(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2019-503003
(P2019-503003A)
(43)公表日　平成31年1月31日(2019.1.31)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/32	***(2013.01)***	G06F	21/32		5B047
G06T 1/00	***(2006.01)***	G06T	1/00	400G	
G06F 1/00	***(2006.01)***	G06F	1/00	370E	

審査請求 未請求　予備審査請求 未請求　（全 16 頁）

(21)出願番号　特願2018-533069 (P2018-533069)
(86)(22)出願日　平成28年12月23日 (2016.12.23)
(85)翻訳文提出日　平成30年7月25日 (2018.7.25)
(86)国際出願番号　PCT/EP2016/082566
(87)国際公開番号　WO2017/109176
(87)国際公開日　平成29年6月29日 (2017.6.29)
(31)優先権主張番号　1522870.3
(32)優先日　平成27年12月24日 (2015.12.24)
(33)優先権主張国　英国 (GB)

(71)出願人　517124778
ズワイプ　アクティーゼルスカブ
ノルウェー王国　０１５１　オスロ　ロードュースガータ　２４
(74)代理人　110000556
特許業務法人　有古特許事務所
(72)発明者　ラルセン，　ステフェン
ノルウェー王国　１１６６　オスロ　ミッドターセン　４８アー

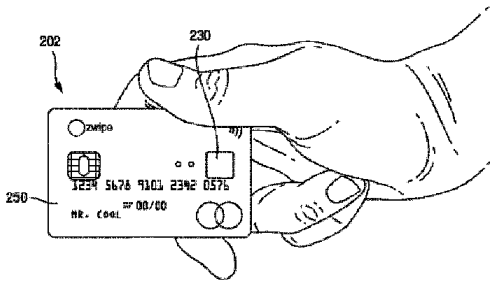
Fターム(参考)　5B047 AA25　BB04　CA02　CA23　CB22

最終頁に続く

(54)【発明の名称】バイオメトリックデバイス

(57)【要約】
スマートカード１０２、２０２を用いる方法は、スマートカード１０２、２３０内に内蔵されたバイオメトリックセンサ１３０、２３０の可能な不正使用を検知し、可能な不正使用が停止した後にスマートカード１０２、２０２のその後の使用を制限するが防止しない工程を含む。この制限は、ベアラが通常行うことが許可されるアクションをベアラが行うことを許可しない工程の１つ以上と、ベアラが１つ以上のアクションを行うことを許可する前に通常要求されるよりも高い認証信頼スコアを要求する工程と、そして、ベアラが１つ以上のアクションを行うことを許可する前に、ベアラが第２の認証工程を通過することを要求する工程とを含む。
【選択図】図４

Fig. 4



【特許請求の範囲】
【請求項１】
内蔵されたバイオメトリックセンサを備えたポータブルバイオメトリック認証デバイスの可能な不正使用を検知する工程と、
可能な不正使用が停止した後のデバイスのその後の使用を制限するが防止しない工程とを含む、方法。
【請求項２】
前記可能な不正使用が、前記デバイスそれ自体によって検知される、請求項１に記載の方法。
【請求項３】
前記可能な不正使用の検知が、バイオメトリックセンサを用いて認証を得るための反復される不成功の試行を検知する工程を含む、請求項１または２に記載の方法。
【請求項４】
前記可能な不正使用が、第１のアクションを行うための認証を得るための第１回目の反復される不成功の試行後に検知され、そして、前記可能な不正使用が、第２のアクションを行うための認証を得るための第２回目の異なる回数の反復される不成功の試行後に検知される、請求項３に記載の方法。
【請求項５】
前記可能な不正使用の検知に応答して、可能な不正を示すアラートを送信する工程をさらに含む、請求項１から４のいずれか一項に記載の方法。
【請求項６】
前記制限が、前記ベアラが第１のアクションを行うことを許可するが、前記ベアラが通常は許可される第２のアクションを行うことを許可しない工程を含む、請求項１から５のいずれか一項に記載の方法。
【請求項７】
前記制限が、前記ベアラが１つ以上のアクションを行うことを許可する前に、前記ベアラに通常要求されるよりも高い認証信頼スコアを要求する工程を含む、請求項１から６のいずれか一項に記載の方法。
【請求項８】
前記制限が、前記ベアラが１つ以上のアクションを行うことを許可する前に、前記ベアラに第２の認証工程を通過するよう要求する工程を含む、請求項１から７のいずれか一項に記載の方法。
【請求項９】
前記制限が、前記バイオメトリックセンサを用いて前記ベアラの認証を防止する工程を含む、請求項１から８のいずれか一項に記載の方法。
【請求項１０】
前記制限が、権限のある人または法人によって除去されるまで残っている、請求項１から９のいずれか一項に記載の方法。
【請求項１１】
前記ベアラが、第２の認証を通過した後に前記制限を除去するよう認証される、請求項１０に記載の方法。
【請求項１２】
前記バイオメトリックセンサが指紋センサである、請求項１から１１のいずれか一項に記載の方法。
【請求項１３】
前記ポータブルバイオメトリック認証デバイスがスマートカードである、請求項１から１２のいずれか一項に記載の方法。
【請求項１４】
内蔵されたバイオメトリックセンサを備えたポータブルバイオメトリック認証デバイスであって、前記バイオメトリックセンサの可能な不正使用を検知し、制限動作モードに入

るように構成されているポータブルバイオメトリック認証デバイス。
【請求項１５】
前記ベアラが認証されて前記制限動作モードで動作しているときに、前記デバイスが、前記スマートカードが制限動作モードで動作しているという表示を含む前記ベアラの認証を示すメッセージを送信するように構成されている、請求項１４に記載のデバイス。
【請求項１６】
前記ベアラが認証されて前記制限動作モードで動作しているときに、前記デバイスが、認証されたベアラに通常許可されるアクションのサブセットのみを許可するメッセージを送信するように構成されている、請求項１５に記載のデバイス。
【請求項１７】
前記ポータブルバイオメトリック認証デバイスが、スマートカードである、請求項１４から１６のいずれか一項に記載のデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、内蔵バイオメトリックセンサを備えたスマートカードと、このようなカードを用いて、そのベアラを認証する方法とに関する。
【背景技術】
【０００２】
クレジットカードやデビットカードなどの電子カードの使用が増えて、支払いや現金引出しが行われるようになればなるほど、不正のリスクも増える。例えば、ユーザのカードが盗まれた場合、権限のない人が、ユーザの銀行口座またはクレジット・プロバイダから権限のない電子決済や現金引出しを行うことができる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
チップ・アンド・ピン保護の使用は、２要素認証、すなわち、物理的なカードとユーザのＰＩＮの知識との所有を通して、この種の不正のリスクを減らす。しかし、この種の認証は時には不便であり得る。さらに、非接触型ペイメント技術がますます普及しており、しばしば、ＰＩＮの入力が要求されない。すなわち、権限のないユーザが、非接触型ペイメントを介して、盗難カードを用いて不正取引をなお行い得る。
【０００４】
提案されている１つの解決策は、カードに内蔵された指紋センサなどのバイオメトリックセンサを備えるスマートカードの使用である。権限のあるユーザは、初めに実際のカード上に自分の指紋を登録し、次いで、任意の支払いまたは引出しを認証するために自分の指または親指を指紋センサ上に置くよう要求される。カード内の指紋照合アルゴリズムが一致を検知すると、カードは、スマートカードセキュアエレメントがＰＯＳまたはＡＴＭ端末と通信することを許可し、金融取引が行われることを許可する。一致がないと取引はない。
【０００５】
このようなバイオメトリックスマートカードの有用性を改善することが、セキュリティの改善を損なうことなく望まれている。
【課題を解決するための手段】
【０００６】
したがって、本発明は、第一の態様では、デバイス内に内蔵されたバイオメトリックセンサを用いて、ポータブルバイオメトリック認証デバイスのベアラの身元を認証する工程と、認証の信頼スコアを決定し、ベアラが認証されて信頼スコアが所定の閾値を下回る場合に第１のアクションを許可し、そして、ベアラが認証されて信頼スコアが所定の閾値を上回る場合に第２のアクションを許可する工程とを含む方法を提供する。
【０００７】

この方法は、指紋、拇印、または他のバイオメトリックスキャンが完全に一致しないときでも、デバイスの使用を許可する。これは、例えば、指紋の場合、ベアラが指を切ったり焼いたりするとき、指紋の変化がデバイスに以前に記録された指紋と比較して損害をもたらす場合に起こり得る。

【０００８】

本明細書で用いられるように、「ポータブル」という用語は、例えば、壁またはより大きなデバイスに取り付けられたものなどの固定スキャナと区別するために理解されるべきである。種々の実施形態では、ポータブルデバイスは、１００グラム未満の質量および/または１００立方センチメートル未満の体積を有していてもよい。デバイスは、カード、フォブなどの形態であってもよい。

【０００９】

大部分のバイオメトリック検証アルゴリズムは、バイオメトリックスキャンを認証するときに、単に、はい／いいえ出力を提供するだけでなく、この名前では必ずしも知られていないが、何らかの形式の「信頼スコア」も提供し、これは一致の精度における信頼度を示すものと理解されよう。

【００１０】

典型的には、信頼スコアは、認証後にのみ一致の信頼度を示す。すなわち、指紋が一致するとみなされない場合、信頼スコアはないかも知れない。しばしば、信頼スコアは、０または０％（ほとんど一致しない）から１または１００％（完全に一致）までの範囲になる（またはその逆）。しかし、信頼スコアは、アルゴリズムに応じて、一致と決定するために用いられるそれ自体であってもよい。例えば、閾値の信頼スコアを上回ると、一致と決定される。

【００１１】

好ましくは、ベアラが認証されて信頼スコアが閾値を上回る場合、第２のアクションセットが許可される。第２のアクションセットは、好ましくは、第１のアクションと、ベアラが認証されて信頼スコアが所定の閾値を下回る場合に許可されない少なくとも１つのアクションとを含む。

【００１２】

いくつかの実施形態では、ベアラが認証されて信頼スコアが閾値を下回る場合、第１のアクションセットが許可されてもよい。第２のアクションセットは、好ましくは、第１のアクションセットにない１つ以上のアクションを含み、そして、好ましくは、第１のアクションセットのすべてを含む。

【００１３】

第１のアクションまたはアクションセットは、好ましくは、不正に行われることになると、第２のアクションまたはアクションセットよりも害が少なくなる。すなわち、バイオメトリックスキャンに影響を及ぼす身体の損傷などの場合に、より低いセキュリティのアクションがベアラに許可されて、類似のバイオメトリックスキャンを有する権限のない人により発生し得るデバイスの不正使用を最小限にするために、より高いセキュリティ機能へのアクセスを制限する一方、ユーザのデバイスは完全には無効にならない。

【００１４】

いくつかの実施形態では、１つ以上のアクションは取引であってもよい。例えば、１つ以上のアクションは、支払い、現金自動預払機からなどの現金引出、銀行振込、または任意の他の金融取引を含む金融取引であってもよい。

【００１５】

一実施形態では、第１のアクションは、口座の残高照会、またはカードの再発行請求などの非金融アクションであってもよく、第２のアクションは、支払い、現金引出、または銀行振込などの金融アクションであってもよい。上記のように、これは、デバイスの何らかの使用をなお許可する一方で、不正な金融取引が行われるというリスクを減らす。

【００１６】

一実施形態では、第１および第２のアクションは金融アクションであってもよい。第１

の金融取引は、所定の第１の金融上限を超えない金融取引であってもよい。次いで、第２の金融取引は、所定の第２のより高い金融上限を超えないか、または金融上限のない金融取引であってもよい。

【００１７】

第１の金融取引は、第１の金融アクションセットを含み、第２の金融取引は、第１の金融アクションセットにない金融アクションを含む第２の金融アクションセットを含んでもよい。

【００１８】

代替の実施形態では、アクションは、１つ以上のセキュアエリアにアクセスする工程を含んでもよい。本明細書では、セキュアエリアとは、アクセスカードまたは他のアクセス認証を要求するエリアのような、一般公衆が容易にアクセスできないエリアを指す。

【００１９】

好ましくは、第１のアクションは、１つ以上の低セキュリティ・セキュアエリアにアクセスする工程を含み、第２のアクションは、１つ以上の低セキュリティ・セキュアエリアと１つ以上の高セキュリティ・セキュアエリアとにアクセスする工程を含む。

【００２０】

例えば、低セキュリティエリアは、１つ以上のパーキングエリア、ロビー、休憩室などへのアクセスを許可するなど、安全なサイト内の共有エリアを含み得る一方、高セキュリティエリアは、より制限されたアクセス、例えば、サイトのユーザのサブセットのみがアクセスできるエリア、例えば、機密情報を有するエリアや高価値商品などを保存するエリアを含み得る。

【００２１】

いくつかの実施形態では、本方法は、ベアラが認証されて信頼スコアが所定の閾値を下回るときと、および任意に、１つ以上の他の基準が満たされるときとに、アラートを送信する工程を含んでもよい。このような基準は、例えば、高レベルの認証が行われた後、または所定数の第１のアクションが行われた後の数日を含んでもよい。アラートは、デバイス発行者および/またはデバイスのベアラに送信されてもよい。これは、デバイス発行者が、例えば、使用が疑わしいかどうかを監視するために、デバイスがこのモードで用いられていることを知っているために望ましいことであり得る。また、知っていない場合、劣化モードでデバイスを用いていることをベアラに知らせてもよい。これは、例えば、新しいバイオメトリック識別子を登録することによって、状況を解決するよう促し得る。

【００２２】

いくつかの実施形態では、複数の閾値が用いられてもよく、信頼スコアがより高い閾値を超える際に追加のアクションが許可される。

【００２３】

好ましい実施形態では、バイオメトリックセンサは指紋センサである。しかし、ＥＫＧ読み取りなどのような他のバイオメトリック識別子が用いられてもよいことは理解されよう。

【００２４】

本方法は、反復される不成功の認証試行を検知する工程を含んでもよい。これは、デバイスそれ自体によって、または別のコンピュータシステムによって検知されてもよい。ベアラの指紋がデバイスに保存された参照指紋と一致しないため、不成功の認可試行は失敗し得るが、他の検知手段が採用されてもよい。

【００２５】

本方法は、反復される不成功の認証試行の検知に応答して、可能な不正を示すアラートを送信する工程をさらに含んでもよい。このアラートは、所定回数の試行の後、および/または、ある他の基準が満たされたことに応答して送信されてもよい。例えば、デバイスが第２のアクションを許可するために用いられているというアラートを送信する前には、第１のアクションを許可するために用いられているときよりも必要な試行回数は少なくて済み得る。

【００２６】
本方法は、反復される不成功の認証試行の検知に応答して、および/または、可能な不正使用を検知して、ベアラの第１および/または第２のアクションを制限する工程をさらに含んでもよい。例えば、ベアラは、高い信頼スコアが検知されたとしても、第２のアクションを行うことを許可されない可能性がある。あるいは、またはさらに、ベアラは、低い信頼スコアでアクションを取ることを許可されない可能性がある。
【００２７】
いくつかの実施形態では、ベアラは、第２の認証工程を通過するなど、第１および/または第２のアクションを行うために追加の基準を満たすよう要求されてもよい。第２の認証工程は、例えば、ＰＩＮを入力する工程を含んでもよい。
【００２８】
制限は、権限のある人または法人によって除去されるまで、残り得る。これは、例えば、ベアラまたはデバイス発行者によって認証された任意の人であり得る。
【００２９】
いくつかの実施形態では、ベアラは、第２の認証を通過した後にのみ制限を除去するよう認証されてもよい。例えば、ベアラは、郵便、電子メール、テキストなどによって、制限を除去するために端末（例えば、銀行端末）に入力され得る再活性化コードが送信されてもよい。あるいは、ベアラは、例えば、デジタルコントロールパネル（例えば、オンラインバンキングまたはセキュアコンピュータインターフェース）にログオンすることによって、パスワードを用いて制限を除去できてもよい。さらに別の実施形態では、ベアラは、その後、制限を除去し得る銀行窓口に写真付身分証明書を提示することなどによって、デバイス発行者に身分証明書を提示するよう要求されてもよい。
【００３０】
この制限された動作モードは、低い信頼スコアのため劣化動作モードと組み合わされてもよいが、別々に用いられてもよい。
【００３１】
したがって、本発明は、別の態様では、内蔵されたバイオメトリックセンサを備えたポータブルバイオメトリック認証デバイスの可能な不正使用を検知する工程と、可能な不正使用が停止した後に、デバイスのその後の使用を制限するが防止しない工程とを含む方法を提供してもよい。本方法は、任意に、上記方法に関連して記載の任意の１つ以上またはすべてのオプションの特徴を含んでもよい。
【００３２】
この方法によれば、バイオメトリックセンサに伴うリスクの一部は、可能な不正使用が検知されたときにデバイスの後の使用を制限することによって無効にし得るが、デバイスを完全に無効にすることはできない。したがって、システムがおそらく不正使用を検知した場合、この可能な不正使用が停止すると、デバイスはアクティブのままであるが機能性は低下する。もちろん、この劣化動作モードの有効性は、デバイスが盗まれたり、他に損なわれるときなど、実際の不正が認められる場合などに、従来の方法でデバイスを完全に無効にすることを妨げるものではない。
【００３３】
上記のように、可能な不正使用を検知する工程は、バイオメトリックセンサを用いて認証を得るための反復される不成功の認証試行を検知する工程を含んでもよい。これは、デバイスそれ自体または別のコンピュータシステムによって検知されてもよい。ベアラの指紋がデバイスに保存された参照指紋と一致しないため、不成功の認証試行は失敗し得るが、他の検知手段も採用してもよい。
【００３４】
本方法は、可能な不正の検知に応答して、反復される不成功の認証試行を検知する工程などによって、可能な不正を示すアラートを送信する工程をさらに含んでもよい。このアラートは、所定数の試行の後、および/または、ある他の基準が満たされることに応答して送信されてもよい。例えば、ベアラがあるアクションを行おうと試みているというアラ

ートを送信する前には、別のアクションよりも必要な試行回数は少なくて済み得る。
【００３５】
劣化動作モードでは、ベアラは、いったん認証されると、少なくとも１つのアクションをなお行い得る。すなわち、この動作モードでは、デバイスは完全には無効になっていない。制限には、ベアラが第１のアクションを行うことを許可されるが、通常は許可される第２のアクションを行うことは許可されないことが含まれてもよい。あるいは、またはさらに、認証には、１つ以上のアクションについては、通常必要とされるよりもより高い信頼スコアが必要とされてもよい。
【００３６】
制限には、第２の認証工程を通過する工程など、１つ以上のアクションを行うためにベアラが追加の基準を満たすよう要求されることが含まれてもよい。第２の認証工程は、例えば、ＰＩＮを入力する工程を含んでもよい。
【００３７】
制限は、権限のある人または法人によって除去されるまで残り得る。これは、例えば、デバイス発行者の権限のある人によって行い得る。あるいは、ベアラは、例えば、郵便、電子メール、テキストなどによって、制限を除去するために端末（例えば、銀行端末）に入力され得る再活性化コードが送信されてもよい。さらに、あるいは、ベアラは、非常に権限のある場合、例えば、デジタルコントロールパネル（例えば、オンラインバンキングまたはセキュアコンピュータインターフェース）を用いて、制限それ自体を除去できてもよい。
【００３８】
制限には、バイオメトリックセンサを無効にする工程、または他に、バイオメトリックセンサを用いてベアラの認証を防止する工程が含まれてもよい。したがって、デバイスは、署名、または、チップ・アンド・ピンのような他の手段によってのみ用いられ得る。
【００３９】
本発明はまた、スマートカードであり得る、この方法で用いるためのポータブルバイオメトリック認証デバイスを提供してもよい。したがって、ポータブルバイオメトリック認証デバイスは、内蔵されたバイオメトリックセンサを備えてもよく、バイオメトリックセンサの可能な不正使用を検知して制限動作モードに入るように構成される。デバイスは、上記方法の任意の態様を実施してもよい。
【００４０】
一実施形態では、ベアラが認証されて制限動作モードで動作しているときに、デバイスは、制限動作モードで動作しているという表示を含むベアラの認証を示すメッセージを送信してもよい。
【００４１】
他の実施形態では、ベアラが認証されて制限動作モードで動作しているときに、デバイスは、認証されたベアラに対して通常許可されるアクションのサブセットのみを許可するメッセージを送信してもよい。
【００４２】
第１の方法に戻ると、種々の実施形態では、認証は、デバイス上で（局所的に）行われてもよく、例えば、スキャンした指紋はデバイスを離れない。例えば、デバイスは、ベアラの身元を認証した後、ベアラが認証されたことを示すメッセージを送信してもよく、メッセージは、信頼スコアを含んでもよいか、または、信頼スコアを示してもよい（例えば、信頼スコアが所定の閾値を下回っている場合に第１のメッセージを送信し、そして、信頼スコアが所定の閾値を上回っている場合に第２の異なるメッセージを送信してもよい）。
【００４３】
さらなる態様では、本発明はまた、上記方法で用いるための、ポータブルバイオメトリック認証デバイスを提供してもよい。したがって、ポータブルバイオメトリック認証デバイスは、内蔵されたバイオメトリックセンサを備えてもよく、バイオメトリックセンサを

用いてデバイスのベアラの身元を認証し、認証の信頼スコアを決定し、そして、ベアラが認証されたかどうかを示し、認証の信頼スコアを示すメッセージを送信するように構成される。

【００４４】

デバイスは、好ましくは、ＲＦＩＤまたはＮＦＣ通信を用いるなど、無線通信が可能である。しかし、デバイスは、例えば、接触パッドなどを介する接触接続を備えていてもよい。種々の実施形態では、デバイスは、無線通信と接触通信との両方を可能にしてもよい。

【００４５】

例示的なデバイスとしては、アクセスカード、クレジットカード、デビットカード、プリペイドカード、ポイントカード、ＩＤカード、および暗号カードのうちの１つが挙げられる。

【００４６】

デバイスは、好ましくは、８５．４７ｍｍ～８５．７２ｍｍの幅と、５３．９２ｍｍ～５４．０３ｍｍの高さとを有するスマートカードであってもよい。スマートカードは、０．８４ｍｍ未満、好ましくは通常のスマートカードの厚さである約０．７６ｍｍ（例えば±０．０８ｍｍ）の厚さを有していてもよい。より一般的には、スマートカードは、スマートカードの仕様であるＩＳＯ７８１６に準拠していてもよい。

【００４７】

上記方法は、このポータブルバイオメトリック認証デバイスの任意の特徴のすべてのうちの任意の１つ以上を採用するデバイスを用いてもよいことが理解されよう。

【００４８】

さらに別の態様では、本発明は、また、内蔵バイオメトリックセンサを備えるポータブルバイオメトリック認証デバイスと通信するためのデバイスリーダーを備えるコンピュータシステムであって、デバイスのベアラの認証の信頼スコアの表示を受信するように構成され、ベアラが認証されて信頼スコアが所定の閾値を下回る場合に第１のアクションを許可し、そして、ベアラが認証されて信頼スコアが所定の閾値を上回る場合に第２のアクションを許可するように構成されているコンピュータシステムを提供してもよい。

【００４９】

コンピュータシステムは、上記の任意のおよび好ましい特徴のうちの任意の１つ以上またはすべてを行うように構成されていてもよい。

【００５０】

以下に、本発明の好ましい実施形態を、例示のみを意図して添付の図面を参照しながらより詳細に説明する。

【図面の簡単な説明】

【００５１】

【図１】従来のパッシブスマートカードの回路である。

【図２】指紋スキャナを備えるパッシブスマートカードの回路である。

【図３】指紋スキャナを備えるパッシブスマートカードのための外部ハウジングである。

【図４】指紋スキャナを備える積層パッシブスマートカードである。

【発明を実施するための形態】

【００５２】

図１は、典型的なパッシブスマートカード２の構造を示す。駆動中のカードリーダー４は、アンテナ６を介して信号を送信する。信号は、典型的には、ＮＸＰ　Ｓｅｍｉｃｏｎｄｕｃｔｏｒｓ社製のＭＩＦＡＲＥ（登録商標）とＤＥＳＦｉｒｅ（登録商標）システムとでは１３．５６ＭＨｚであるが、ＨＩＤ　Ｇｌｏｂａｌ　Ｃｏｒｐ．社製の低周波ＰＲＯＸ（登録商標）では１２５ｋＨｚであり得る。この信号は、同調コイルとコンデンサとを備えるスマートカード２のアンテナ８によって受信され、次いで、通信チップ１０に渡される。受信信号は、ブリッジ整流器１２によって整流され、そして、整流器１２の直流出力は、通信チップ１０からのメッセージングを制御する処理ユニット１４に提供される

。
【００５３】
処理ユニット１４からの制御信号出力は、アンテナ８を横切って接続された電界効果トランジスタ１６を制御する。トランジスタ１６をオンとオフとにスイッチすることによって、信号がスマートカード２によって送信され、リーダー４内の適当な制御回路１８によって復合され得る。このタイプのシグナリングは、後方散乱変調として知られており、リーダー４がそれ自体への戻りメッセージに駆動するために用いられるという事実によって特徴づけられる。
【００５４】
図２は、カードリーダー１０４と、図１に示す従来技術のパッシブスマートカード２のバリエーションであるパッシブスマートカード１０２との構造を示す。図２に示すスマートカード１０２は、指紋認証エンジン１２０を備えるように適合されている。
【００５５】
さらに、スマートカード１０２は、ＲＦ（無線周波数）信号を受信するためのアンテナ１０８と、アンテナ１０８によって給電されるパッシブ通信チップ１１０と、またアンテナ１０８によって給電されるパッシブ指紋認証エンジン１２０とを備える。
【００５６】
本明細書で用いられるように、「パッシブスマートカード」という用語は、通信チップ１１０が、例えば、カードリーダー１１８によって生成された励起場から収集されたエネルギーによってのみ給電されるスマートカード１０２を意味すると理解されるべきである。すなわち、パッシブスマートカード１０２は、リーダー１１８に依存して、ブロードキャストのための電力を供給する。パッシブスマートカード１０２は、通常バッテリを備えないが、バッテリは、回路（ただし、ブロードキャストのためではない）の補助部品に給電するために備えられてもよく、このようなデバイスは、しばしば「セミパッシブデバイス」と呼ばれる。
【００５７】
同様に、「パッシブ指紋／バイオメトリック認証エンジン」という用語は、励起場、例えば、カードリーダー１１８によって生成されたＲＦ励起場から収集されたエネルギーによってのみ給電される指紋／バイオメトリック認証エンジンを意味すると理解されるべきである。
【００５８】
アンテナ１０８は、誘導コイルと、カードリーダー１０４からＲＦ信号を受信するように調整されるコンデンサとを備える同調回路を備える。リーダー１０４によって生成された励起場に曝されると、アンテナ１０８に電圧が誘起される。
【００５９】
アンテナ１０８は、アンテナ１０８の各端に１つずつ、第１および第２の端部出力線１２２、１２４を備える。アンテナ１０８の出力線は、指紋認証エンジン１２０に接続され、指紋認証エンジン１２０に電力を供給する。この構成では、整流器１２６が設けられ、アンテナ１０８によって受信された交流電圧を整流する。整流された直流電圧は、平滑コンデンサを用いて平滑化され、指紋認証エンジン１２０に供給される。
【００６０】
指紋認証エンジン１２０は、処理ユニット１２８と、好ましくは、図３および４に示すエリア指紋リーダー１３０である、指紋リーダー１３０とを備える。指紋認証エンジン１２０は受動的であり、したがって、アンテナ１０８からの電圧出力のみによって給電される。処理ユニット１２８は、合理的な時間内にバイオメトリック照合を行えるように、非常に低電力かつ非常に高速であるように選ばれたマイクロプロセッサを備える。
【００６１】
指紋認証エンジン１２０は、指紋リーダー１３０に提示された指または親指をスキャンし、処理ユニット１２８を用いて、指または親指のスキャンした指紋を、予め保存された指紋データと比較するように構成される。次いで、スキャンした指紋が予め保存された指

紋データと一致するかどうか決定される。好ましい実施形態では、指紋画像を捕捉し、カード１０２のベアラを認証するために要する時間は１秒未満である。

【００６２】

一致と決定すると、通信チップ１１０は、認証されて、指紋認証エンジン１２０を通信チップ１１０の処理ユニット１１４に接続する通信線を介してカードリーダー１０４に信号を送信する。通信チップ１１０は、従来の通信チップ１０と同様に、後方散乱変調によって信号を送信する。

【００６３】

状況によっては、カード１０２の所有者が負傷して、カード１０２に登録されている指の損傷につながり得る。この損傷は、例えば、評価されている指の部分の傷跡であり得る。従来のシステムでは、良好なセキュリティを保証するために、一致と決定するための閾値は非常に高く設定されているかも知れない。しかし、その結果、このような損傷は、所有者がカード１０２によって認証されないことを意味し得る。

【００６４】

以下の方法は、バイオメトリックカード１０２の劣化動作モードを可能にし、このような傷害などの場合にベアラによるカード１０２の限定された使用を可能にし得る。これは、傷害が治癒するか新しいカード１０２が発行されるようになるまで、または既存のカード１０２に新しい指紋（例えば、別の指の指紋、または傷害／傷跡を含む。）を登録することが可能になるまで、ユーザが基本機能をなお行えることを意味する。

【００６５】

指紋認証ユニット１２０は、一致と決定するために比較的低い閾値を用いるように構成される。次いで、認証を行うときに、指紋認証ユニット１２０は信頼スコアも決定する。送信された信号は、カードのベアラが認証されたという表示と、認証の信頼スコアとの両方を含む。これにより、カードリーダー１１８（または、それが接続されているコンピュータシステム）は、カード１０２のベアラに与えるアクセスのレベルを決定することができる。

【００６６】

一実施形態では、スマートカード１０２は、剛性ハウジング１３４を備えるトークンなどであってもよく、剛性ハウジング１３４から指紋センサ１３０が露出される。この構成を図３に示す。別の実施形態では、スマートカード２０２は、図４に示すような積層型スマートカード２０２であってもよい。このようなスマートカードは、典型的には、スマートカードの国際仕様であるＩＳＯ７８１６に準拠する。

【００６７】

一実施形態では、スマートカード１０２は、クレジットカード、デビットカード、または他の支払いカードなどの金融カードである。カードリーダー１１８は、ＰＯＳ端末または現金自動預払機の端末であってもよい。カードリーダー１１８は、３つのレベルの信頼度を認識し、対応するレベルの性能を可能にするように構成される。

【００６８】

レベル１）

レベル１のスコアは、完全機能性動作モードを許可する。このレベルでは、非常に低い本人拒否率（ｆａｌｓｅ　ｒｅｊｅｃｔｉｏｎ　ｒａｔｅ：ＦＲＲ）、すなわち、非常に高いバイオメトリックマッチング信頼スコアを有する完全一致が必要である。これは、典型的には、カードのベアラを認証するために従来のシステムで必要とされ得るレベルである。一致がこれらの基準を満たすと、カードは完全な機能性で動作する。例えば、支払いまたは現金引出しの場合、カードを用いて最大カード承認額までの取引が認証され得る（例えば、上限４００ドル）。

【００６９】

レベル２）

レベル２のスコアは、機能性が低減された動作モードを許可する。このレベルでは、低いマッチングスコアを有する部分一致および/または中間のＦＲＲが必要であり得る。こ

のレベルの一致は、典型的には、従来のシステムでは拒否され得る。しかし、ベアラが権限のある人であるという合理的な可能性がなお存在する。一致がこれらの基準を満たすと、カードはなお動作するが、機能性は低下する。例えば、支払いまたは現金引出しの場合、カードを用いて減額された承認額までの取引が認証され得る（例えば、上限５０ドル）。

【００７０】

レベル３）

レベル３のスコアは動作を許可しない。このレベルは、典型的には、非常に高いＦＲＲがあるときに起こり得る。このレベルのスコアでは、カードは動作しない。例えば、支払いや現金引出しの場合、取引は認証されない。

【００７１】

大部分のバイオメトリック照合アルゴリズムは、ある種のマッチングスコアまたは信頼スコアを提供することに留意すべきである。しばしば、ベアラを認証するか否かの決定が、このスコアがある閾値を超えるか否かに基づいて行われる。このように、多くの既存のバイオメトリック照合アルゴリズムが、この方法を実施するために用いられ得る。

【００７２】

カード１０２が、不成功すなわち複数のレベル３のスキャンの認証の反復試行を検知すると、カードは、可能な不正を示す信号をリーダー１１８に送信し得る。例えば、カードは、３回の不成功の試行後、このようなメッセージを送信し得る。

【００７３】

種々の実施形態では、カードがレベル３のスキャンを検知するたびに、権限のないベアラがカードの使用を試行したことを知らせるメッセージと行われた連続試行数とをリーダー１１８に送信してもよい。

【００７４】

次いで、カードは、ある回数不成功の認証試行の後に、動作不能になるか、または、さらなる低減動作モードに置かれるように構成されてもよい。カードは、例えば、銀行の端末にＰＩＮを入力すること、または、写真付身分証明書を銀行員に提示することによって、カードが再有効化されるまでこのモードに置かれてもよい。

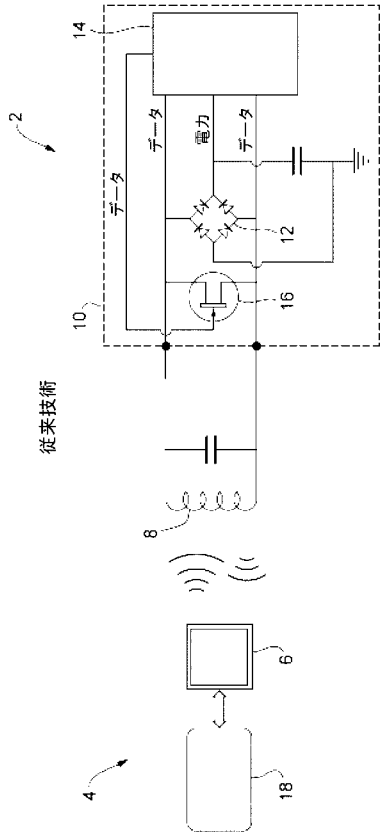
【００７５】

低減動作モードが有効にされると、カード１０２は、ＰＩＮまたは他の検証手段でのみ使用可能であり得る。カードは、また、あるいは、ＰＩＮまたは後で正しく認証された指紋とともに用いられたときであっても、課された取引限度、例えば＄２５が低減され得る。

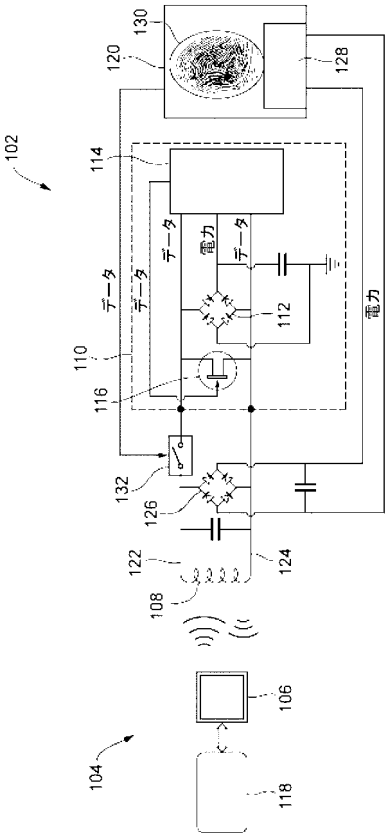
【００７６】

上記実施形態は主に金融スマートカードに関するものであるが、この動作モードは、バイオメトリック認証モジュール１２０を備える任意の他のタイプのデバイスに適用し得ることが理解されよう。例えば、本方法は、アクセス制御システムに適用し得る。レベル１のスキャンは、ベアラがアクセスすることが許可されているすべてのエリアへのアクセスを許可し、劣化動作モードをなお許可するレベル２のスキャンは、建物や駐車場などの低セキュリティエリアへのアクセスを許可し、ベアラは、例えば、交換カードなどを請求するためにセキュリティデスクになお達し得る。このようなシステムでは、スマートカード１０２は、例えば、フォブなどと交換され得る。

【図１】

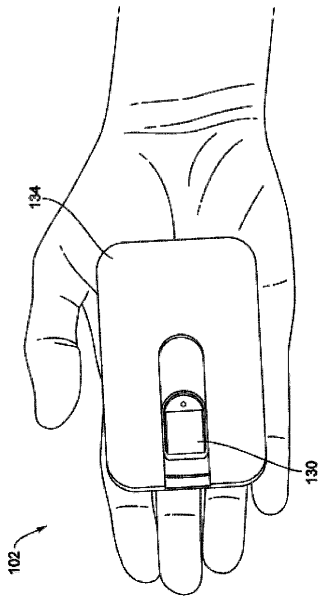


【図２】



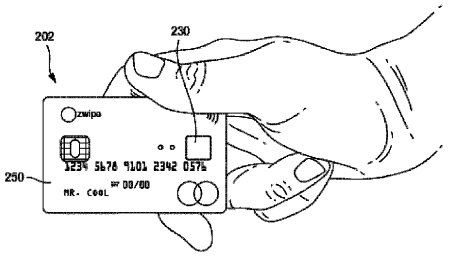
【図３】

Fig. 3



【図４】

Fig. 4



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/082566

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/074615 A1 (HAN BYRON [US] ET AL) 12 March 2015 (2015-03-12) paragraph [0513] paragraph [0522] paragraph [0608] paragraph [0629] - paragraph [0630] -----	1-12,14, 17
X	WO 2014/015386 A1 (CHERRY PETER [AU]) 30 January 2014 (2014-01-30) paragraph [0048] - paragraph [0049] -----	1-3,5, 12-14
X	US 2010/071031 A1 (CARTER STEPHEN R [US] ET AL) 18 March 2010 (2010-03-18) paragraph [0045] paragraph [0046] paragraph [0048] claim 14 ----- -/--	1,2,12, 14-17

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

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 February 2017	06/03/2017

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

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/082566

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2008/060922 A2 (SIMON RODOLPHE J [US]) 22 May 2008 (2008-05-22) paragraph [0024]	1,2,5,6, 12-17
A	US 2004/148526 A1 (SANDS JUSTIN M [US] ET AL) 29 July 2004 (2004-07-29) paragraph [0095] paragraph [0096]	1-17

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/082566

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015074615 A1	12-03-2015	AU 2014334869 A1	17-03-2016
		AU 2016201310 A1	17-03-2016
		CN 105659522 A	08-06-2016
		CN 106095247 A	09-11-2016
		DE 112014004134 T5	21-07-2016
		EP 3044903 A1	20-07-2016
		EP 3101868 A1	07-12-2016
		JP 2016224960 A	28-12-2016
		JP 2017500656 A	05-01-2017
		KR 20160048215 A	03-05-2016
		KR 20160054573 A	16-05-2016
		TW 201528120 A	16-07-2015
		TW 201610826 A	16-03-2016
		US 2015074615 A1	12-03-2015
		US 2015146945 A1	28-05-2015
		WO 2015057320 A1	23-04-2015
WO 2014015386 A1	30-01-2014	AU 2013204744 A1	13-02-2014
		CN 104487987 A	01-04-2015
		EP 2877962 A1	03-06-2015
		JP 2015522890 A	06-08-2015
		KR 20150051989 A	13-05-2015
		RU 2015100234 A	20-09-2016
		US 2015206148 A1	23-07-2015
		WO 2014015386 A1	30-01-2014
US 2010071031 A1	18-03-2010	NONE	
WO 2008060922 A2	22-05-2008	US 2008120509 A1	22-05-2008
		WO 2008060922 A2	22-05-2008
US 2004148526 A1	29-07-2004	US 2004148526 A1	29-07-2004
		WO 2004068283 A2	12-08-2004

フロントページの続き

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