解釈可能である。

【００９１】

電子デバイスおよびデュアルリーダによって運ばれるソフトウェアを保護する機構は、不正なソフトウェアがそこの中へ導かれることを回避するように、好ましくは存在する。このソフトウェアは署名され、その署名はロードされるときに検証されてもよい。これらの署名は、あらゆるトランザクションの前に検証されることもできる。ソフトウェアは、例えばそれが動くことになっているシステムの要素のIDへの参照をそのコードに追加することによってシステムの各特定要素に対して異なるようにすることもできて、そのため、1つのソフトウェアのハッキングまたは危殆化は、システムの多くまたは全ての要素ではなく、それが動くことになっているものしか危殆化しない。ソフトウェアのハッキングかまたは危殆化によってそれが意味するのは、それが動くことになっているシステムの要素がそのような置き換えに気付くことができずに、このようなソフトウェアを異なるもので置き換える能力のことである。例えば、ファイルを安全にするために用いる技術は「ハッシュ」として公知の方法を使用してきており、このような方法、例えばMD5は、いくつかのポイントで完全に安全ではないと報告されている。

【００９２】

好ましくは、システムの種々の要素の間の通信の全ては、それらがシステムの要素だけに理解可能で、この目的のために認定されて、サーバにリンクされたシステム外の第三者の要素から生じることが可能でないように、または、ユーザの代わりにデュアルリーダを制御するように実行される。

【００９３】

システムの各要素、すなわち各サーバ、デュアルリーダまたは電子デバイスは、それだけが知っていて、しかし、その公開鍵はその識別子と関係している秘密鍵を有することができる。システムの各要素はシステムの他のそれぞれの要素専用の秘密鍵を有することもでき、いずれのこのような秘密鍵のハッキングも、それが関連していたデバイスとの通信のセキュリティしか危殆化せず、同じカテゴリの全てのデバイスとの通信のセキュリティを危殆化はしない。

【００９４】

都合のよいことに、サーバの、各デュアルリーダの、または、各電子デバイスのこれらの秘密鍵のどれも、決してそのキャリアを残さず、そして、適切なエレクトロニクス技術によって都合よく物理的に保護される。

【００９５】

サーバの鍵および各デュアルリーダの鍵が更新されることを可能にする機構を提供することができる。

【００９６】

不正の検出

デュアルリーダがクロックを含むので、第1および第2のデバイスにおいて登録される情報は交換の時間でタイムスタンプすることができる。

【００９７】

サーバは、トランザクションのいずれかのトランザクションへのチェイニングが、トランザクションと関連した、サーバでパラメータ化されたいずれかのルールに従っていないことを生じさせる場合、電子デバイスに記録されたトランザクションをキャンセルすることができる。

【００９８】

好ましくは、トランザクションは、それらがサーバに報告された後にだけ、デュアルリーダから削除される。デュアルリーダは、それらの全部のメモリが用いられている場合、それらは新規のトランザクションのために作動することができないことを示す、光か他のインジケータを都合よく備えている。

【００９９】

いかなる異常、例えばチェイニング、署名または日付異常も、好ましくは不正としてマークされる。

【０１００】

例えば不正な署名があり不正と検出されたあらゆる残高、あらゆるトランザクション、あらゆるリストは、サーバに報告されて、無効としてマークされる。

【０１０１】

不正の処理

サーバは、不正を検出して、いかなるトランザクション、リスト、残高または電子デバイスも不正であるとマークするように構成することができる。

【０１０２】

それらの無効化およびあり得る修正は、電子デバイスに送信される。

【０１０３】

電子デバイスまたはリーダは、不正であるとマークされ、動作不能にされ、認可された電子デバイスまたはデュアルリーダのリストから削除され、そのようにマークされ得る。不正な電子デバイスのリストはデュアルリーダに伝達されることが可能であり、その結果上記リーダはそれに接続することができる不正な電子デバイスを停止させる。

【０１０４】

周知の不正なリーダを用いてなされて、まだ確認されていないトランザクションは、そのトランザクションのなされた瞬間からサーバにセットされた合理的な時間が経過するまで、サーバによって確認することができず、このようなトランザクションは、デバイスに疑わしいとしてマークされることもできて、上記合理的な時間が経過するまで、または、これらのトランザクションがサーバによって有効に確認されるまで、他のトランザクション自体に従属するのを防止することもできる。

【０１０５】

データの完全性

数量およびトランザクションまたは他の動作を登録する特定の動作は、互いに関して整合的でなければならない。数量またはファイルを修正することによってトランザクションを変換することは、2つの要素、すなわちトランザクションおよび数量またはファイルが、一緒に更新されるかまたは削除されなければ、成し遂げることは可能でない。これらの

情報ブロックが完全に正しく登録された場合にだけ電子デバイスの更新ブロックが確認されることを確実にするプロセスを、用いることができる。例えば、これらの書込みブロックの情報に参照を割り当てることができ、ブロックの要素の全てが正しく書き込まれた場合にだけ、この参照が有効であるとしてマークされる。余分な情報を削除するために、参照された削除命令、つまり後で実際にこの余分な情報を削除する手順を、同様に登録することが可能である。

【０１０６】

通信のセキュリティ

種々の技術は、種々のサーバ、電子デバイスとデュアルリーダ間の通信のセキュリティを確実にすることができる。以下の説明は、このようなセキュリティを考慮に入れている技術について、網羅的であることを意図するのではなく単に例示するためのものである。

【０１０７】

リストによるセキュリティ

システムの各要素、すなわち各サーバ、各デュアルリーダおよび各電子デバイスは、どこにも複製されておらず、しかし、その対応する公開鍵がシステムにとって公知で、リストにコンパイルされている、1つまたは複数の秘密鍵を有することができる。サーバ、デュアルリーダまたは電子デバイスが複数の秘密鍵を有している場合、これらの秘密鍵の一部もしくは全部は、特定のまたはグループの他のサーバ、リーダまたはデバイスに関連することができて、それらの対応する公開鍵はそれらが関連する特定のまたはグループのこのような他のサーバ、リーダまたはデバイスによって公知となる。この鍵は、いかなるイベントにおいてもシステム(サーバ、電子デバイスおよびデュアルリーダ)のいかなる要素とも関連している秘密鍵と同じであるか、異なってもよく、そのソフトウェアを更新して、それ自体を更新して、そのメモリの中のデータを暗号化するために用いる。

【０１０８】

これらのリストは、したがって、各要素と関連した公開鍵のリストである。したがって、サーバの公開鍵のリスト、リーダの公開鍵のリストおよび電子デバイスの公開鍵のリストがあり、このようなリストは、複数の秘密鍵の場合、それらが関連する他の特定のまたはグループのサーバ、リーダまたはデバイスの情報を有する。

【０１０９】

サーバは、デュアルリーダが行うように、これらのリストのそれぞれを保持し、電子デバイスは全て、サーバの公開鍵の、そしてデュアルリーダの公開鍵の、リストを有する。

【０１１０】

システムの要素が十分に長い時間の間(デュアルリーダからサーバに、電子デバイスからリーダに、または電子デバイスからサーバに)接続されるときに、リストは更新される。

【０１１１】

データのいかなる送信もこれらのリストの1つに列挙される要素だけに実行されて、指定受信者要素だけがそれを読み込むことが可能であるように暗号化され、指定受信者がメッセージの送信者の真正性を検証することが可能であるように署名される。

【０１１２】

システムは、サーバの要求により、秘密鍵およびそれらの関連する公開鍵が更新されるようにすることができる。

【０１１３】

このシステムによって、各電子デバイスが同じシステムのただ1つのリーダまたは1つのサーバと通信することを確実にすることができる。同様に、各リーダがシステムのただ1つのサーバまたは1つの電子デバイスと通信して、暗号化された方法でそうすることを確実にすることができる。

【０１１４】

リストによるセキュリティには各電子デバイスおよびリーダにおけるリストの著しい保存および更新処理を必要とする欠点があるが、第1に、秘密鍵の窃盗に対して防御するこ

とを可能にする利点があり、これらの鍵は物理的に各ハードウェアキャリアに位置していてそれから離れないように設計されており、それにより、必要とする安全化の技術の数がより少なく、そして、第2に、その多重度を確実にする利点があり、リーダまたは電子デバイスに影響を与える鍵の窃盗はこのリーダまたは電子デバイスだけしか危殆化しない。複数の秘密鍵の使用はこのような鍵のハッキングの影響を緩和することができ、鍵を危殆化することが影響を及ぼすサーバ、リーダおよびデバイスの数はより少なく、例えば危殆化したサーバ鍵である、複数の秘密鍵システムの一部は、このような危殆化された秘密鍵が関連しているシステムの他の要素を安全でなくすだけである。秘密鍵は、随時、または、それらのハッキングの疑いがある際に更新することもできて、そのため、最新の対応する公開鍵を認識しているシステムの要素は、システムの一部であるように見せかけるが実際は、それが新規の秘密鍵を処理せず以前の鍵の1つだけしか処理しない要素と通信することができない。

【０１１５】

共有鍵によるセキュリティ

電子デバイスの鍵のリストまたはデュアルリーダの鍵のリストまたはサーバの鍵のリストは、デュアルリーダの、電子デバイスの、または、サーバの共有鍵の小さいリストと、それぞれ置き換えることができる。これらの鍵は、それらが秘密で、システムを離れてはならない場合であっても、それらがシステムのいくつかの要素で見つかる限り、共有されていると言われる。この交換は一部分であってもよく、例えば、電子デバイスのリストまたはリーダのリスト、あるいは、電子デバイスのリストおよびリーダのリスト、あるいは、いくつかのリーダおよび電子デバイスおよびサーバのリストに影響を与えるだけである。これらの場合、電子デバイスのリストが、例えば、もはや存在しなくて、電子デバイスの共有鍵と置き換えられ、それから、システムの要素は通信するためにこの共有鍵を使用しなければならず、それにより、システム外の要素と通信することを回避する。これらの鍵は、非対称でもよく、秘密鍵／公開鍵システムであって、リストに登録された各要素で見つかるリストの要素の秘密鍵、およびシステムの各要素における公開鍵が上記リストの要素との通信に入ることが可能であり、または、対称形であって、上記リストに登録される要素上、そしてシステムの要素における両方に見つかるこの同じ鍵が、上記リストに登録される要素と通信することが可能である。これらの鍵は、2つの最近更新された要素が、盗まれたものであり得る鍵と通信することを回避するように、定期的に更新することができる。この更新はサーバによって実行され、それは、各電子デバイスの、および、各デュアルリーダの公開鍵の知識によって、秘密に新規の共有鍵をそれに送信する。リストによるかまたは共有鍵によるセキュリティを用いてであれば、システムの2つの要素は、それらが方の要素に配置されている秘密鍵に対応する公開鍵を各々有し、この秘密鍵がユニークでその要素だけに配置されている場合、またはシステムの種々の要素によって共有されていて、それからシステムのいくつかの要素に配置される場合、したがって、互いに通信することが認可され得る。システムの要素は、それらの間で、または、それらとシステムの他の要素との間で共有される同じ一つの秘密鍵を各々知っている場合にも、互いに通信することができる。

【０１１６】

1つの例示的な実装において、電子デバイスおよびリーダは電子デバイスおよびそれらのIDの公開鍵の、および、デュアルリーダのリストをもはや含まず、1つの鍵だけがデュアルリーダによって共有され、別の鍵が電子デバイスによって共有される。各電子デバイスおよび各デュアルリーダも秘密鍵を有するが、サーバだけがそれらの関連する公開鍵のリストを有する。それから、サーバは、上記共有鍵を変更および更新することができる。

【０１１７】

別の例示的な実装において、デュアルリーダの共有鍵の存在は、各電子デバイスにおけるリーダの公開鍵およびそれらのIDのリストに対する要件を回避することを可能にする。

【０１１８】

別の例示的な実装において、電子デバイスの共有鍵の存在は、各デュアルリーダにおけ

る電子デバイスの公開鍵のリストに対する要件を回避することを可能にする。
【０１１９】
周辺機器のセキュリティ
リーダによって接続されて、用いられる周辺機器は、周辺機器に提供される情報が信頼され得るように、または、リーダによって周辺機器に提供される情報が安全なままであり得るように、好ましくは安全にされる。したがって、周辺機器は、リーダにこのような接続されるデバイスが信頼可能であることを確認することが可能であるサーバで、好ましくは集合的に、または、個々に登録され得る。認証手順は、周辺機器が秘密鍵を含み、関連する公開鍵がサーバにとって公知で、共有鍵の作成がリーダと周辺機器の間の後の通信のために使われることができるという検証を含むことができる
【０１２０】
追加セキュリティ
他のセキュリティ対策を導入することができ、以下を含む。
・　電子デバイスをユーザと関連付けることであって、このような関連付けは、電子デバイスに、または、サーバに報告される。
●　電子デバイスの保有者が自分自身を識別して、例えばPINコードを入力することによって、または、デュアルリーダの隣に電子デバイスを配置する前に生体認証デバイスを用いることによって、トランザクションを確認する要件。これらの識別手段は、デュアルリーダ上に、または、電子デバイス上に無差別に位置していてもよく、またはデュアルリーダが接続可能である装置によってデュアルリーダがアクセス可能でさえあってもよい。したがって、デュアルリーダまたは電子デバイスはユーザを識別するための手段を含むことができ、これらの手段は生体認証が可能である。
・　トランザクションを確認するかまたはPINを入力するための電子デバイスへのボタンまたは生体認証デバイスの追加。
・　メッセージ、ファイルまたは数量を表示するための電子デバイスへのスクリーンの追加。
・　有効期限日付などの属性のファイルへの追加。
【０１２１】
本発明は、その例示的な非限定的なモードの実装の以下の詳細な説明を読み込み、そして、添付の図面を検討すると直ちに、よりよく理解することが可能であろう。
【図面の簡単な説明】
【０１２２】
【図１】本発明を実施するための例示的なシステムを概略的に示す。
【図２】本発明による例示的なデータ交換方法の種々のステップを示すブロック図である。
【図３】本発明の変形実装の図2に類似した図である。
【図４】本発明による電子デバイスとサーバに接続しているサードパーティソフトウェア間のデータフローのタイミングの例の図である。
【図５】本発明による電子デバイスとサーバの間でデータを同期するために実施可能な種々のステップを示す図である。
【図６】電子デバイスの、または、リーダのリストおよび鍵を更新するために実施可能な種々のステップを示す図である。
【図７】電子デバイスの、または、リーダのソフトウェアを更新するために実施可能な種々のステップを示す図である。
【図８】リーダをサーバと同期させるために実施可能な種々のステップを示す図である。
【図９】安全なデバイスにおけるファイルを作成するかまたは訂正するためにユーザによって実施可能な種々のステップを示す図である。
【発明を実施するための形態】
【０１２３】
図1は、本発明による方法を実施するための例示的なシステムを示す。

【０１２４】
このシステムは、示される例のクレジットカードのフォーマットで、情報を本発明による2つの電子デバイス20Aおよび20Bと交換するように構成される、本発明によるデュアルリーダ10を含む。
【０１２５】
デュアルリーダ10および電子デバイス20Aおよび20Bは、例えばインターネットまたは無線リンクを介して、そして、該当する場合、マイクロコンピュータ40または携帯電話41などの補助デバイスによって、情報を少なくとも1つのリモートサーバ30と交換することができる。
【０１２６】
2つの電子デバイス20Aと20Bの間でトランザクションを実行するための本発明による例示的な方法のステップの図2を参照して、ここで説明を行う。トランザクションが行われることが可能であるように電子デバイス20Aおよび20Bが同時にデュアルリーダ10に接続していなければならないので、このトランザクションはこの例では、同期していると言われ、第1の安全な接続および第2の安全な接続は、時間的に重複しており、第1の接続は接触を基にしたものでもよくて、第2の接続は非接触でもよい。
【０１２７】
したがって、トランザクションは、本発明による第1の電子デバイス20Aを有する第1のユーザAと本発明による第2の電子デバイス20Bを有する第2のユーザBの間に起こる。
【０１２８】
ユーザAは、ステップ201で、自分の電子デバイス20Aをデュアルリーダに挿入することによって開始する。ユーザBは、そこに含まれるファイルおよび数量の性質をリーダに知らせるために、おそらくステップ201その2においてリーダの隣に、自分の電子デバイスを配置することができる。
【０１２９】
ステップ202において、ユーザAは、自分が実行することを望む動作、例えば。トランザクション／残高または残高-残高を作成する、を選択し、後者の選択は2つのデバイス20Aおよび20Bの残高を示すことに対応する。
【０１３０】
次に、ステップ203で、ユーザは、方向(送信かまたは受信)、ファイル、またはトランザクションの数量を選択し、そして、該当する場合、数量、すなわち金融トランザクションの場合は量を提供する。
【０１３１】
いくつかのトランザクションがリンクされている場合、すなわち、交換は、同時に送信されるかまたは受信されるいくつかのファイルまたは数量から成っていなければならない場合、ステップ203は繰り返されでもよい。
【０１３２】
ステップ204において、いくつかのトランザクションはまた、最初に選択されたトランザクションがそのように要求する場合、自動的に生成することもでき、例えば、転送された文書は価格に関連付けることができて、それらの値と一致している支払がそれらの転送に応じて発生することが必要であり得、または、逆に言えば、数量の支払は受信デバイスの上に設定されて領収書を生成することができ、このような自動的に生成されたトランザクションはユーザに示され、ユーザは、動作を確認するか、またはもしあれば、自動的に生成されたトランザクションをただ確認するために、おそらく自分のPIN(個人識別番号)コードを入力する。
【０１３３】
ユーザBは、ステップ205で、デュアルリーダ10のスクリーンに、自分にトランザクションを提供しているか、または、自分の残高を発見するための情報の項目を読み込むことができる。
【０１３４】

ユーザは、動作がこれを必要とする場合、ステップ206においてPINコードを入力することができ、そして、ステップ207において、自分の電子デバイス20Bをデュアルリーダ10に配置してトランザクションを実行する。いくつかのトランザクションが、遂行されるべきで、かつ確認されるべきトランザクションのリストにまだ載っていない、いくつかの自動的に生成されたトランザクションを必要とする、とデバイスB上で報告される場合、そのような自動トランザクションが生成されて、プロセスはステップ204で再開する。

【０１３５】

ステップ208において、リーダは、トランザクションが終了したことを表示する。

【０１３６】

それから、ユーザBはステップ209において自分のカードを除去することができて、ユーザAはステップ210において同じことをすることができる。

【０１３７】

ステップ211において、リーダは、交換に関する情報をサーバに送信する。

【０１３８】

グループ化されたトランザクションの場合、同じ一つのコードが、各トランザクションに割り当てられてもよい。トランザクションは、まず第1の電子デバイスに登録されるが、「条件付き」と識別されてコードと関連付けられる。条件付きであることによってシステムはクレジットでなく電子デバイスへ書き込まれるデビットを考慮することができ、クレジットは条件付きであることが除去された場合にだけ考慮される。それから、トランザクションは、また、条件付きで第2のデバイスに登録されて、同じコードと関連付けられるが、しかし、この場合、条件付きであることが除去されない限り、どのトランザクションも考慮され得ないか、またはデビット処理トランザクションだけしか考慮され得ない。上記条件付きであることは、条件付き除去ラインと呼ばれる新たなラインの第2のデバイスへの書込みによって、書込み終了時点で、システムでパラメータ化される合理的な時間の範囲内で、除去されてもよい。この最後のラインは、一旦リーダに送信されると、第1のデバイスに送信されて、第1の電子デバイス上に登録されたこの単一ラインはこのデバイスにおける同じコードと関連したトランザクションに対して条件付きであることを除去する。命令は、その後に、サーバに伝達される。条件付きであることの除去が第2の電子デバイス上に合理的な時間の範囲内で登録されない場合、リーダは、第2のカードのこの読み取りの間、または第1のカードの再読み取りの間、またはその後に、グループ化されたトランザクションをキャンセルする書込み動作を作り出す。この書込み動作は、第1のデバイスがそれをまだ受けていない場合は第1のデバイスに、または第2のデバイスがそれをまだ受けていない場合は第2のデバイスに、そして、サーバに伝達される。このコードと関連したデビットまたはクレジットトランザクションの全ては、それから、キャンセルされる。サーバは、その後に、2つの電子デバイスへ書き込まれるこれらのトランザクションを削除する命令を準備することに対する責任を果たすことができる。

【０１３９】

システムに存在するファイルの、または、数量の転送は、上記ファイルおよび数量に付加される他のルール、例えばそれらの転送を身分証明書のコピーの転送に対して条件付きにすることによって拘束されることもでき、それはおそらくそれ自体電子デバイスの保有者のバイオメトリック認証に対して条件付きである。転送制約は、例えば、トレーダ発行の請求書に対して、請求書の総計に対応する金銭の相互転送でもよく、そうでなければ、オブジェクトを購入するときに法律によって要求される二酸化炭素排出クレジットの転送でもよい。

【０１４０】

非同期トランザクションの場合の、本発明の1つの変形実装の図3を参照して、ここで説明がなされる。

【０１４１】

ユーザAは、ステップ301で、デュアルリーダ10の近くに自分の電子デバイス20Aを持ってくることによって開始し、ユーザBは、ステップ301その2で同じことを行う。これらの

動作は、リーダに、リーダの隣に配置される各電子デバイスに含まれるファイルおよび数量のリストを送信するために用い、リーダが、その構成に応じて、電子デバイス上に転送可能なファイルおよび数量を知っていることを省くことが可能である場合、それらの動作は省略することができる。

【０１４２】

ステップ302において、ユーザAは、自分が実行することを望む動作、例えば、トランザクション／残高または残高-残高を作成する、を選択し、後者の選択は、2つのデバイス20Aおよび20B上で利用可能な数量を表示することに対応する。

【０１４３】

次に、ステップ303で、ユーザは、方向(送信かまたは受信)、ファイル、またはトランザクションの総計を選択する。

【０１４４】

いくつかのトランザクションがリンクされている場合、ステップ303は繰り返されてもよい。

【０１４５】

ステップ304において、ユーザAは自分のPINコードを入力して、動作を確認することができる。

【０１４６】

それから、トランザクションは、「未知の」相手を有するデュアルリーダ10によって準備される。

【０１４７】

ステップ305において、デュアルリーダは、提案されるトランザクションを表示して、ユーザAに自分のカードを近くに持ってくるように促す。

【０１４８】

ステップ306において、ユーザAは、例えばカード形式の自分のデバイスを近くに持ってくる。デビットトランザクションの全ては、この電子デバイス上でデビット処理される各利用できる数量がデビット処理される総計に少なくとも等しく、そしていかなるクレジット処理された数量もその最大値を超えないように検証される。リーダは、この電子デバイスからデビット処理されるファイルおよび数量を、サーバによって電子デバイスにすでに登録されているファイルおよび数量にリンクしている、以前のトランザクションのコピーを作成する。1つまたは複数の利用できる数量が十分でない場合、動作はキャンセルされ、逆のケースでは、ステップ307で、ユーザBは、おそらく、自分のPINコードを入力して自分のデバイスを近くに持って来るように促される。

【０１４９】

ステップ308において、ユーザBは、自分のPINコードを入力する。

【０１５０】

ステップ309において、ユーザBは、例えばカード形式の自分のデバイス20Bを近くに持ってくる。デビットトランザクションの全ては、このデバイス上でデビット処理される各利用できる数量がデビット処理される総計に少なくとも等しいように検証される。1つまたは複数の利用できる数量が十分でない場合、トランザクションをキャンセルする書込み動作が生成されてこのデバイスに登録される。逆の場合には、トランザクションがそこで登録される。デバイス20Aにおけるステップ306で集められた以前のトランザクションは、電子デバイス20Bへコピーされる。したがって、交換に関する情報の項目は、同じ一つのレジスタまたは同じ一つのファイルに関する以前の交換に関する情報を含む。リーダは、この電子デバイス20Bからデビット処理されるファイルおよび数量を、サーバによって電子デバイスにすでに登録されているファイルおよび数量にリンクしている、以前のトランザクションのコピーを作成する。登録およびコピーは命令を書き込んでトランザクションを確認することによって認められ、それがこれらのトランザクションをデバイス20B上で有効にする。

【０１５１】

ステップ310において、ユーザBは自分のデバイスを除去するように促され、ユーザAは自分のデバイスを近くに持ってくるように促される。

【０１５２】

ステップ311において、ユーザAは、自分のデバイスを近くに持ってくる。確認または無効化の命令が、電子デバイス20Aに送信される。このデバイス20Aへ書き込まれたトランザクションは、デバイス20Bの最終的に分かる識別情報によって、同時に更新される。ステップ309で集められた以前のトランザクションは、電子デバイス20Aへコピーされる。このステップ311が省略される場合、これらの動作はその後にサーバとの別の同期の間に実行されるが、それはこれらサーバが同じリーダによって、または、デバイス20Bがその後に通信した別のリーダによってそれらに伝えられた確認命令を受信した後である。

【０１５３】

ステップ312において、リーダは、トランザクションが終了したことを表示して、ユーザAに自分のデバイスを除去するように促す。

【０１５４】

ステップ313において、この交換の間に生成されたトランザクションおよび確認命令は、ステップ306および309でデバイス20Aおよび20Bからコピーされたトランザクションとともに、サーバに送信される。

【０１５５】

図4は、ユーザ、関連する電子デバイスおよび、ファイルの挿入(クレジット)もしくは除去(デビット)またはシステムの、電子デバイスに割り当てられる数量における変化を制御している外部のウェブサイト間のデータ交換の例を示す。

【０１５６】

電子デバイス20Aまたは20Bは、例えばクレジットカード形式である。それは、デュアルリーダ10により、または、コンピュータもしくは電話により、サーバと通信することができる。ユーザは、それ自体がサーバ30と通信するウェブサイトと通信することができる。

【０１５７】

ステップ401において、ユーザは、サードパーティサイトとのセッションを開く。

【０１５８】

ステップ402において、ユーザは、おそらくリーダの隣に電子デバイス20Aを配置する。上記リーダは、サーバに接続されており、デバイス20Aとサーバ30を同期させる。数量は、図5にて図示したように、最新のトランザクションに応じて更新される。転送がファイルの、または、デバイスからサードパーティサイトへの数量の転送を必要としない場合、このステップは必要とされないことがある。

【０１５９】

ステップ403において、ユーザは、上記サイトとの間で転送されるサードパーティサイトにおけるトランザクションのファイルまたは数量および方向を選ぶ。電子デバイスの残高を更新する命令が準備される。

【０１６０】

ステップ404において、サードパーティサイトは、それがトランザクションを行うことが可能なことを検証する。それは、例えば暫定的にユーザの銀行口座をデビット処理することができて、それからサーバに、考えられるファイルを送信し、最後に、トランザクションを表示して、ユーザの電子デバイス20Aをリーダの近くに持ってくることによって、または、電子デバイス20Aがサーバとすでに通信している場合はアイコンをクリックすることによって、それを確認するように、ユーザに申し出る。

【０１６１】

ステップ405において、ユーザは、自分の電子デバイス20Aをリーダ10の近くに持ってくるか、またはアイコンを押す。それから、数量を更新する命令は、デバイス20Aへ書き込まれる。ステップ404においておそらくサードパーティサイトから送信されるファイルは、デバイス20Aに、および、おそらくシステムのサーバにコピーされる。このステップが合理的な時間の範囲内に行われない場合、トランザクションはキャンセルされて、サード

パーティサイトはこれを知らされて、ステップ404で送信される考えられるファイルはサーバから、および、デバイス20Aから削除される。逆のケースにおいては、サードパーティサイトは、動作が成功していることを知らされる。デバイス20Aからサードパーティサイトへ送信されるファイルは、サーバからサードパーティサイトへ有効に送信されて、おそらくサーバから削除され、それから、デバイスから上記ファイルを削除する命令が生成される。

【０１６２】

ステップ406において、リーダは、トランザクションが終了したことを表示して、ユーザに自分のデバイス20Aを除去するように促す。

【０１６３】

ステップ407において、ユーザは、自分のデバイス20Aを除去する。

【０１６４】

図5は、例えばクレジットカード形式の電子デバイスとサーバの間で行われることが可能な、同期交換の例を示す。この交換は、電子デバイスがリーダと通信して、リーダがサーバと通信するときに、行われる。したがって、それは、所要時間の間、リーダにカード20Aを挿入することまたは、カード20Aをリーダの隣に配置することだけを必要とする。下記のステップは、リーダ10を通した、電子デバイス20Aとサーバ30との間での交換を説明する。

【０１６５】

ステップ501において、ユーザは、自分の電子デバイス20Aをリーダの近くに持ってくる。

【０１６６】

ステップ502において、サーバ30は、デバイス20Aに、それがすでに準備したトランザクション削除命令をおそらく送信する。

【０１６７】

ステップ503において、電子デバイス20Aに存在するトランザクション削除命令の全てが実施される。

【０１６８】

ステップ504において、デバイス20Aに存在するが、サーバに存在しない命令、トランザクションおよびファイルの全ては、サーバ10を通してサーバへコピーされる。

【０１６９】

ステップ505において、サーバは、新しい数量を、算出するか、またはシステムのサーバの1つによって算出してもらい、そしてデバイス20Aへコピーされるか、またはそれから削除されるトランザクションのリストを準備する。

【０１７０】

ステップ506において、削除命令、トランザクション、ファイルおよび、サーバ30に存在するが、電子デバイス20Aに存在せず、しかしステップ505において算出されるべき、または算出される新しい数量の全ては、電子デバイス20Aにコピーされる。

【０１７１】

ステップ507において、電子デバイス20Aに存在するトランザクション削除命令の全てが実施される。

【０１７２】

ステップ508において、ユーザは、自分の電子デバイスを除去するように促される。

【０１７３】

図6は、鍵の更新処理の、そして、リーダまたは電子デバイスに存在する鍵のリストの、更新処理の例示的な編成を示す。

【０１７４】

この図は電子デバイス(DE)およびリーダが存在すると仮定するが、しかし、以下のステップはリーダだけの同期にもあてはまる。

【０１７５】

ステップ601において、電子デバイスまたはリーダは、その識別情報をサーバに送信する。

【０１７６】

サーバは、

a．　鍵の更新処理、

b．　鍵のリストの更新処理、

を準備して、暗号化して、署名し、

その結果、電子デバイスまたはリーダだけがそれらを読み込むことが可能である。それは、秘密鍵は電子デバイスまたはリーダに存在する、ということをそれが知っているその鍵の1つによって暗号化ファイルに署名する。これらの更新ファイルは、削除されるべき、置き換えられるべき、そして追加されるべき要素に関する情報を含む。それらは、段階的な更新処理を許容するように、いくつかのファイルに分割することができる。

【０１７７】

ステップ602において、暗号化されかつ署名されたファイルは、電子デバイスまたはリーダに送信される。

【０１７８】

ステップ603において、電子デバイスまたはリーダは、ファイルの署名を検証して、それを暗号解読する。

【０１７９】

ステップ604において、電子デバイスまたはリーダは、鍵および鍵のリストをこの目的のために設けられているその内蔵メモリにインストールして、そして、この更新を考慮に入れることを引き起こす。

【０１８０】

ステップ605において、デバイスまたはリーダは、サーバに更新ファイルを考慮に入れることを知らせる。

【０１８１】

ステップ606において、電子デバイスまたはリーダは、そのメモリから、もう使われていない情報を削除する。

【０１８２】

図7は、リーダの、または、電子デバイスのソフトウェアの更新処理の例示的な実装を示す。

【０１８３】

この図は電子デバイス(DE)およびリーダが存在すると仮定するが、しかし、以下のステップはリーダだけの同期にもあてはまる。

【０１８４】

ステップ701において、電子デバイスまたはリーダは、その識別情報をサーバに送信する。

【０１８５】

ステップ702において、サーバは、電子デバイスまたはリーダだけがそれを読み込むことが可能であるように、インストールされるソフトウェアを暗号化する。それはまた、公開鍵は電子デバイスまたはリーダに存在する、ということをそれが知っているその鍵の1つによって、このように暗号化されたファイルに署名する。

【０１８６】

ステップ703において、暗号化されかつ署名されたファイルは、電子デバイスまたはリーダに送信される。

【０１８７】

ステップ704において、電子デバイスまたはリーダは、ファイルの署名を検証して、それを暗号解読する。

【０１８８】

ステップ705において、電子デバイスまたはリーダは、すでにインストールされるソフ

トウェアをまだ削除せずに、この目的のために設けられているその内蔵メモリにソフトウェアをインストールする。

【０１８９】

ステップ706において、電子デバイスまたはリーダは、新規のソフトウェアが実際にコピーされていて、電子デバイス(またはリーダ)の起動命令を変更するということを検証し、それにより、上記デバイスは、それが再び起動するときに、新規のソフトウェアを用いて再び起動する。

【０１９０】

ステップ707において、電子デバイスまたはリーダは、再び起動される。

【０１９１】

起動に際して、ステップ708において、電子デバイスの、または、リーダの古いソフトウェアは、それがまだそこに存在する場合には削除される。

【０１９２】

図8は、サーバとのリーダの例示的な同期を説明する。

【０１９３】

ステップ801において、証明書およびリストが更新される。

【０１９４】

ステップ802において、リーダで実行されてその上に格納されるトランザクションが、サーバに送信されて、それから削除される。

【０１９５】

ステップ803において、不正だとマークされるかまたは停止されるべき電子デバイスのリストの受信があり得る。

【０１９６】

図9は、安全なデバイス上でファイルを作成するかまたは訂正するためにユーザによって実施され得る種々のステップを表す。

【０１９７】

ステップ901において、ユーザは、リーダの隣に自分の安全なデバイスを持ってくる。

【０１９８】

ステップ902において、ユーザは、自分が訂正したいファイルを選択するか、または「新規ファイルを作成する」をリーダのメニューから選ぶ。

【０１９９】

ステップ903において、ファイルに関連付けられた量がファイルに関連付けることができる最大量に等しく、そしてファイルが「修正可能」としてマークされている場合、ファイルがリーダに表示されて、その編集を許容している関数が起動される。ユーザが「作成された新規ファイル」を選択した場合、ブランクファイルがリーダに表示されて、その編集を許容している関数が起動される。

【０２００】

ステップ904において、ユーザはファイルを編集する。

【０２０１】

ステップ905において、ユーザは、その最小量、最大量、インクリメントなどのファイルの特性、または、システム内のファイルについて行われ得ることに影響を与える、例えば「転送され得る」、あるいは「閲覧するために生体認証デバイスを必要とする」などの他の特性のいくつかを編集することができる。それから、ファイルに付加される量は、その最大許容量に設定される。

【０２０２】

ステップ906において、ユーザは、リーダの隣のデバイスに再び接近する。

【０２０３】

ステップ907において、ファイルは、デバイスにコピーされる。

【０２０４】

ステップ908において、リーダがサーバに接続されている状態が起こる場合に、または

後でリーダがサーバに接続されると、ファイルは、サーバにコピーされる。

【０２０５】

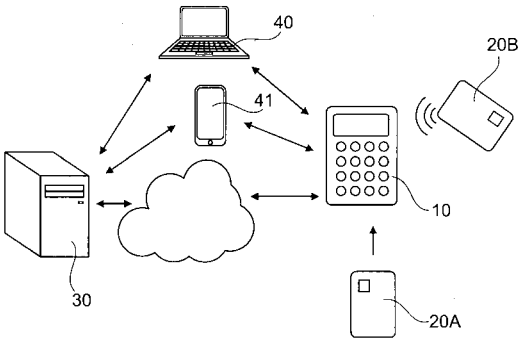
ステップ909において、カードは、別のリーダとのサーバへの接続を通して、サーバにファイルのコピーを置くこともできる。

【符号の説明】

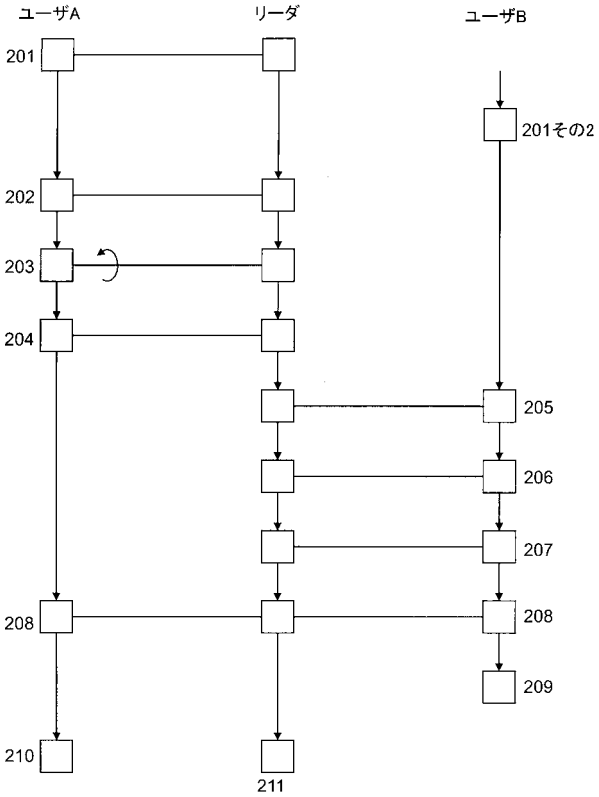
【０２０６】

10　デュアルリーダ
20A　電子デバイス
20B　電子デバイス
30　リモートサーバ
40　マイクロコンピュータ
41　携帯電話

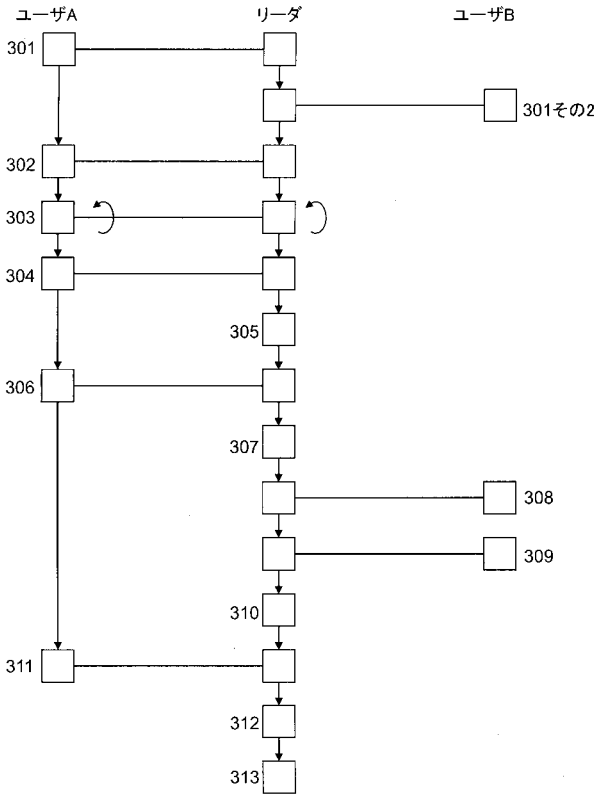
【図１】



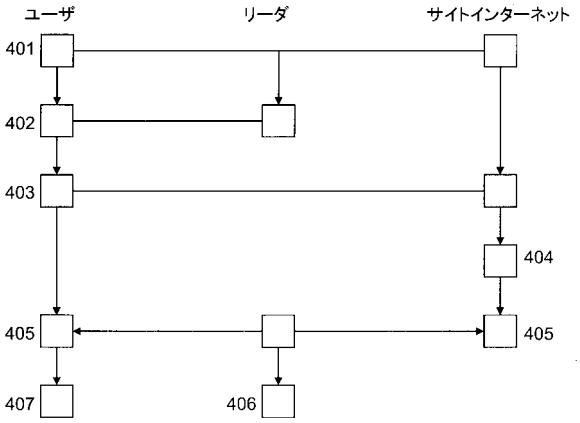
【図２】



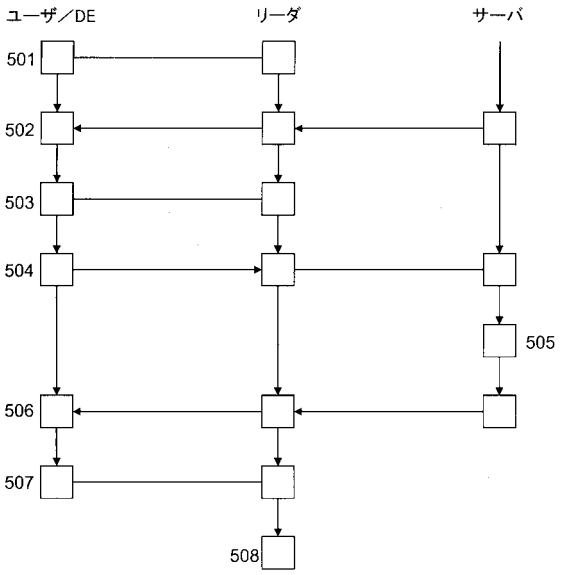
【図３】


ユーザA
リーダ
ユーザB
301
301その2
302
303
304
305
306
307
308
309
310
311
312
313

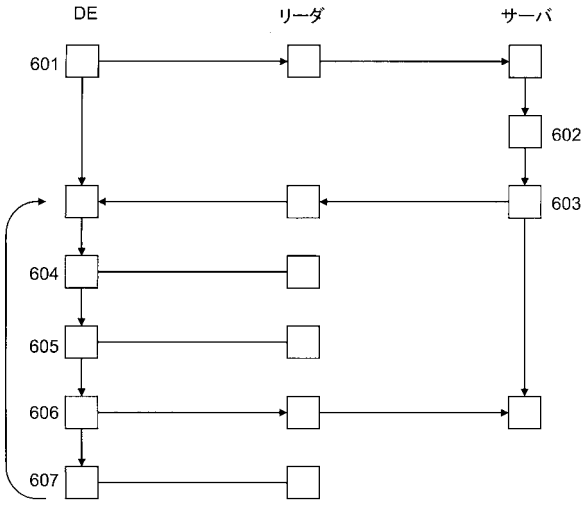
【図４】


ユーザ
リーダ
サイトインターネット
401
402
403
404
405
405
406
407

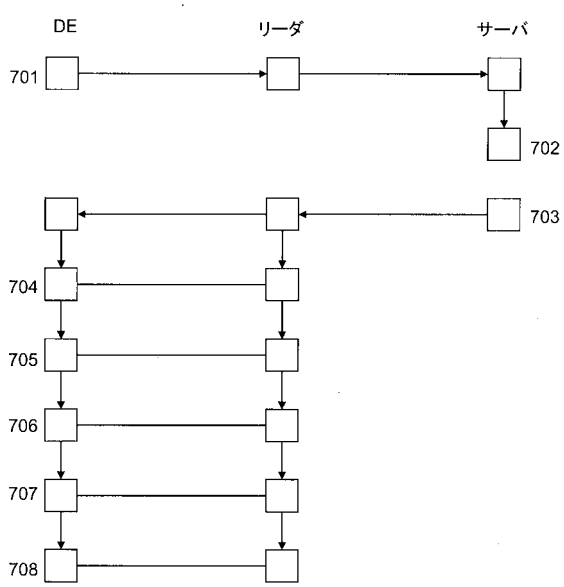
【図５】


ユーザ／DE
リーダ
サーバ
501
502
503
504
505
506
507
508

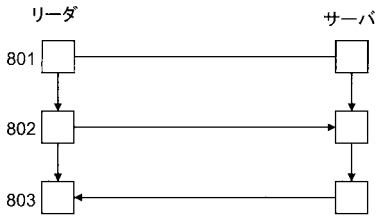
【図６】


DE
リーダ
サーバ
601
602
603
604
605
606
607

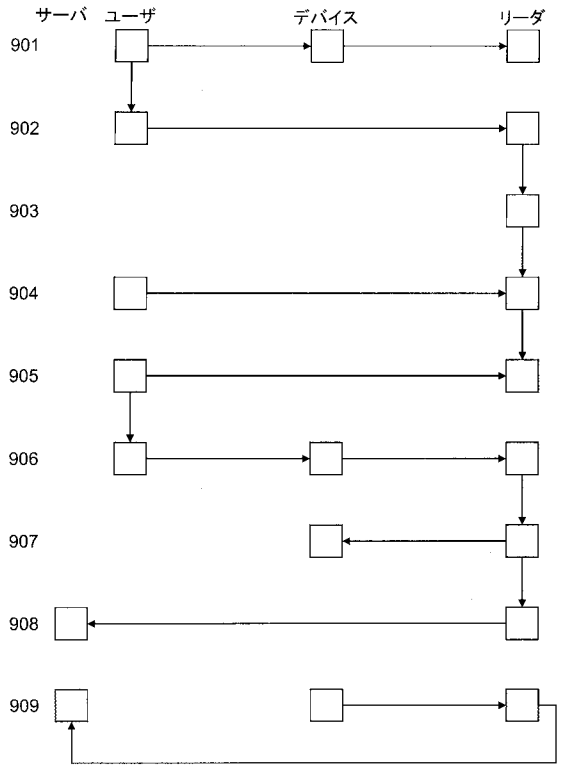
【図７】


DE
リーダ
サーバ
701
702
703
704
705
706
707
708

【図８】


リーダ
サーバ
801
802
803

【図９】


サーバ
ユーザ
デバイス
リーダ
901
902
903
904
905
906
907
908
909

【外国語明細書】
2019194858000001.pdf