

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4565840号
(P4565840)

(45) 発行日 平成22年10月20日 (2010.10.20)

(24) 登録日 平成22年8月13日 (2010.8.13)

(51) Int. Cl.	F I
H04L 9/32 (2006.01)	H04L 9/00 675A
G06F 21/20 (2006.01)	H04L 9/00 673D
G09C 1/00 (2006.01)	G06F 15/00 330B
	G09C 1/00 640D

請求項の数 26 (全 11 頁)

(21) 出願番号	特願2003-570546 (P2003-570546)	(73) 特許権者	595020643
(86) (22) 出願日	平成15年2月12日 (2003.2.12)		クォアルコム・インコーポレイテッド
(65) 公表番号	特表2005-518721 (P2005-518721A)		QUALCOMM INCORPORATED
(43) 公表日	平成17年6月23日 (2005.6.23)		アメリカ合衆国、カリフォルニア州 92
(86) 国際出願番号	PCT/US2003/004387		121-1714、サン・ディエゴ、モア
(87) 国際公開番号	W02003/071770		ハウス・ドライブ 5775
(87) 国際公開日	平成15年8月28日 (2003.8.28)	(74) 代理人	100091351
審査請求日	平成18年1月31日 (2006.1.31)		弁理士 河野 哲
(31) 優先権主張番号	10/077,365	(74) 代理人	100088683
(32) 優先日	平成14年2月15日 (2002.2.15)		弁理士 中村 誠
(33) 優先権主張国	米国 (US)	(74) 代理人	100109830
(31) 優先権主張番号	10/139,873		弁理士 福原 淑弘
(32) 優先日	平成14年5月6日 (2002.5.6)	(74) 代理人	100084618
(33) 優先権主張国	米国 (US)		弁理士 村松 貞男

最終頁に続く

(54) 【発明の名称】 音響2因子認証システム及び方法

(57) 【特許請求の範囲】

【請求項1】

少なくとも個人識別番号と、信頼されたエンティティに対して提供された機密の公開鍵とを安全な接続を介して承認コンピュータに与えることと、

前記承認コンピュータと、このコンピュータから離れた少なくとも一つの受信機との間の通信リンクを確立することであって、前記通信リンクは、安全であることが強制されていないことと、

前記受信機において、秘密鍵によって生成された少なくとも一つの信号を表す少なくとも一つの音響信号を受信することであって、前記受信機は、前記音響信号を署名信号に変換することと、

前記受信機において、前記音響信号とは別個に受信される前記個人識別番号を受信することと、

前記署名信号を前記個人識別番号を用いて暗号化し、暗号化された署名信号を与えることと、

前記暗号化された署名信号を前記個人識別番号と前記機密の公開鍵とを用いて前記承認コンピュータが検証するために、前記暗号化された署名信号を、前記承認コンピュータに送ることとを備え、

前記暗号化された署名信号を、前記個人識別番号を用いて復号し、さらに、前記機密の公開鍵を用いて検証する認証方法。

【請求項2】

前記暗号化の動作は、前記受信機において行われる請求項 1 に記載の認証方法。

【請求項 3】

ハンドヘルドトークンを用いて前記音響信号を前記受信機へ送信することを備えた請求項 1 に記載の認証方法。

【請求項 4】

所望のトランザクションを前記受信機に入力することであって、前記承認コンピュータは、前記署名信号が検証された場合にのみ、前記トランザクションを実行することを前記受信機に承認することを更に備えた請求項 1 に記載の認証方法。

【請求項 5】

前記ハンドヘルドトークンは、少なくとも一つのメッセージを前記秘密鍵と組み合わせることによって署名信号を生成する請求項 3 に記載の認証方法。

【請求項 6】

前記メッセージは、少なくとも一つのタイムスタンプの少なくとも一部を含む請求項 5 に記載の認証方法。

【請求項 7】

前記タイムスタンプの一部は、予め定めた数よりも多いビットを有するタイムスタンプの、予め定めた数の下位ビットである請求項 6 に記載の認証方法。

【請求項 8】

安全であることが強制されていないリンクを介した 2 因子認証のためのシステムであって、

デジタル署名されたメッセージを表している少なくとも一つの無線信号を生成する少なくとも一つのポータブルトークンと、

前記無線信号と、前記無線信号と別個に受信される個人識別番号とを受信する少なくとも一つの受信機であって、前記個人識別番号を用いて前記署名されたメッセージを暗号化して、暗号化された署名メッセージを与える受信機と、

少なくとも前記暗号化された署名メッセージを、前記リンクを介して受信する少なくとも一つの承認コンピュータであって、前記署名メッセージの検証を試みるために、前記個人識別番号と、信頼されたエンティティに対して提供された機密の公開鍵とにアクセスする承認コンピュータとを備え、

前記承認コンピュータは、前記暗号化された署名メッセージを前記個人識別番号を使って復号し、次に前記識別情報を用いて前記機密の公開鍵にアクセスし、前記機密の公開鍵を用いることによって前記署名されたメッセージを検証するシステム。

【請求項 9】

前記無線信号は、前記デジタル署名されたメッセージを与えるために、少なくとも機密の公開鍵の識別情報と、前記公開鍵に対応した秘密鍵によって署名されたメッセージともまた表している請求項 8 に記載のシステム。

【請求項 10】

前記受信機は、前記暗号化された署名メッセージと、識別情報と、前記承認コンピュータに対して署名されたメッセージとを送信する請求項 9 に記載のシステム。

【請求項 11】

少なくとも個人識別番号と、信頼されたエンティティに対して提供された機密の公開鍵とにアクセスし、遠隔配置された少なくとも一つの受信機と、安全であることが強制されていないリンクを介して通信する承認コンピュータを含む認証システムであって、

前記受信機において、秘密鍵から生成された少なくとも一つのデジタル署名を表す少なくとも一つの無線信号を受信する手段であって、前記受信機は、前記無線信号を署名信号に変換する手段と、

前記受信機において、前記個人識別番号を受信する手段と、

暗号化された署名信号を与えるために、前記個人識別番号を用いて前記署名信号を暗号化する手段であって、前記暗号化された署名信号は、前記個人識別番号と前記機密の公開鍵とを用いて、前記署名信号の検証を行うために、前記リンクを介して前記承認コンピュ

10

20

30

40

50

ータに送られる手段と、

前記暗号化された署名信号を、前記個人識別番号を用いて復号し、前記署名信号を与える手段と、

前記機密の公開鍵を用いて前記署名信号を検証する手段と
を備えた認証システム。

【請求項 1 2】

前記暗号化する手段は、前記受信機にある請求項 1 1 に記載の認証システム。

【請求項 1 3】

ハンドヘルドトークンを用いて前記無線信号を前記受信機へ送信する手段を備えた請求項 1 1 に記載の認証システム。

【請求項 1 4】

請求項 1 1 に記載の認証システムにおいて、

所望のトランザクションを前記受信機に入力する手段であって、前記承認コンピュータは、前記署名信号が検証された場合にのみ、前記受信機が前記トランザクションを実行することを承認する手段を更に備えた認証システム。

【請求項 1 5】

前記ハンドヘルドトークンは、少なくとも一つのメッセージを、前記秘密鍵と組み合わせることによって、署名信号を生成する請求項 1 3 に記載の認証システム。

【請求項 1 6】

前記メッセージは、少なくとも一つのタイムスタンプの少なくとも一部を含む請求項 1 5 に記載の認証システム。

【請求項 1 7】

前記メッセージは更に疑似乱数と組み合わせられている請求項 1 5 に記載の認証システム。

【請求項 1 8】

前記無線信号は、音響信号である請求項 1 1 に記載の認証システム。

【請求項 1 9】

前記無線信号は、音響信号である請求項 8 に記載の認証システム。

【請求項 2 0】

少なくとも個人識別番号と、信頼されたエンティティに対して提供された機密の公開鍵とを安全な接続を介して承認コンピュータに与えることと、

前記承認コンピュータとこのコンピュータから離れた少なくとも一つの受信機との間の通信リンクを確立することであって、前記通信リンクは、安全であることが強制されていないことと、

前記受信機において、秘密鍵によって生成された少なくとも一つの信号を表す少なくとも一つの音響信号を受信することであって、前記受信機は、前記音響信号を署名信号に変換することと、

前記受信機において、前記音響信号とは別個に受信される前記個人識別番号を受信することと、

前記署名信号を前記個人識別番号を用いて暗号化し、暗号化された署名信号を与えることと、

前記暗号化された署名信号を、前記個人識別番号と前記機密の公開鍵とを用いて検証するために前記承認コンピュータに送ることと、

前記暗号化された署名信号を、前記個人識別番号を用いて復号して前記署名信号を与える、次に、前記機密の公開鍵を用いて前記署名信号を検証することと

を備えた方法を実行させるようにコンピュータシステムを制御する命令を含むコンピュータ読取可能記録媒体。

【請求項 2 1】

前記暗号化の動作は、前記受信機において行われる請求項 2 0 に記載のコンピュータ読取可能記録媒体。

10

20

30

40

50

【請求項 2 2】

ハンドヘルドトークンを使って前記音響信号を前記受信機へ送信することを備えた請求項 2 0 に記載のコンピュータ読取可能記録媒体。

【請求項 2 3】

所望のトランザクションを前記受信機に入力することであって、前記承認コンピュータは、前記署名信号が検証された場合にのみ、前記受信機が前記トランザクションを実行することを承認することを更に備えた請求項 2 0 に記載のコンピュータ読取可能記録媒体。

【請求項 2 4】

前記ハンドヘルドトークンは、少なくとも一つのメッセージを前記秘密鍵と組み合わせることによって署名信号を生成する請求項 2 2 に記載のコンピュータ読取可能記録媒体。

10

【請求項 2 5】

前記メッセージは、少なくとも一つのタイムスタンプの少なくとも一部を備えている請求項 2 4 に記載のコンピュータ読取可能記録媒体。

【請求項 2 6】

前記タイムスタンプの一部は、予め定めた数よりも多いビットを有するタイムスタンプの予め定めた数の下位ビットである請求項 2 5 に記載のコンピュータ読取可能記録媒体。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、一般に音調を用いた認証に関する。

20

【背景技術】

【0 0 0 2】

インターネット利用が増大し、例えば、製品やサービスをオンラインで購入すること、オンラインでバンキングすること、及び遠隔銀行に接続された A T M を利用することのよう多くの種類の便利な電子商取引が可能になった。しかしながら、電子商取引の最も便利な点は、泥棒が貴重な情報を盗んだり、他の誰かになりすまし、製品を購入したり、銀行口座からお金を引き出したりすることを容易にした。

【0 0 0 3】

従って、電子トランザクションにセキュリティを与えることは重要である。この目的のため、交換されている個人情報隠すために多くの電子トランザクションが暗号化されている。しかし、暗号化はセキュリティの一つの局面に過ぎない。なぜなら、泥棒にとって、暗号を破り、例えばクレジットカードのようなその他の有効な項目の財産に入り込み、所有者になりすまし、暗号化されたトランザクションに参加することは可能だからである。

30

【0 0 0 4】

これを念頭におけば、認証はセキュリティの重要な局面であることが容易に理解されよう。電子商取引に関し、認証を求める人は、コンピュータインタフェースを通じてそれを行う。結果として、通常、この人であると言った人が本当であることを検証するために、人の生物学的特徴（容姿、筆跡、指紋等）の確認に頼ることは、バイオ感知コンピュータアクセサリが広く搭載されていないので実現可能ではない。

40

【0 0 0 5】

これによって、2 つの認証因子が残った。すなわち、クレジットカードや、キーファブのような所持品に基づいて人を認証することか、あるいは、パスワードや個人識別番号（P I N）のような人が知るものに基づいて認証することである。A T M 現金引落機のような特別に取り扱いに慎重を要するアプリケーションでは、両方の因子が望ましい。

【0 0 0 6】

現在、A T M 利用者は、クレジットカードのような認証デバイスを A T M に用い、次に P I N を入力する。この方法によって、2 因子認証が達成される。しかしながら、A T M は、カード上の秘密情報と P I N との両方を、認証のために中央銀行コンピュータに送信しなければならない。その結果、この銀行と A T M との間の接続は、泥棒がラインを盗み

50

見し、両認証因子を発見することがないように安全でなければならない。さもなければ、この泥棒は、このユーザの口座からお金を盗むことができるようになるからである。これは、接続インフラストラクチャにおける多大な負担を強いる。

【0007】

特許出願1は、ハンドヘルド音波に基づいた「トークン」を開示している。これは、人が、秘密情報を表す音響信号を、この信号に基づいて認証するために、「認証装置」、「検証装置」、あるいは「受信機」と称されるデバイスへの送信を操作することができるものである。これらの出願で認識されたように、音波に基づいたトークンの利点は、音を受信し、この音から発する電子信号を送信する大規模なインフラストラクチャが既に存在していることである。具体的には、音響情報を示すデータを送信するための大規模な電話システムが存在している。また、電話とは別に、同じシステム（例えばインターネット）によって接続された多くの計算機は、マイクロフォンとスピーカとを持っている（あるいは、それらを持つように容易に変更することができる）。

10

【0008】

ここで認められるように、ATMのコンテキストで使用された場合には、音波トークンは、ATMが、機密の鍵がなく個人情報に偽造されることのないようにして、トークン上の個人情報をATMに送信するという利点を持つ。ATMは単に認証のために個人情報を、中央銀行コンピュータに送信する。したがって、ATMのみならず、ATMと銀行との間の接続もまたこの認証因子を保護するために安全にする必要は無い。しかしながら、本発明は更に、第2の認証因子であるPINはいまだに接続安全性を必要とする。これは、PINは一般にほんの4～6桁から構成されるに過ぎず、攻撃者は、ATMと銀行との間の接続を盗み見ることができるからである。そして、仮に、この通信が、推定されたPINの検証を許可した場合には、この攻撃者は、トークンを盗み、口座へのアクセスを取得するまで、100万あるいはその程度の可能なPIN値のトライアウトを単に行い、うまく動作するものを覚えることができる。その結果、銀行とATMとの間の安全な通信は、残念ながら、未だに必要とされている。

20

【0009】

上記の問題を認識することによって、ここで開示された本発明が提供されている。

【特許文献1】米国特許出願番号10/077, 385

【非特許文献1】“National Institute for Standards and Technology (NIST) Federal Information Processing Standards Publication” 186-2, January, 2000

30

【発明の開示】

【0010】

本出願は、ここで参考文献として組み込まれている「Method and Apparatus for Simplified Audio Authentication」と題され、2002年2月15日に提出された共に係属中の米国出願番号10/077, 385（特許出願1）の一部継続出願である。

【0011】

認証の方法は、例えば銀行コンピュータのような承認コンピュータに対して機密の公開鍵とPINとを与えることと、承認コンピュータと、このコンピュータと離れている例えばATMのような受信機との間の通信リンクを確立することとを備えている。この通信リンクは、安全でなくても良い。その結果、ユーザの音響信号を受信機（例えばATM）において受信することができる。この信号は、秘密鍵で生成されたデジタル署名を表しており、受信機は、音響信号を署名信号に変換する。PINはまた、例えばこの受信機に対応したデータ入力デバイスにPINを入力したユーザによって、受信機によって受信される。これによって、PINは、音響信号とは別個に受信される。署名信号は、PINを用いて暗号化され、暗号化された署名信号が与えられる。これは、その後、PINと機密の公開鍵を用いてこの署名を検証するために承認コンピュータに送られる。

40

【0012】

好適には、署名信号は、受信機によってPINを用いて暗号化される。一方、音響信号は、好適には、ハンドヘルドトークンを用いて送信される。所望のトランザクションが、

50

承認コンピュータを備えた受信機に入力される。この承認コンピュータは、署名が検証された場合にのみ、受信機がトランザクションを実行することを承認する。

【0013】

この署名は、承認コンピュータが、署名信号を出力するために、暗号化された署名信号を、PINを用いて復号することによって検証される。その後、結果として得られた署名信号は、機密の公開鍵を用いて検証される。

【0014】

ある好適な実施例では、トークンが、メッセージに秘密鍵を組み合わせることによって、署名信号を生成する。このメッセージは、少なくともタイムスタンプの一部、例えば、タイムスタンプの予め定めた数の最下位ビットのようなタイムスタンプの一部を含むことができる。ここで、タイムスタンプは、前記予め定めた数よりも多くのビットを持っている。

10

【0015】

別の局面では、システムが、安全である必要がない接続を介した2因子認証のために開示されている。このシステムは、デジタル署名されたメッセージを表す無線信号を生成するポータブルトークンを含む。受信機は、無線信号とPINとを受信する。このPINは、無線信号とは別個に受信される。受信機は、署名された信号をPINを用いて暗号化し、暗号化された署名メッセージにする。承認コンピュータは、この接続を介して暗号化された署名メッセージを受信し、署名メッセージの検証を試みるためにPINと機密の公開鍵とにアクセスする。

20

【0016】

また、別の局面では、認証のためのシステムが、少なくともPINと機密の公開鍵とにアクセスし、コンピュータと隔たれている少なくとも一つの受信機と接続を介して通信する承認コンピュータを含んでいる。この通信リンクは、安全である必要は無い。このシステムは、メッセージと秘密鍵とを組み合わせることによって生成されたデジタル署名を表す無線信号を、受信機において受信する手段を含んでいる。この受信機は、無線信号を署名信号に変換する。受信機における手段は、PINも受信する。暗号化された署名信号を与えるために、PINを用いて署名信号を暗号化するための手段が提供される。暗号化された署名信号は、PINと機密の公開鍵とを用いて署名を検証するためにリンクを介して承認コンピュータに送られる。

30

【発明を実施するための最良の形態】

【0017】

本発明の詳細は、その構成及び動作ともに、同一部位に対して同一の符番を付している添付図面を参照することによって最も良く理解することができる。

【0018】

まず、図1に、一般に10で示すように、キーファブまたは他の小型デバイスで構成することができるポータブルハンドヘルドトークン12を含むシステムが示されている。しかしながら、本発明は、ラップトップコンピュータ、無線ハンドセット又は電話、データトランシーバ、又はページング及び位置決め受信機を含み、希望されれば車両（車、トラック、ボート、航空機、列車を含む）搭載型のハンドヘルド又はポータブルな移動通信局のような他のトークン構成に適用する。無線通信デバイスはまた、時として、ユーザ端末、移動局、移動ユニット、加入者ユニット、移動無線又は無線電話、無線ユニット、又はある通信システムでは単に「ユーザ」及び「モバイル」とも称される。

40

【0019】

いずれの場合であれ、トークン12は、線14によって図示され、受信機16によって受信することができる音響信号を生成することができる。受信機16は、承認コンピュータ18に対応している。図示した実施例では、受信機16は、例えばビル、家、車両、又は2因子認証を用いた仮承認されたユーザに対するアクセスを制限することが望まれるその他の任意の構成要素に対応した受信デバイスであるものと理解されるべきであるが、受信機16は、ATMであり、承認コンピュータ18は、銀行メインコンピュータである。

50

好適なトークン１２は、音響信号を生成する音波トークンである一方、本原理は、例えばブルートゥース及び赤外線といった無線周波数（r f）のような電磁波無線通信原理を用いるものを含み、後述するデジタル署名を受信機１６に送信する他の無線信号生成トークンに適用している。

【００２０】

好適な音響信号１４は、トークン１２の電子データストア２０に格納された秘密鍵を用いて生成されるデジタル署名を表すことができる。疑似乱数（P N）生成器２１をトークン１２上に含めることもできる。対応する機密の公開鍵又は機密の公開鍵識別子もまた、簡単に開示する目的のためにそこに格納することができる。

【００２１】

当該技術分野で知られており、例えば「National Institute for Standards and Technology (NIST) Federal Information Processing Standards Publication 186-2, January, 2000」（非特許文献１）に記載されている秘密鍵／公開鍵原理に従うと、トークン１２における署名アルゴリズム（トークン１２内のマイクロプロセッサ２２によって実行される）は、入力として秘密鍵と、署名されP N生成器２１からの乱数「k」を持つメッセージの少なくとも一部とを取得し（したがって「結合し」）、ランダムペア（r、s）であるデジタル署名を与える。好適には、マイクロプロセッサ２２は、トグルスイッチ、音声起動デバイス、またはプッシュボタンのような一つ又は複数の起動要素２４からの起動信号を受信すると、署名アルゴリズムを実行する。署名されているメッセージと、秘密鍵に対応する機密の公開鍵の識別とはまた、好適には、マイクロプロセッサ２２によって生成された信号に含まれる。マイクロプロセッサ２２は、当該技術分野で知られた必要な時計、アナログデジタル変換回路、及びデジタルアナログ変換回路と同様に、適切にデジタルプロセッサを含みうると理解されるべきである。

【００２２】

マイクロプロセッサ２２は、多数の起動要素２４が使用された場合に、一つ又は複数がストア２２内のそれぞれの秘密鍵に対応できるようにデータストア２０にアクセスする。電子署名信号は、音響信号１４に変換されるためにオーディオスピーカ２６に送られる。この音響信号は、可聴であるかも、また可聴でないかもしれない。必要ならば、マイクロフォン２８は、音響信号を受信し、それらを、処理のためにマイクロプロセッサ２２に送られる電子信号に変換するためにトークン１２に備えることもできる。E M波無線原理が使用された場合、スピーカ２６は、例えばr f送信機またはI R送信機によって置き換えられる。

【００２３】

好適な音響信号１４は、マイクロフォン又はその他の音響受信デバイス３０によって受信機１６において受信される。音響信号は、マイクロフォン２０によって変換され、電子署名信号（望ましい場合には、機密の公開鍵I Dとオリジナルの仮署名メッセージを伴う）に戻される。そして、マイクロプロセッサ３２に送られる。これは、必要ならばデータストア３４にアクセスする。必要ならば、スピーカ３６は、音響信号をトークン１２に戻すために受信機１６に備えることもできる。この信号は、トークン１２上のマイクロフォン２８によって受信される。

【００２４】

受信機１６がA T Mであり、承認コンピュータ１８が中央銀行コンピュータである場合、承認コンピュータ１８は、プロセッサ３８を含むことができる。プロセッサ３８は、データストア４０にアクセスし、受信機１６から受信されたデジタル署名を検証する（又は、検証しない）ことによって選択的に承認を許可する。データストア４０は、信号によって表される秘密鍵に関連している機密の公開鍵（及びそのI D）を格納するリスト又はデータベーステーブルのようなデータ構造を含むことができる。いずれの場合であれ、銀行をA T Mと接続している線４１は、以下に記載されている暗号方法の斬新な利用により、安全である必要はない。

【００２５】

図 2 は、本発明のロジックを示している。ブロック 4 2 で始まるように、公開鍵の ID を伴ったトークン 1 2 に関連している機密の公開鍵が、承認コンピュータ 1 8（例えばメイン銀行コンピュータ）に与えられる。また、ユーザの PIN が提供される。この提供は、人間によって、あるいは安全な接続を介して安全に行われる。「機密の公開鍵」は、当該技術分野で知られた秘密鍵／公開鍵原理に従った公開鍵を意味しており、機密の公開鍵が一般にアクセス可能ではない場合を除いて、メイン銀行コンピュータのように信頼されたエンティティに対してのみ提供される。

【0026】

ブロック 4 4 では、ユーザが起動要素 2 4 のうちの一つを操作した場合には、トークン 1 2 内の署名アルゴリズムは、例えばランダムペア（ r 、 s ）のような電子署名を生成するために秘密鍵、疑似乱数、及びタイムスタンプの全て又は一部のようなメッセージを入力として受信する。その後ユーザは、両認証因子を受信機 1 6 に入力する。特に、ブロック 4 6 では、デジタル署名が、署名されたメッセージ、及び望まれる場合には、対応する機密の公開鍵の ID とともに無線で（例えば、聴覚的に）受信機 1 6 に送信される。そして、ブロック 4 8 では、ユーザは、例えばほとんどの ATM に備えられている数値キーパッドを使って、PIN を入力する。ブロック 5 0 では、所望の トランザクション（例えば、引落、振込等）が入力される。ブロック 4 6、4 8、5 0 におけるステップは、あらゆる要望において実行可能であるものと理解されるべきである。

【0027】

本発明に従って、ブロック 5 2 では、受信機 1 6 が、PIN を用いて署名（ r 、 s ）を暗号化する。この暗号化は、例えば AES 暗号原理を使った対称的な暗号化でありうる。暗号化された署名は、暗号化されていない機密の公開鍵 ID と、署名されている暗号化されていない仮署名メッセージ（例えば、タイムスタンプ又はその最下位の 2 ビット）とともにメインコンピュータプロセッサ 3 8 に送られる。

【0028】

ブロック 5 4 では、メインプロセッサ 3 8 は、PIN を用いてデジタル署名を先ず復号化する。そして、機密の公開鍵 ID とオリジナルの仮署名メッセージとを用いて、プロセッサは、データストア 4 0 から適切な機密の公開鍵を検索し、当該技術で知られた公開鍵／秘密鍵に従って署名を 検証 する。もしもこの 検証 が成功した場合には、承認コンピュータ 1 8 は、受信機 1 6 に対して信号を送り、アクセスを許可する。ATM 検証 1 6 及び銀行コンピュータ承認コンピュータ 1 8 の場合、銀行コンピュータは、要求された トランザクション を実行するために ATM に信号を送る。

【0029】

ATM と銀行との線 4 1 上における通信を妨害する攻撃者は、PIN を推定することができないものと認められよう。具体的には、「正しい」PIN を用いて署名を復号することは、正しくない PIN、すなわち、署名を 検証 することなく理解されることができないランダムペア、機密の公開鍵と、署名されているデータとがなくてはなされない何かを使って復号することと等価なものを生成する（タイムスタンプの最下位ビットのみが送信されることに着目されたい）。この特徴は、線 4 1 における安全のための最終的な要求を取り除く。

【0030】

ここで示され、その詳細が記載されている音響 2 因子認証のための特別なシステム及び方法は、本発明の上記目的を完全に達成することができる一方、本発明の表された好適な実施例、すなわち主要要件の代表例は、本発明によって広く考慮されるものであることと、本発明の範囲は、当該技術分野における熟練者にとっては明らかである他の実施例にも十分に含むことと、本発明の範囲は、「一つであり唯一」と明確に述べられていないのであれば、単数である要素に対する参照が「一つであり唯一」を意味することを意図しておらず、むしろ「一つ又は複数」を意味する請求項以外の何れによっても制限されることはないこととが理解されるべきである。当該技術における通常の熟練者にとって知られている、あるいは知られるものとなる上記した好適な実施例の要素に対する全ての構造的及び

機能的な等価物は、ここでは明らかに参考文献として組み込まれており、本発明の請求項によって含まれることを意図している。更に、デバイス又は方法にとって、本発明によって解決されることが求められるそれぞれ及び全ての問題に対処する必要はない。なぜなら、それは請求項によって含まれるべきであるからである。更には、要素、構成要素、又は方法ステップが請求項で明白に列挙されているか否かに関わらず、本開示におけるいかなる要素、構成要素、又は方法ステップも、公衆に対してなされたものであることを意図していない。仮に、この要素が、「するための手段 (means for)」という表現を用いてはっきりと列挙されていない場合、あるいは方法請求項の場合には「動作」の代わりに「ステップ」として列挙されていない場合には、ここにおけるいかなる請求項要素も、35 U.S.C. 112条、第6パラグラフの規定の下で解釈されるべきではない。

10

【図面の簡単な説明】

【0031】

【図1】図1は、オーディオベースの認証のための本システムのブロック図である。

【図2】図2は、本ロジックのフローチャートである。

【符号の説明】

【0032】

12…トークン

14…線

16…受信機

18…承認コンピュータ

20

20…データストア

21…疑似乱数生成器

22…マイクロプロセッサ

24…起動要素

26…オーディオスピーカ

28, 30…マイクロフォン

32…マイクロプロセッサ

34…データストア

36…スピーカ

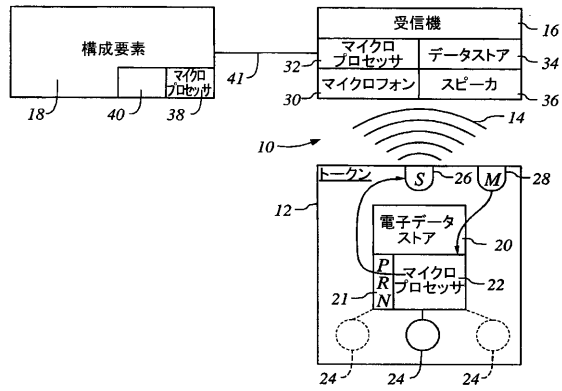
38…メインプロセッサ

30

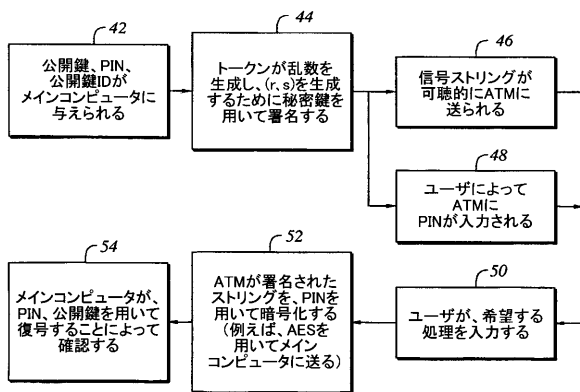
40…データストア

41…線

【図 1】



【図 2】



フロントページの続き

(74)代理人 100092196

弁理士 橋本 良郎

(72)発明者 ガントマン、アレクサンダー

アメリカ合衆国、カリフォルニア州 92129、サン・ディエゴ、クリークウッド・レーン 8704

(72)発明者 ローズ、グレゴリー・ジー

オーストラリア国、ニュー・サウス・ウェールズ州 2137、コンコード、アーチャー・ストリート 40

審査官 新田 亮

(56)参考文献 国際公開第02/005078 (WO, A1)

特開2001-007802 (JP, A)

特開平11-289324 (JP, A)

特開2001-265217 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 9/32

G06F 21/20

G09C 1/00