(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6329485号
(P6329485)
(45)発行日　平成30年5月23日(2018.5.23)　(24)登録日　平成30年4月27日(2018.4.27)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/31
H04L 9/32 (2006.01)　　H04L 9/00 673C

請求項の数 9　(全 14 頁)

(21)出願番号　特願2014-536127(P2014-536127)
(86)(22)出願日　平成24年9月26日(2012.9.26)
(65)公表番号　特表2015-501028(P2015-501028A)
(43)公表日　平成27年1月8日(2015.1.8)
(86)国際出願番号　PCT/EP2012/004033
(87)国際公開番号　WO2013/056783
(87)国際公開日　平成25年4月25日(2013.4.25)
審査請求日　平成27年4月22日(2015.4.22)
審判番号　不服2017-8832(P2017-8832/J1)
審判請求日　平成29年6月16日(2017.6.16)
(31)優先権主張番号　102011116489.1
(32)優先日　平成23年10月20日(2011.10.20)
(33)優先権主張国　ドイツ(DE)

(73)特許権者　514098986
トラストニック　リミテッド
イギリス国　シービー１　２ジェイディー　ケンブリッジ、ステーション　ロード　２０
(74)代理人　110000855
特許業務法人浅村特許事務所
(72)発明者　スピッツ、ステファン
ドイツ連邦共和国、カールスフェルト、パルクシュトラーセ　１８

合議体
審判長　辻本　泰隆
審判官　仲間　晃
審判官　山崎　慎一

最終頁に続く

(54)【発明の名称】移動端末、処理端末、及び、移動端末を用いて処理端末で処理を実行する方法

(57)【特許請求の範囲】
【請求項１】
移動端末（２０）を用いて処理端末（４０）で処理を実行する方法であって、
処理端末（４０）によってユーザを識別するステップと、
処理端末（４０）に対して識別されたユーザを認証するステップであって、移動端末（２０）の入力装置（２２、２４）を用いて、識別されたユーザによって入力されたパスワードが、識別されたユーザのために処理端末（４０）又は前記処理端末に接続されたバックグラウンド・システム（８０）に保存されたパスワードと、一致するかどうか確認することによって、認証するステップと、を備え、
ここで、プロセッサユニット（３３）が、移動端末（２０）内に提供され、前記プロセッサユニットには、通常のランタイム環境（ＮＺ）及び安全なランタイム環境（ＴＺ）が実装され、
入力装置のドライバ（３４）は、安全なランタイム環境（ＴＺ）に実装され、入力を移動端末（２０）の入力装置（２２、２４）を介して、移動端末（２０）のプロセッサユニット（３３）の安全なランタイム環境（ＴＺ）へ、更なる処理のために安全に転送するように構成され、
ユーザを認証するステップの間に、安全な通信経路が、移動端末（２０）と処理端末（４０）の間に形成され、少なくともセキュリティに関連したデータは、暗号化方法によって暗号化された形態で送信され、
通信モジュール・ドライバ（３５）が、移動端末（２０）と処理端末（４０）の間に安

全な通信経路を形成するために、安全なランタイム環境（ＴＺ）に実装されて、プロセッサユニット（３３）によって提供されたデータを、移動端末（２０）の通信モジュール（２６）と前記安全な通信経路を介して、安全に処理端末（４０）に送信するように構成されている、方法。

【請求項２】

処理端末（４０）によってユーザを識別するステップの間に、ユーザが所有している支払いカード（６０）に保存され、ユーザを一意に識別する識別データ要素が、処理端末（４０）の読取機（４８）によって接触方式または非接触方式で読み込まれ、又は、移動端末（２０）に保存され、ユーザまたは移動端末（２０）を一意に識別する識別データ要素が、読み込まれる、請求項１に記載された方法。

【請求項３】

ユーザを認証するステップの前に、少なくとも一方向の認証が、移動端末（２０）の通信モジュール（２６）と処理端末（４０）の間で使用され、この認証の間に、処理端末（４０）が、移動端末（２０）に対して認証される、および、移動端末（２０）が、処理端末（４０）に対して認証される、の少なくとも一方が行われる、請求項２に記載された方法。

【請求項４】

移動端末（２０）、および、処理端末（４０）と処理端末（４０）に接続されたバックグラウンド・システム（８０）の少なくとも一方に保存される認証キー（Ｋ、Ｋ＊）が、移動端末（２０）と処理端末（４０）の少なくとも一方によって認証を実行するために用いられ、移動端末（２０）に保存されるキー（Ｋ）は、個別のキーである、請求項３に記載された方法。

【請求項５】

移動端末（２０）と処理端末（４０）間の安全な通信経路を経た通信は、認証キー（Ｋ、Ｋ＊）に基づいて暗号化され、認証キー（Ｋ、Ｋ＊）は、各処理用の新規なそれぞれのセッションキーを作り出すために、それぞれのマスターキーとして使われるようになっている、請求項４に記載された方法。

【請求項６】

安全なランタイム環境（ＴＺ）は、ＡＲＭ（商標）ＴｒｕｓｔＺｏｎｅ（商標）である、請求項１乃至請求項５のいずれか一項に記載された方法。

【請求項７】

移動端末（２０）は、携帯電話であり、前記携帯電話のオペレーティングシステムは、通常のランタイム環境（ＮＺ）で動作する、請求項１乃至請求項６のいずれか一項に記載された方法。

【請求項８】

処理端末（４０）で処理を実行するための移動端末（２０）であって、

ユーザによってパスワードを入力するための入力装置（２２、２４）と、

通常のランタイム環境（ＮＺ）および安全なランタイム環境（ＴＺ）が実装されるプロセッサユニット（３３）と、を備え、

ここで、入力装置ドライバ（３４）が、安全なランタイム環境（ＴＺ）に実装され、入力を移動端末（２０）の入力装置（２２、２４）を介して、移動端末（２０）のプロセッサユニット（３３）の安全なランタイム環境（ＴＺ）へ、更なる処理のために安全に転送するように構成され、

アプリケーション（３６）も、プロセッサユニット（３３）の安全なランタイム環境（ＴＺ）に実装され、移動端末（２０）の入力装置（２２、２４）を用いてユーザによって入力されたパスワードが、このユーザのために処理端末（４０）又は前記処理端末に接続されたバックグラウンド・システム（８０）に保存されたパスワードと、一致するかどうか確認することによって、処理端末（４０）に対してユーザを認証できるように構成されており、

通信モジュール・ドライバ（３５）が、移動端末（２０）と処理端末（４０）の間に安

全な通信経路を形成するために、安全なランタイム環境（ＴＺ）に実装されて、プロセッサユニット（３３）によって提供されたデータを、移動端末（２０）の通信モジュール（２６）と前記安全な通信経路を介して、安全に処理端末（４０）に送信するように構成されており、

少なくともセキュリティに関連したデータは、前記安全な通信経路上を暗号化方法によって暗号化された形態で送信される、

移動端末（２０）。

【請求項９】

請求項８に記載の移動端末（２０）を含むシステム（１０）であって、

処理端末（４０）は、

ユーザを識別するように構成される制御ユニット（５０）と、

移動端末（２０）と処理端末（４０）の間に安全な通信経路を形成するための通信モジュール（４６）と、

を備え、

ここで、処理端末（４０）は、移動端末（２０）の入力装置（２２、２４）を用いてユーザに入力されたパスワードが、処理端末（４０）又は前記処理端末に接続されたバックグラウンド・システム（８０）に保存された識別されたユーザのためのパスワードと、一致するかどうか決定することによって確認が実行され、ユーザを認証するように構成されている、システム（１０）。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、移動端末（特に携帯電話）、処理端末、及び、当該移動端末を用いて当該処理端末で処理を実行する方法に関するものである。

【背景技術】

【０００２】

例えば、現金を引き出すため、現金を使用せずに購入品の代金を払うため、及び、チケットなどを購入するためなど、端末で決裁処理を実行するために、銀行顧客はEC、デビットまたはクレジットカード（以下略して支払いカードまたはカードと記載する）を使用できる。現金を引き出すために、顧客は、自分の支払いカードをキャッシュ・マシン（現金自動預払機またはＡＴＭとも呼ばれる）の形態の処理端末のカード読み取り装置に挿入し、現金自動預払機のキーパッドを用いて自分だけが知っている暗証番号（ＰＩＮ）を入力する。現金自動預払機は、ＰＩＮの正当性を点検するとともに出金を決定する認証センターを有するバックグラウンド・システムに接続されている。顧客が正しいＰＩＮを入力した場合、顧客に選択された額が顧客に支払われ、顧客の口座から支払額が引き落とされる。

【０００３】

一般に、現金自動預払機において、ＰＩＮを入力するために「ＰＩＮパッド」と呼ばれるキーパッドが使用される。ＰＩＮパッドは、現金自動預払機の暗号化ハードウェアと共にユニットを形成し、ＰＩＮが暗号化されていない形態で決して外界に渡らないように構成される。とりわけ、バックグラウンド・システムの認証センターにリクエストを転送するときに、現金自動預払機に実装される処理を実行するためのソフトウェアは、前々から、とりわけ暗号化されたＰＩＮ（当然に適用される）を用いてのみ動作する。

【０００４】

処理端末（特に、処理端末のキーパッドを使用してＰＩＮを入力しなければならない現金自動預払機）を用いて処理を実行するときに、「スキミング攻撃」の危険がある。この種のスキミング攻撃の典型的な攻撃パターンは、例えば、現金自動預払機において、口座番号、及び／又は、顧客の氏名、それに加えてＰＩＮといった、顧客の支払いカードの磁気帯に保存される顧客を識別するためのデータを同時に覗き見ることである。顧客のカードからのデータは、その後、典型的には空のカードにコピーされ、攻撃者によってＰＩＮ

とともに使用されて、現金自動預払機から現金が引き出される。従って、スキミング攻撃は、再生攻撃（リプレイアタック）である。カードは顧客が所有したままなので、一般に顧客がこの種の攻撃に気づくのは、新しい銀行取引明細書を受け取った場合だけ、又は、借越協約が借越しになった後に銀行が介入する場合だけ、すなわち、攻撃者が現金を顧客の口座からすでに回収し、それにより損害が発生した後だけである。

【０００５】

一方では、現金自動預払機において、スキミング攻撃の異なる形態が、知られるようになってきた。その共通の特徴は、現金自動預払機に取り付けられる読取機の小型化が進んだことで、読取機を用いた不正操作がきわめて容易になったという事実である。１つの異なる形態は、現金自動預払機の顧客の支払いカード用の挿入軸に小さいプラスチック・フレームの形態で読取機を直接に取り付けることを含む。そして、カードは、容易に追加された読取機を通して現金自動預払機に引き込まれ、カードの磁気帯の内容はその過程で読み込まれる。他の異なる形態は、銀行の支店のドア・オープナに追加の読取機を据え付けることを含む。その理由は、銀行の支店（現金自動預払機へのアクセスがある）のロビーへのアクセスには、カードを挿入することが必要なことがしばしばあるためである。

【０００６】

ＰＩＮの入力は、通常、例えば、現金自動預払機のキーパッドの上方に貼り付けられたプラスチック小片に隠された小さな無線カメラを使用して撮影される。疑い深いユーザであってさえも、この小片は、通常、ほとんど識別不可能である。しかしながら、キーパッドの完全な偽物もまた使用され、それは実際のキーパッドの上に貼り付けられて顧客によるキーパッドの入力（特に、ＰＩＮ）をたやすく記録する。

【０００７】

スキミング攻撃を防ぐ従来の方法は、通常、使い勝手の良いものではなく、複雑になっており、かつ／又は、スキミング攻撃を部分的に妨げることができるだけである。

【発明の概要】

【発明が解決しようとする課題】

【０００８】

このような背景に対して、本発明は、処理端末で処理を実行する方法と、スキミング攻撃に対して比較的に単純で、かつ、使い勝手の良い予防を提供する、対応する処理端末と、を提供することを目的としている。

【課題を解決するための手段】

【０００９】

本発明の第１の態様によれば、請求項１による移動端末を用いて処理端末で処理を実行する方法によって、この目的が達成される。本発明の第２の態様および第３の態様によれば、装置の独立請求項は、対応する移動端末および対応する処理端末に関する。本発明の有利な改良は、下位の請求項に規定される。

【００１０】

本発明は、処理端末（特に、現金自動預払機）で処理を実行するときに必要とされる、顧客を認証するためのパスワード（特に、ＰＩＮ）の入力を、スキミング攻撃にさらされる処理端末のキーパッドから、安全な移動端末（好ましくは、安全な携帯電話）の安全な入力装置へと、移動するという基本的な概念に基づくものである。安全な携帯電話は、安全な通信経路を介して処理端末と通信する。

【００１１】

この目的のために、安全な移動端末は、通常のランタイム環境および安全な、信頼されたランタイム環境が実装されるプロセッサユニットを備える。この場合、安全なランタイム環境は、通常のランタイム環境から分離されて、セキュリティが重要なアプリケーションを実行するために用いる。

【００１２】

本発明によれば、移動端末の入力装置を制御するための入力装置ドライバは、移動端末の安全なランタイム環境に実装され、移動端末の入力装置を用いて、移動端末のプロセッ

サユニットの安全なランタイム環境へと、入力を安全に転送するように構成される。これによって、移動端末の入力装置が、プロセッサユニットの信頼されたランタイム環境に安全に接続されるため、入力装置と移動端末のプロセッサユニット間の通信経路が、不正操作のための攻撃域として除外されることが、確実になる。

【００１３】

好ましくは、移動端末は、移動端末と処理端末の間に安全な通信経路を形成するように構成される通信モジュールも備える。この好ましい実施例において、通信モジュール・ドライバも、移動端末の安全なランタイム環境に好ましくは実装され、かつ、プロセッサユニットにより提供されるデータを、通信モジュールおよび安全な通信経路を介して、安全に処理端末に発信するように構成される。これによって、通信モジュールが、プロセッサユニットの信頼されたランタイム環境に安全に接続されるため、プロセッサユニットと移動端末の通信モジュール間の通信経路が、不正操作のための攻撃域として除外されることが、確実になる。

【００１４】

安全なランタイム環境の好ましい実施例のひとつは、従来技術から公知のＡＲＭ（商標）ＴｒｕｓｔＺｏｎｅ（商標）である。この場合、好ましくは同様に公知のＭｏｂｉＣｏｒｅ（商標）オペレーティングシステムである、分離された安全なオペレーティングシステムが、このＴｒｕｓｔＺｏｎｅ（商標）内部で動作する。

【００１５】

好ましくは、移動端末は、ディスプレイ装置ドライバによって制御されるディスプレイ装置も備える。ディスプレイ装置ドライバは、好ましくは、プロセッサユニットの安全なランタイム環境に実装される。入力装置およびディスプレイ装置がタッチスクリーンの形態である移動端末において、これは特に有利である。

【００１６】

処理端末で処理を実行するための本発明による方法において、支払カード（例えば、ＥＣ、デビット、又はクレジットカード）を用いて、支払いカードが処理端末の挿入軸に挿入され、処理端末の読取機によって読み込まれることによって、顧客は、好ましくは処理端末に対して識別される。支払いカードは、好ましくは、顧客を一意に識別することを可能にする、顧客に関連する識別データ要素（例えば、主要口座番号（ＰＡＮ）、口座番号、カード番号、顧客の氏名、および／または、その他）を格納する磁気帯を備える。同様に、顧客は、代替的にまたは追加的に支払いカードを用いて非接触方式で識別されることもできる。すなわち、エア・インタフェースを介して支払いカードと処理端末の間で安全な通信によって識別されることもできると考えられる。

【００１７】

処理端末が異なる処理が選択されることを許容する場合には、好ましい実施例においては、顧客が支払いカード及び格納されたデータ（少なくとも１つの識別データ要素を含む）を用いて処理端末に対して識別された後に、顧客は自信が望む処理を（例えば、処理端末のキーパッドまたはタッチスクリーンを用いて）選択するはずである。しかしながら、同様に、移動端末を用いて（例えば移動端末の入力装置を用いて）実行される望まれる処理の選択は、好ましくは、正確には安全な通信経路が移動端末と処理端末の間に形成された後であると考えられる。

【００１８】

顧客が識別データ要素を用いて識別され、かつ、処理がおそらく顧客によって選択された後、安全な通信経路が、エア・インタフェースを介して処理端末と移動端末の通信モジュールの間に好ましくは設定される。本発明の範囲内で、安全な通信経路とは、少なくとも安全に関連したデータ（例えば、ＰＩＮ）が移動端末と処理端末の間で（例えば、暗号化方法を用いて）暗号化された形態で送信される通信経路のことを意味するものと理解される。

【００１９】

処理端末と移動端末の通信モジュールは、好ましくは、エア・インタフェースを介した

処理端末と移動端末の間の通信が、近距離無線通信の規格またはプロトコルによって実行されるように構成される。その場合、移動端末が処理端末の近接場に入ると、移動端末と処理端末の間に安全な通信経路が形成される。好ましい近距離無線通信の規格またはプロトコルは、ＮＦＣ、ブルートゥース、ＲＦＩＤ、ＷＬＡＮ、ＤＥＣＴ、ＺｉｇＢｅｅまたは赤外線である。ＮＦＣ標準による通信の好ましい使用の間、好ましくは、処理端末がＮＦＣ読取機の役割を担い、移動端末またはその通信モジュールがＮＦＣタグまたはＮＦＣトランスポンダ（応答装置）の役割を担う。代案として、処理端末と移動端末の間のＮＦＣ通信は、ピア・ツー・ピア方式で実行されることもできる。しかしながら、近距離無線通信の規格またはプロトコルを用いて移動端末と処理端末の間で通信していても、移動端末および処理端末は、他の通信方式を用いて（例えば、ＳＭＳを用いて）、互いに無線で通信することもできる。

【００２０】

移動端末と処理端末の間の安全な通信経路を設定するときには、少なくとも一方向の認証（例えば、チャレンジレスポンス方式の形態）が、好ましくは使用される。その認証の間に、処理端末は、移動端末に対して本物であることが認証される。これにより、移動端末は、攻撃者が所有しており処理端末のようにふるまう通信装置を用いることなく、処理端末と実質的に通信することが確実になる。

【００２１】

他の好ましい実施例では、正確には好ましくは再びチャレンジレスポンス方式の認証を用いて、移動端末も、処理端末に対して認証される必要がある。この好ましい実施例の利点は、特に、支払いカードによって識別された顧客が所有する移動端末と通信しているか、又は、他の移動端末（例えば、可能性のある攻撃者が所有する移動端末）と通信しているか、処理端末が確認できるという事実である。後の場合では、好ましくは処理端末が処理を実行することを拒絶するようにしておく。

【００２２】

認証を実行するために、処理端末（または処理端末に接続しているバックグラウンド・システム）及び移動端末に、適切な電子キーを保存できる。これらは、望ましくはそれぞれの移動端末用の個々のキーを有する複数の認証キー、および、例えば顧客のための識別データ要素と共にバックグラウンド・システムに保存される処理末端の対応する単一のキーである。

【００２３】

安全な通信経路が処理端末と移動端末の通信モジュールの間に形成された後、移動端末の入力装置はパスワード（好ましくは、ＰＩＮ）の入力のために使用できる。この場合、処理端末のディスプレイ装置および／または移動端末のディスプレイ装置に、対応する表示をすることができる。代替的にまたは追加的に、顧客は、もうひとつの合図（例えば、着信音）を用いて、移動端末の安全な入力装置を用いてパスワードを入力するように求められることができる。

【００２４】

移動端末の安全な入力装置を使用して顧客によって入力されたパスワードは、通信モジュールおよび安全な通信経路を介して処理端末に送信される。この場合、パスワードは、プレーンテキストではなく、好ましくは、暗号化された形態で送信される。その場合、暗号化は、認証キーに基づく。１つの好ましい実施例によれば、認証キーは、この場合、各処理のためのそれぞれのセッションキーを作り出すために、それぞれのマスターキーとして用いられる。それぞれのセッションキーは、例えば、移動端末及び処理端末が乱数を交換し、この乱数がそれぞれ移動端末に格納されたマスターキー又は処理端末に格納されたマスターキーを用いて、暗号化されることによって作り出される。

【００２５】

移動端末の入力装置を使用して顧客によって入力され、安全な通信経路を介して処理端末に送信されるパスワードは、処理端末および／または処理端末に接続しているバックグラウンド・システムに識別データ要素とともに保存されるパスワードと同一であることが

確認された後に、処理端末および／または処理端末に接続しているバックグラウンド・システムによって、顧客が望む処理（例えば現金の引き出し）が可能にされる。

【００２６】

処理アプリケーション（ＭｏｂｉＣｏｒｅ（商標）オペレーティングシステムの範囲内では処理トラストレット(ｔｒａｎｓａｃｔｉｏｎ　ｔｒｕｓｔｌｅｔ)とも呼ばれる）は、好ましくは、移動端末の安全なランタイム環境で動作し、移動端末による本発明による処理を実行するのに必要なステップを、制御（すなわち、実行および／または促進）する。

【００２７】

代替的な実施例によると、支払いカードの機能（特に顧客を識別するため）は、顧客の移動端末に一体化されることも考えられる。この場合、顧客は、支払いカードを用いて接触方式又は非接触方式で識別されるのではなく、移動端末に格納されており移動端末又は顧客を一意に識別する識別データ要素を用いて識別される。

【００２８】

当業者が認識するように、本発明は、例えば、現金を引き出したり預け入れたりといった処理において、または、例えばＰＩＮを入力することが必要な支払いカードを用いる支払い作業といった現金を用いない支払処理において、などの数多くの場合に好適に用いることができる。本発明の意味において、処理端末は、現金を引き出しおよび／または預け入れる現金自動預払機（ＡＴＭ）であってもよいし、販売場所で現金を用いず支払うためのＰＯＳ端末であってもよいし、例えば、送金を実行するための銀行サービス端末であってもよいし、チケット端末等であってもよい。安全な移動端末は、特に、携帯電話、スマートフォン、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等でもよい。

【００２９】

上記の好適な改良は、本発明の第１の態様の範囲内（すなわち、処理端末において処理を実行するための方法の範囲内）で、第２の態様の範囲内（すなわち、この目的のために構成された移動端末の範囲内）で、そして、第３の態様の範囲内（すなわち、それに応じて構成された処理端末の範囲内）で、好適に実装されることができる。

【図面の簡単な説明】

【００３０】

更なる特徴、利点および本発明の目的は、複数の例示的実施形態および別の実施例の以下の詳細な説明から現れる。以下の図面を参照する。

【図１】トランザクション・システムの一部としての移動端末および処理端末の好ましい実施例の概略図。

【図２】本発明による処理方法の好ましい実施例の概略図。

【００３１】

図１は、（特に、現金を引き出すために）処理を実行するための現金自動預払機の形態の処理端末４０および携帯電話の形態の移動端末２０の概略図を示す。移動端末２０および処理端末４０は、特に、処理端末４０に接続されるバックグラウンド・システム８０も含むトランザクション・システム１０の一部である。バックグラウンド・システム８０は、バックグラウンド・システム８０に接続される、多数の処理端末（例えば処理端末４０）によって、アクセスされることができる多数のデータ項目を安全に保存する。

【００３２】

携帯電話の形態の移動端末２０は、ユーザ入力のための入力装置またはキーパッド２２と、情報を表示するディスプレイまたは表示装置２４と、を備えている。キーパッド２２およびディスプレイ２４は、タッチスクリーンの形態であってもよい。移動端末２０は、処理端末４０との安全なＮＦＣ通信経路を形成するように好ましくは構成された通信モジュール２６も備えることができる。移動端末２０が携帯電話となっている、図１に示す好ましい場合では、移動端末２０は、好ましくは移動無線モジュール２８（例えば、移動無線ネットワークを介した通信のための、ＳＩＭカード）も備えることもできる。

【００３３】
携帯電話の形態の移動端末２０は、例えば、マイクロコントローラなどの、移動端末２０の様々な構成部品を適切に制御するように構成される、プロセッサユニット３０を備えることもできる。明確化のために、プロセッサユニット３０の構造が、図１において移動端末２０の外側に、もう一度詳細に図示されている。
【００３４】
通常の、安全でないランタイム環境ＮＺ（「ノルマル・ゾーン」）およびＡＲＭ（商標）ＴｒｕｓｔＺｏｎｅ（商標）と称する形態の安全なランタイム環境ＴＺ（「ＴｒｕｓｔＺｏｎｅ」）は、プロセッサユニット３０に実装される。ＡＲＭ（商標）ＴｒｕｓｔＺｏｎｅ（商標）は、会社ＡＲＭ（商標）により開発された、「安全な」信頼された領域と、一般に信頼できない「通常の」領域と、を提供するシステムアーキテクチャである。この場合、プロセッサユニットが信頼された領域において、または、信頼できない領域において、作動されるかどうかは、監視される。信頼された領域と信頼できない領域の間での切り替えも、監視される。
【００３５】
ここで記載されている好ましい実施例において、安全なオペレーティングシステム３３（安全なＯＳ）（好ましくは従来技術から公知のＭｏｂｉＣｏｒｅ（商標）オペレーティングシステム）は、ＴｒｕｓｔＺｏｎｅ　ＴＺで動作する。対照的に、通常のランタイム環境ＮＺは、従来の携帯電話オペレーティングシステム３２を含んでいる。移動端末２０がスマートフォンである場合、通常のランタイム環境ＮＺに実装されるオペレーティングシステム３２は、広い範囲の機能を有するいわゆる「リッチＯＳ」である。移動端末２０のこの種のオペレーティングシステムは、例えば、Ａｎｄｒｏｉｄ、アップルｉＯＳ、Ｗｉｎｄｏｗｓ（商標）フォン等でもよい。
【００３６】
ＴｒｕｓｔＺｏｎｅ　ＴＺは、移動端末２０を用いて、セキュリティが重要なアプリケーションおよびサービスを実行するために用いる。この場合、アプリケーションは、例えばオペレーティングシステムと離れた機能性（例えば、銀行取引又は決裁処理のための処理ルーチン）を意味するものとして理解される。サービスは、オペレーティングシステム（例えば、キーパッド２２、若しくは移動端末２０のディスプレイ２４のドライバ、又は暗号化の機能性）に近い機能性を意味するものとして理解される。
【００３７】
この場合、安全なランタイム環境ＴＺは、通常のランタイム環境ＮＺから分離されて、セキュリティが重要な方法をカプセル化する。これにより、承認されていない第三者による攻撃から、効果的に保護することができる。ＴｒｕｓｔＺｏｎｅ　ＴＺ内部で動作しているセキュリティが重要なアプリケーションは、トラストレッツ（Ｔｒｕｓｔｌｅｔｓ）と呼ばれる。この場合、図１には、例証としてトラストレッツ３６（「ＡＴＭ－ＴＲ」）を描写する。これと対照的に、従来のアプリケーションは、通常のランタイム環境ＮＺで動作する。この場合、図１には、例証としてアプリケーション３７（「ＡＰＰ１」）が示される。信頼できない領域ＮＺ（例えばアプリケーション３７（「ＡＰＰ１」））からのアプリケーションおよびサービスは、信頼された領域ＴＺ（例えばトラストレッツ３６（「ＡＴＭ－ＴＲ」））のアプリケーションおよびサービスにアクセスしない。
【００３８】
オペレーティングシステムに近いサービスとして、キーパッド・ドライバ３４および通信モジュール・ドライバ３５が、ＴｒｕｓｔＺｏｎｅ　ＴＺに、好ましくは実装される。キーパッド・ドライバ３４は、移動端末２０のキーパッド２２を介して、移動端末２０のプロセッサユニット３０の安全なランタイム環境ＴＺに、安全に入力を転送するように構成される。移動端末２０のキーパッド２２がプロセッサユニット３０の信頼されたランタイム環境ＴＺに安全に接続されるため、キーパッド２２と移動端末２０のプロセッサユニット３０との間の通信経路（潜在的な安全ギャップである）が不正操作するための攻撃域として除外されることが、これによって確実になる。通信モジュール・ドライバ３５は、

通信モジュール２６を介して安全にプロセッサユニット３０により提供されるデータを処理端末４０に発信するように構成される。通信モジュール２６がプロセッサユニット３０の信頼されたランタイム環境ＴＺに安全に接続されるため、プロセッサユニット３０と移動端末２０の通信モジュール２６との間の通信経路も不正操作するための攻撃域として除外されることが、これによって確実になる。

【００３９】

移動端末の利用可能なディスプレイ及びこれらのディスプレイを制御する構成部品の数のために、信頼された領域ＴＺのディスプレイドライバの実装は、一般に、キーパッド・ドライバ（例えば、キーパッド・ドライバ３４）の実装よりも、いっそう複雑である。それにもかかわらず、ディスプレイドライバ（不図示）は、キーパッド・ドライバ３４および通信モジュール・ドライバ３５に加えてＴｒｕｓｔＺｏｎｅ　ＴＺに実装されることもできる。この場合、ディスプレイドライバは、プロセッサユニット３０により提供されるデータを安全に表示２４に発信して、ディスプレイに前記データを表示させるように構成される。これにより、ディスプレイ２４がプロセッサユニット３０の信頼されたランタイム環境TZに安全に接続されるため、プロセッサユニット３０と移動端末２０のディスプレイ２４との間の通信経路が、不正操作するための攻撃域としても除外される。

【００４０】

すでに上述したように、移動端末２０は、好ましくは、通信モジュール２６を用いたエア・インタフェースを介して、ＮＦＣ標準による処理端末４０と通信できる。このために、処理端末４０は、ＮＦＣ標準による通信に適した、対応する通信モジュール４６も備えている。

【００４１】

好ましい実施例において、処理端末４０（従来の現金自動預払機の形態であってもよい）は、データの入力および顧客による指示のためのキーパッド４２（例えば、ＰＩＮパッドの形態）と、例えば、顧客のための情報および選択オプションを示すためのディスプレイ４４と、支払いカード６０を処理端末４０に挿入するための挿入軸４７と、を備える。周知の方法で、読取機４８の形態である処理端末４０の構成部品は、挿入軸４７に挿入される支払いカード６０からデータを読み込む。データは、好ましくは、支払いカード６０の磁気帯に保存されている。処理端末４０は、顧客に選択された処理が処理端末４０によって許可される場合に、顧客によって希望された額の現金を支払うために用いることができる現金支払部４９も備える。図１に示される処理端末４０は、本発明の好ましい一実施例によるＰＩＮパッドの形態でキーパッド４２を備えているものの、処理端末４０は原則として従来の方法でも動作することもできるため、キーパッド４２は省略されるか、又はディスプレイ４４とともに組み合わされてタッチスクリーンを形成することが同様に考えられる。

【００４２】

処理端末４０の異なる構成部品を最適に制御するために、処理端末４０は、例えば、プロセッサユニットでもよい電子制御ユニット５０も備える。処理端末４０の制御ユニット５０は、好ましくは、その通信モジュール４６及びバックグラウンド・システム８０と通信する。通信は、処理方法の好ましい実施例（図２を参照して後述される）は、移動端末２０、処理端末４０、及び、可能性のあるバックグラウンド・システム８０によって実行されることができるような手法による。

【００４３】

図２は、移動端末２０及び処理端末４０、又は、バックグラウンド・システム８０によって実行される個々のステップを示す。バックグラウンド・システム８０は、処理（特に、現金の支払い方法）を実行する方法の好ましい実施例では、処理端末に接続される。

【００４４】

第１のステップＳ１では、好ましくは、顧客が支払いカード６０を処理端末４０の挿入軸４７に挿入するという事実によって、かつ、顧客を一意に識別するための少なくとも１つの識別データ要素（例えば、支払いカードの磁気帯に保存されている）が処理端末４０

の読取機４８によって読み取られるという事実によって、顧客は処理端末４０に対して識別される。この場合、支払いカード６０の磁気帯に保存される顧客の主要口座番号（ＰＡＮ）は、好ましくは処理端末４０の読取機４８によって読み込まれて、バックグラウンド・システム８０に転送される。読み込まれた識別データ要素に関連付けられ、かつ、好ましくは少なくともＰＩＮ及び個別の電子キーＫ＊を備えるデータレコードが、その後、バックグラウンド・システム８０において決定される。

【００４５】

図２のステップＳ２では、バックグラウンド・システム８０に保存されるキーＫ＊と、移動端末２０のプロセッサユニット３０の安全なランタイム環境ＴＺに保存されるキーＫと、に基づいて、移動端末２０と処理端末４０の間で、好ましくはチャレンジレスポンス方式の認証が実行される。当業者に知られているように、処理端末４０に対して移動端末２０を認証するために、処理端末４０は、例えば、乱数を移動端末２０に発信できる。乱数は、次に、安全なランタイム環境ＴＺに保存されるキーＫを用いた同意された暗号化アルゴリズムに従って、移動端末２０によって暗号化される。そして、この暗号化の結果は再び処理端末４０に発信される。手順は、処理端末４０、および／または、処理端末に接続しているバックグラウンド・システム８０において、同様である。すなわち、処理端末４０によって移動端末２０に送信された乱数は、バックグラウンド・システム８０に保存されたキーＫを用いて暗号化され、暗号化の結果が移動端末２０によって送信される暗号化された乱数と同一かどうか決定するために、チェックが行われる。これが事実ならば、処理端末４０は、移動端末２０に保存されたキーＫがバックグラウンド・システム８０に保存されるキーＫと同一であり、従って移動端末２０が真正である、と推測できる。当業者に知られているように、処理端末４０は、対応する手法で、移動端末２０に対して認証されることができる。すなわち、移動端末２０が乱数を処理端末４０に送信し、この乱数が移動端末２０及び処理端末４０の両方によって暗号化される、という理由による。

【００４６】

当業者は、移動端末２０において、そして、処理端末に接続している処理端末４０、又は、バックグラウンドでシステム８０において、キーＫ及びキーＫ＊を、安全に保存されることができる方法に関する、多数の方法に気づいている。例えば、移動端末２０を生産し、かつ／または、個人用にするときに、これを実施できる。移動端末がすでにフィールドにある場合、例えば、フィールドにあるＳＩＭカードを個人用にするときに用いられるように、安全なＯＴＡ方法がさらに、または、代わりに用いられることが可能である。

【００４７】

処理端末４０および移動端末２０が図２のステップＳ２において、相互に認証されたあと、ＰＩＮを図２のステップＳ３の移動端末２０に入力するために、処理端末４０はリクエスト（要請）を送信する。次に、移動端末２０のキーパッド２２は、好ましくは、ＰＩＮ入力のために使用可能にされる。そして、移動端末２０の安全なキーパッド２２を使用してＰＩＮを入力することを顧客に促すために、対応する表示が移動端末２０のディスプレイ２４に表示される。顧客が移動端末２０の安全なキーパッド２２を使用してＰＩＮを入力したあと、このＰＩＮは、処理端末４０で同意された暗号化アルゴリズムを用いて図２のステップＳ５において暗号化され、暗号化された形態での処理端末４０に発信される（図２のステップＳ５）。

【００４８】

処理を実行するための本発明による方法の好ましい実施例において、図２に図示したように、ＰＩＮの暗号化および解読は、特に、キーＫおよびＫ＊に同様に基づく。しかしながら、当業者は、キーＫ及びＫ＊以外の秘密キーを、認証のため、かつ、通信経路を介して移動端末２０と処理端末４０の間に送信されるデータの暗号化のために、使用されることができることを理解できるであろう。

【００４９】

安全性を増加させるために、処理を実行するための本発明による方法の好ましい実施例において、図２に図示したように、各処理のためのそれぞれの新規なセッションキーを作

り出すために、キーＫおよびＫ＊が、それぞれのマスターキーとして使われる。それぞれのセッションキーは、例えば、移動端末２０および処理端末４０が更なる乱数を交換し、この乱数が、移動端末２０に保存されるキーＫ、および、同意された暗号化アルゴリズムに従って処理端末４０（または処理端末に接続しているバックグラウンド・システム８０）に保存されるキーＫ＊によって、それぞれ暗号化されている、ために発生できる。移動端末２０のキーパッド２２を使用している顧客によるＰＩＮ入力は、図２のステップＳ５において、この手法によって、移動端末２０で作り出されるセッションキーを用いて暗号化されて、処理端末４０に発信される（図２のステップＳ６）。

【００５０】

図２のステップＳ７において、移動端末２０のキーパッド２２を使用している顧客により入力されて、安全な通信経路を介して処理端末４０に発信されるＰＩＮが、処理端末４０および／または、処理端末に接続されるバックグラウンド・システム８０において、識別データ要素と併せて保存されるＰＩＮと同一であると決定されたあと、顧客が所望する処理（例えば、現金の引き出し）が、処理端末４０によって、及び／又は、処理端末に接続されるバックグラウンド・システム８０によって可能にされる。この場合、ＰＩＮがバックグラウンド・システム８０においてどのように保存されているかによって、処理端末４０および／または処理端末に直接に接続されているバックグラウンド・システム８０に依存して、移動端末２０によって送信された暗号化されたＰＩＮを用いて、または、移動端末２０によって送信された暗号化されたＰＩＮを解読した結果のＰＩＮを用いて、処理端末４０および／または処理端末に直接に接続されているバックグラウンド・システム８０によって、チェックが実行されることができる。換言すると、移動端末２０によって送信された暗号化されたＰＩＮが、図２のステップＳ７の前にキーＫ＊を用いて解読される実施例が考えられる。

【００５１】

当業者が認識するように、処理端末４０が、異なる処理および／または変形例（例えば顧客が引き出したい金額の選択）の選択を許容する場合、顧客がこの選択をする更なるステップ（図２に例示されない）の用意がされる。この選択は、好ましくは、ステップＳ７の後に顧客によってなされ、すなわち、ＰＩＮが検査された後になされるが、しかし、より早い時点でなされることもできる。顧客によって所望される処理の選択は、キーパッド４２または処理端末４０のディスプレイ４４（タッチスクリーンの形態である）を用いて、および／または、キーパッド２２または移動端末２０のディスプレイ２４（タッチスクリーンの形態である）を用いて、なされることができる。

【００５２】

図１に示すように、かつ、上述したように、アプリケーション（またはＭｏｂｉｃＣｏｒｅオペレーティングシステムの場合にはトラストレッツ）３６（「ＡＴＭ－ＴＲ」）は、移動端末２０の安全なランタイム環境で動作して、特に移動端末２０によって、図２に関連して上述した方法ステップを実行するか、または、促進するように構成される。例えば、アプリケーション３６（「ＡＴＭ－ＴＲ」）は、図２のステップＳ２において、処理端末を用いて相互チャレンジレスポンス方式の認証と、移動端末２４のキーパッド２２を用いてＰＩＮ入力と、を実行又は促進するように構成されている。

【００５３】

図１及び図２に示す好ましい実施例に関して、顧客が支払いカード６０を処理端末４０の挿入軸４７に挿入し、このカードが処理端末４０の読取機４８によって読み込まれるという事実によって、顧客が第一に識別される、ということを上述したが、顧客が、非接触式の手法、すなわち、支払いカード６０と処理端末４０との間のエア・インタフェースによる通信によって、支払いカード６０を用いて、代替的に、又は、追加的に、識別されることができる、という実施例も同様に考えられる。

【００５４】

顧客を識別するために用いられる支払いカード６０を完全になしで済まし、その機能が移動端末２０又は移動端末の構成部品に一体化される、という本発明の実施例も考えられ

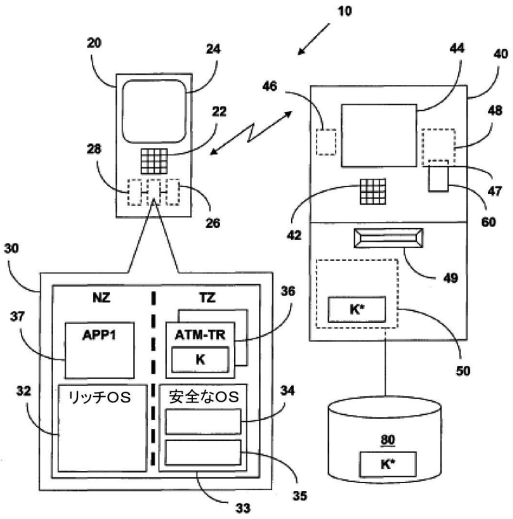
る。例えば、移動端末２０に保存される識別データ要素を非接触式で読み込むことによって、顧客が識別されることさえもできた。ここで、適切な考えられる識別データ要素は、以下の通りである：通信モジュール２６の、若しくは、移動端末２０のプロセッサユニット３３の固有のチップ番号、又は、通信モジュール２６の、若しくは、プロセッサユニット３３のメモリに保存される固有のシリアル番号、例えば、ＥＰＣ（「Ｅｌｅｃｔｒｏｎｉｃ　Ｐｒｏｄｕｃｔ　Ｃｏｄｅ」）、または、ＵＩＩ（「Ｕｎｉｑｕｅ　Ｉｔｅｍ　Ｉｄｅｎｔｉｆｉｅｒ」）など。仮に、移動端末２２が、移動無線ネットワークによる通信用に設計され、対応する安全な移動無線モジュール２８を備えていれば（例えば、ＳＩＭ等の形態）、識別データ要素は、移動無線モジュール２８のＩＭＳＩ（「Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｍｏｂｉｌｅ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ」）または移動端末２０に割り当てられる固有の電話番号でもよい。

【符号の説明】

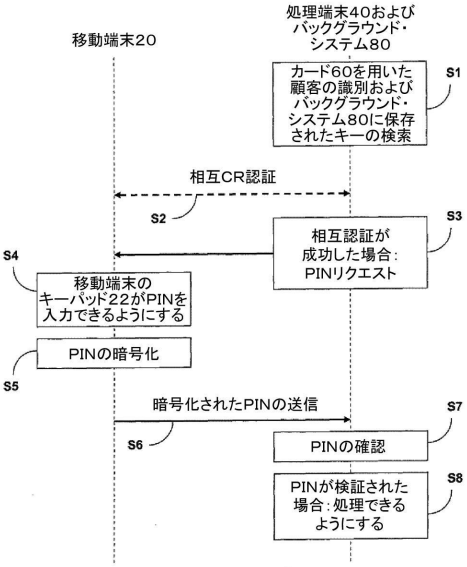
【００５５】

１０	トランザクション・システム
２０	移動端末
２２	移動端末のキーパッド
２４	移動端末のディスプレイ
２６	移動端末の通信モジュール
２８	移動無線モジュール
３０	プロセッサユニット
ＮＺ	安全でないランタイム環境（Ｎｏｒｍａ１Ｚｏｎｅ）
ＴＺ	安全なランタイム環境（ＴｒｕｓｔＺｏｎｅ）
３２	安全でないオペレーティングシステム（リッチＯＳ）
３３	安全なオペレーティングシステム（安全なＯＳ）
３４	キーパッド・ドライバ
３５	通信モジュール・ドライバ
３６	処理アプリケーション（ＡＴＭ－ＡＰＰ）
３７	アプリケーション
４０	処理端末
４２	処理端末のキーパッド
４４	処理端末のディスプレイ
４６	処理端末の通信モジュール
４７	挿入軸
４８	読取機
４９	現金支払部
５０	制御ユニット
６０	支払いカード
８０	バックグラウンド・システム
Ｋ、Ｋ＊	電子キー

【図１】


10
20
24
22
28
26
30
NZ
TZ
APP1
ATM-TR
K
リッチOS
安全なOS
32
33
34
35
36
37
40
44
46
48
47
60
42
49
K*
50
80
K*

【図２】


移動端末20
処理端末40および
バックグラウンド・
システム80
カード60を用いた
顧客の識別および
バックグラウンド・
システム80に保存
されたキーの検索
S1
相互CR認証
S2
S3
相互認証が
成功した場合：
PINリクエスト
S4
移動端末の
キーパッド22がPINを
入力できるようにする
PINの暗号化
S5
暗号化されたPINの送信
S6
S7
PINの確認
PINが検証された
場合：処理できる
ようにする
S8

フロントページの続き

(56)参考文献 特開２００７－１８８２１６（ＪＰ，Ａ）
特開２０１０－６２８２３（ＪＰ，Ａ）
特開２００４－１９９６９３（ＪＰ，Ａ）
特開２００６－１７９０１１（ＪＰ，Ａ）
国際公開第０１／１７２９６（WO，Ａ１）
米国特許出願公開第２００９／０２５４９８６（ＵＳ，Ａ１）
特表２０１０－５３２１０７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
G06F21/30-21/46