(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6556145号
(P6556145)

(45)発行日　令和1年8月7日(2019.8.7)　(24)登録日　令和1年7月19日(2019.7.19)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A
G06F 21/35 (2013.01)　H04L 9/00 673E
G06F 21/35

請求項の数 20　(全 21 頁)

(21)出願番号　特願2016-544601 (P2016-544601)
(86)(22)出願日　平成26年12月23日 (2014.12.23)
(65)公表番号　特表2017-503427 (P2017-503427A)
(43)公表日　平成29年1月26日 (2017.1.26)
(86)国際出願番号　PCT/US2014/072102
(87)国際公開番号　WO2015/103031
(87)国際公開日　平成27年7月9日 (2015.7.9)
審査請求日　平成29年2月22日 (2017.2.22)
(31)優先権主張番号　61/922,215
(32)優先日　平成25年12月31日 (2013.12.31)
(33)優先権主張国・地域又は機関
米国 (US)

早期審査対象出願

前置審査

(73)特許権者　516196967
ヴァスコ　データ　セキュリティ　インターナショナル　ゲゼルシャフト　ミット　ベシュレンクテル　ハフツング
スイス　ツェーハー－８１５２　グラットブルク　バルツ－ツィンマーマンシュトラーセ　７　ワールド－ワイド　ビジネス　センター
(74)代理人　100104411
弁理士　矢口　太郎
(72)発明者　マリエン、ディルク
ベルギー王国、ビー－２５５０　ランスト、ブロデストラット　９

審査官　和平　悠希

最終頁に続く

(54)【発明の名称】モバイルアプリケーションの安全性を確保する方法および装置

(57)【特許請求の範囲】

【請求項１】

アクセス装置と、ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保するための認証装置と、を有する装置であって、

前記アクセス装置は、近距離無線通信（ＮＦＣ）転送装置を有し、前記認証装置はアクセス装置に永久的に固定されているものであり、

前記認証装置は、

秘密鍵を格納するように構成されたメモリーコンポーネントと、

前記秘密鍵と動的変数値とを暗号化して組み合わせることによって動的認証情報を生成するように構成されたデータ処理コンポーネントと、

前記認証装置を近距離無線通信（ＮＦＣ）転送装置に接続する近距離無線通信（ＮＦＣ）インターフェースと、

前記ユーザからの入力を取得するためのユーザ入力インターフェースと、

を有し、

前記認証装置は、

近距離無線通信（ＮＦＣ）タグとして前記近距離無線通信転送装置に対して提示されるものであり、

前記近距離無線通信タグの第一のデータコンテンツ内に前記生成された動的認証情報を含めることにより該動的認証情報を前記近距離無線通信転送装置に利用可能とするように構成されているものであり、かつ、当該第一のデータコンテンツは前記近距離無線通信

タグのデータコンテンツを読み出す近距離無線通信（ＮＦＣ）機構を用いて前記近距離無線通信転送装置によって読み出し可能になっているものであり、

前記データ処理コンポーネントが前記動的認証情報を生成する工程、または前記認証装置が前記生成された動的認証情報を前記近距離無線通信転送装置に利用可能とする工程、のうち少なくとも１つに対する条件として前記ユーザからの特定の入力を要求するように構成されており、

前記ユーザ入力インターフェースによってユーザにより起動されるようになっており、前記ユーザがこの認証装置を前記ユーザ入力インターフェースによって起動した後でのみこの認証装置は近距離無線通信（ＮＦＣ）タグとして前記近距離無線通信転送装置に対して提示されるように構成されているものである、

前記装置。

【請求項２】

請求項１記載の装置において、前記認証装置は、さらに、

１型、２型、３型または４型の近距離無線通信（ＮＦＣ）フォーラムに準拠したタグとして提供され、

前記近距離無線通信転送装置が、近距離無線通信フォーラムに準拠したタグから近距離無線通信データ交換フォーマット（ＮＤＥＦ：ＮＦＣ　ｄａｔａ　Ｅｘｈａｎｇｅ　Ｆｏｒｍａｔ）のメッセージを読み出す近距離無線通信（ＮＦＣ）機構を用いて、前記生成された動的認証情報を読み出すために、該動的認証情報を前記認証装置の近距離無線通信データ交換フォーマットファイルの該データ交換フォーマット（ＮＤＥＦ）メッセージにおける該データ交換フォーマット（ＮＤＥＦ）レコードに含めることによって該動的認証情報を前記転送装置に利用可能とするように構成されているものである、装置。

【請求項３】

請求項１記載の装置において、前記認証装置は、さらに、

クロックを有し、

前記動的変数は前記クロックによって提供される時刻値に基づくものである、認証装置。

【請求項４】

請求項１記載の装置において、前記動的変数は、前記メモリーコンポーネント内に格納され、特定のイベントが発生する毎に前記認証装置によって更新されるイベント関連値に基づくものである、装置。

【請求項５】

請求項４記載の装置において、前記特定のイベントは、前記動的認証情報の生成と同時に発生するものである、装置。

【請求項６】

請求項４記載の装置において、前記イベント関連値は、前記特定のイベントが発生する毎に前記認証装置によって単調増加または単調減少されるカウンタを有するものである、装置。

【請求項７】

請求項１記載の装置において、前記秘密鍵と前記動的変数値とを暗号化して組み合わせる工程は、前記動的変数値に対称暗号化アルゴリズムを適用する工程を有し、前記対称暗号化アルゴリズムは前記秘密鍵でパラメータ化されるものであり、前記秘密鍵は前記生成された動的認証情報を検証するための機関と共有されるものである、装置。

【請求項８】

請求項１記載の装置において、さらに、

ユーザ識別子を格納し、

近距離無線通信タグのデータコンテンツを読み出す近距離無線通信機構を用いて前記近距離無線通信転送装置により読み出し可能である、前記近距離無線通信タグのデータコンテンツ内に前記動的認証情報を含めることにより、前記ユーザ識別子を前記近距離無線通信転送装置に利用可能とするように構成されているものである、

装置。
【請求項９】
請求項１記載の装置において、前記ユーザ入力インターフェースはアクティベーションボタンを有し、前記特定の入力はユーザが前記アクティベーションボタンを押す工程を含むものである、装置。
【請求項１０】
請求項１記載の装置において、さらに、前記近距離無線通信転送装置を有するアクセス装置への取り付け用に接着コンポーネントを有するものである、認証装置。
【請求項１１】
請求項１記載の装置において、前記近距離無線通信転送装置を有するアクセス装置の保護シェルまたは保護カバー内に含まれるものである、装置。
【請求項１２】
請求項１記載の装置において、
前記動的変数は外部データに基づいており、
前記認証装置は、さらに、近距離無線通信タグのデータコンテンツを更新する近距離無線通信機構を用いて前記近距離無線通信転送装置により更新された、前記近距離無線通信タグの第二のデータコンテンツから外部データを抽出することにより、前記近距離無線通信転送装置から該外部データを受信するように構成されているものである、装置。
【請求項１３】
請求項１２記載の装置において、さらに、
前記認証装置はユーザ出力インターフェースを有し、
前記外部データは取引データを有し、
前記認証装置は、さらに、前記取引データをユーザに提示し、前記提示された取引データに対する前記ユーザによる承諾または拒否を前記ユーザ入力インターフェースで取得し、前記ユーザが前記提示された取引データを承諾した場合にのみ、前記動的認証情報を生成し、および／または、前記生成された動的認証情報を前記近距離無線通信転送装置に利用可能にするように構成されているものである、装置。
【請求項１４】
請求項１３記載の装置において、前記ユーザ入力インターフェースは、前記承諾を取得するための承諾ボタンと、前記拒否を取得するための拒否ボタンを有するものである、装置。
【請求項１５】
請求項１３記載の装置において、さらに、
前記認証装置は、前記近距離無線通信転送装置から前記外部データを受信した後、所定の期間、近距離無線通信タグとして前記近距離無線通信転送装置に提供されないように構成されており、かつ前記ユーザが前記提示された取引データを承諾または拒否した後にのみ、前記近距離無線通信転送装置に再び提供されるように構成されているものである、装置。
【請求項１６】
請求項１記載の装置において、さらに、
近距離無線通信タグのデータコンテンツを更新する近距離無線通信機構を用いて前記近距離無線通信転送装置により更新された、前記近距離無線通信タグの第三のデータコンテンツからパスワード値を抽出することにより、前記近距離無線通信転送装置から該パスワード値を受信し、
前記受信したパスワード値が正しいかどうかを検証し、
前記パスワード値を受信し、かつ該パスワード値が正しいと検証した場合にのみ、前記動的認証情報を生成し、および／または前記生成した認証情報を前記近距離無線通信転送装置に利用可能にするように構成されているものである、
装置。
【請求項１７】

ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保するためのシステムであって、
動的認証情報を生成する認証装置と、
前記コンピュータベースのアプリケーションのサーバ部をホストし、前記認証装置によって生成された前記動的認証情報を検証するアプリケーションサーバと、
前記ユーザによる前記コンピュータ・ベース・アプリケーションへのアクセスを許可するためのアクセス装置であって、コンピュータネットワークによって前記アプリケーションサーバに接続され、前記認証装置から前記動的認証情報を取得し、かつ前記取得した動的認証情報を検証のために前記アプリケーションサーバに転送するように構成されているものである、前記アクセス装置と、
を有し、
前記アクセス装置は近距離無線通信（ＮＦＣ）転送装置を有し、
前記認証装置は、
秘密鍵を格納するように構成されたメモリーコンポーネントと、
前記秘密鍵と第一の動的変数の第一の値とを暗号化して組み合わせることによって前記動的認証情報を生成するように構成されたデータ処理コンポーネントと、
前記認証装置を前記近距離無線通信転送装置に接続する近距離無線通信（ＮＦＣ）インターフェースと、
前記ユーザからの入力を取得するためのユーザ入力インターフェースと、
を有し、
前記認証装置は、アクセス装置に永久的に固定されているものであり、かつ、
近距離無線通信（ＮＦＣ）タグとして前記近距離無線通信転送装置に対して提示されるものであり、
前記近距離無線通信タグの第一のデータコンテンツ内に前記生成された動的認証情報を含めることにより、該動的認証情報を前記近距離無線通信転送装置に利用可能とするように構成されているものであり、かつ、前記第一のデータコンテンツは前記近距離無線通信タグのデータコンテンツを読み出す近距離無線通信（ＮＦＣ）機構を用いて前記近距離無線通信転送装置によって読み出し可能になっているものであり、
前記データ処理コンポーネントが前記動的認証情報を生成する工程、または前記認証装置が前記生成された動的認証情報を前記近距離無線通信転送装置に利用可能とする工程、のうち少なくとも１つに対する条件として前記ユーザからの特定の入力を要求するように構成されており、
前記ユーザ入力インターフェースによってユーザにより起動されるようになっており、前記ユーザがこの認証装置を前記ユーザ入力インターフェースによって起動した後でのみこの認証装置は近距離無線通信（ＮＦＣ）タグとして前記近距離無線通信転送装置に対して提示されるように構成されているものであり、
前記アクセス装置は、近距離無線通信タグのデータコンテンツを読み出す近距離無線通信機構を用いて前記近距離無線通信転送装置により読み出し可能である、前記近距離無線通信タグの前記第一のデータコンテンツから前記動的認証情報を抽出することにより、前記動的認証情報を取得するものであり、
前記アプリケーションサーバは、前記認証装置により生成され、前記アクセス装置により取得および転送された前記動的認証情報を受信し、前記受信した動的変数を第二の動的変数の第二の値と共に暗号化アルゴリズムを用いて検証するように構成されているものである、
システム。
【請求項１８】
請求項１７記載のシステムにおいて、前記秘密鍵と前記第一の動的変数の前記第一の値とを暗号化して組み合わせる工程は、前記第一の動的変数の前記第一の値に対称暗号化アルゴリズムを実行する工程を有し、該対称暗号化アルゴリズムは前記秘密鍵でパラメータ化され、前記秘密鍵は前記認証装置と前記アプリケーションサーバとの間で共有され、前

記アプリケーションサーバは前記秘密鍵のサーバコピーを用いて前記動的認証情報を検証するものである、システム。

【請求項１９】

請求項１７記載のシステムにおいて、

前記認証装置および前記アクセス装置は結合用の秘密（ｂｉｎｄｉｎｇ　ｓｅｃｒｅｔ）を共有し、

前記アクセス装置は、さらに、前記近距離無線通信転送装置が、近距離無線通信タグのデータコンテンツを更新する近距離無線通信機構を用いて、前記近距離無線通信タグの第二のデータコンテンツを更新することにより前記結合用の秘密から導き出された結合値を前記認証装置に通信するように構成され、

前記認証装置は、さらに、

近距離無線通信タグのデータコンテンツを更新する前記近距離無線通信機構を用いて前記近距離無線通信転送装置により更新された、前記近距離無線通信タグの前記第二のデータコンテンツから前記結合値を抽出することにより、前記アクセス装置から前記結合値を受信し、

前記結合用の秘密を用いて前記受信した結合値を検証し、

前記受信した結合値が正しいと検証した場合にのみ、前記動的認証情報を生成し、および／または、前記生成した動的認証情報を前記近距離無線通信転送装置に利用可能にするものである、

システム。

【請求項２０】

ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保する方法であって、

アクセス装置に永久的に固定されている認証装置であり、前記ユーザからの入力を取得するためのユーザ入力インターフェースと近距離無線通信転送装置に接続するための近距離無線通信（ＮＦＣ）インターフェースを有する認証装置で、第一の動的変数の第一の値と、前記認証装置に格納されかつ前記アプリケーションのサーバ部をホストするアプリケーションサーバと共有する秘密鍵とを暗号化して組み合わせることにより動的認証情報を生成する工程であって、前記認証装置は近距離無線通信タグとして前記近距離無線通信転送装置に提供されるものである、前記生成する工程と、

前記認証装置で、前記近距離無線通信タグの第一のデータコンテンツ内に前記生成された動的認証情報を含めることにより該動的認証情報を前記近距離無線通信転送装置に利用可能とする工程であって、ここで、

当該第一のデータコンテンツは前記近距離無線通信タグのデータコンテンツを読み出す近距離無線通信（ＮＦＣ）機構を用いて前記近距離無線通信転送装置によって読み出し可能になっているものであり、

前記認証装置が前記動的認証情報を生成する工程、または前記認証装置が前記生成された動的認証情報を前記近距離無線通信転送装置に利用可能とする工程、のうち少なくとも１つに対する条件として前記ユーザからの特定の入力を要求するようになっているものであり、

前記認証装置はユーザ入力インターフェースによってユーザにより起動されるようになっており、前記ユーザがこの認証装置を前記ユーザ入力インターフェースによって起動した後でのみこの認証装置は近距離無線通信（ＮＦＣ）タグとして前記近距離無線通信転送装置に対して提示されるようになっているものであり、

前記近距離無線通信転送装置を有し、コンピュータネットワークによって前記アプリケーションサーバに接続されたアクセス装置を用いて、前記ユーザが前記コンピュータベースのアプリケーションにアクセスするのを許可する工程と、

前記アクセス装置で、近距離無線通信タグのデータコンテンツを読み出す前記近距離無線通信転送装置を用いて前記近距離無線通信転送装置により読み出された、前記近距離無

線通信タグの前記データコンテンツから動的認証情報を抽出することにより、前記動的認証情報を取得する工程と、
前記アクセス装置で、前記動的認証情報を前記アプリケーションサーバに転送する工程と、
前記アプリケーションサーバで、前記認証装置で生成され、前記アクセス装置で取得された前記動的認証情報を受信する工程と、
前記アプリケーションサーバで、前記受信した動的認証情報を検証する工程と、を有する、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、２０１３年１２月３１日付けで出願された、「Ａ ＭＥＴＨＯＤ ＡＮＤ ＡＰＰＡＲＡＴＵＳ ＦＯＲ ＳＥＣＵＲＩＮＧ Ａ ＭＯＢＩＬＥ ＡＰＰＬＩＣＡＴＩＯＮ（モバイルアプリケーションを安全にする方法および装置）」という名称の米国仮特許出願第６１／９２２，２１５号に対して優先権を主張するものであり、その全体が本明細書に参照により組み込まれる。
【０００２】
本発明は、コンピュータとアプリケーションへのリモートアクセスおよびコンピュータネットワークによるリモート取引を安全にすることに関する。より具体的には、本発明は、スマートフォンを用いてリモートアプリケーションにアクセスしてユーザを認証する方法および装置に関する。
【背景技術】
【０００３】
コンピュータのシステムおよびアプリケーションに対するリモートアクセスが普及するにつれて、インターネットなどの公衆回線網によってアクセスされる取引の数と種類が劇的に増加した。この需要により、セキュリティ、特に、アプリケーションに遠隔にアクセスしている個人が自ら主張している個人であることを保障する方法、遠隔で行われている取引が正当な個人によって開始されたことを保障する方法、および取引データがアプリケーションサーバに受信される前に変更されていないことを保障する方法の必要性が強調されてきた。
【０００４】
近年、リモートアプリケーションにアクセスするために、ＰＣ（パーソナルコンピュータ）よりむしろスマートフォンを使用することが益々普及してきている。これは、ユーザがスマートフォンを使用中に、リモートアプリケーションと安全にインタラトすることを保障するための解決策が求められていることを意味する。元来ＰＣに使用するために開発された既存の解決策は、様々な理由でスマートフォンに使用するにはあまり満足できるものではない。動的なパスワードおよび署名を生成するソフトウェアアプリケーションのような純粋なソフトウェア解決策は、ＰＣと同様にスマートフォンが、益々あらゆる種類のマルウェアの標的になってきているので、攻撃に対して脆弱である。スマートカードまたはＵＳＢトークンのようなハードウェア解決策は、しばしばスマートフォンにサポートされていない特定の通信用インターフェース（スマートカードリーダ、ＵＳＢポート等）を必要とする。ユーザが変換されるべきデータ（ワン・タイム・パスワードなど）をコピーすることに依存する強力な認証トークンのような他のハードウェア解決策は、文字通りスマートフォンで手一杯のユーザにはしばしば煩わしいものとして認識される可能性がある。
この出願の発明に関連する先行技術文献情報としては、以下のものがある（国際出願日以降国際段階で引用された文献及び他国に国内移行した際に引用された文献を含む）。
（先行技術文献）
（特許文献）

（特許文献１）　米国特許第８，７８９，１４６号明細書
（特許文献２）　米国特許出願公開第２００９／００４８９７１号明細書
（特許文献３）　米国特許出願公開第２００９／０１４３１０４号明細書
（特許文献４）　米国特許出願公開第２０１０／０１７８８６８号明細書
（特許文献５）　米国特許出願公開第２０１２／００２３５６７号明細書
（特許文献６）　米国特許出願公開第２０１２／０１６７１９４号明細書
（特許文献７）　米国特許出願公開第２０１２／０２６５９８８号明細書
（特許文献８）　米国特許出願公開第２０１３／０３４３５４２号明細書
（特許文献９）　米国特許出願公開第２０１４／０１８１９５５号明細書
（特許文献１０）　米国特許第８，９４３，３１１号明細書
（特許文献１１）　米国特許第９，１０４，８５３号明細書
（特許文献１２）　国際公開第２０１３／０３４６８１号
（特許文献１３）　国際公開第２０１０／０４３９７４号
（非特許文献）
（非特許文献１）　Ｐａｒｄｉｓ　Ｐｏｕｒｇｈｏｍｉ；　Ｍａｎａｇｉｎｇ　ＮＦＣ　Ｐａｙｍｅｎｔ　Ａｐｐｌｉｃａｔｉｏｎｓ　ｔｈｒｏｕｇｈ　Ｃｌｏｕｄ　Ｃｏｍｐｕｔｉｎｇ；　ＩＥＥＥ；　Ｙｅａｒ：２０１２；　ｐａｇｅ：　７７２－７７７

【発明の概要】
【発明が解決しようとする課題】
【０００５】
スマートフォンを使用してユーザとリモートアプリケーションとの間で安全にインタラクションを行うための、安全で且つ便利な解決策が必要とされる。
【課題を解決するための手段】
【０００６】
本発明は、最近ほとんどのスマートフォンが他のデバイスと通信しデータを交換するＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ：近距離無線通信）技術をサポートしていることを発明者らが洞察したことに基づいている。
【０００７】
ＮＦＣは、例えば、非接触式スマートカードと通信するのに使用することができる。しかし、多くのスマートフォンのオペレーティングシステムは、低レベルのＡＰＩにアクセスを与え、ＮＦＣタグを用いてＮＦＣを介してコマンドおよび応答を直接交換することはない。代わりに、多くのスマートフォンは、いくつかの限定された高レベルのサービスのみをＮＦＣによってサポートしている可能性がある。
【０００８】
発明者らの別の洞察としては、ほとんどのスマートフォンがＮＦＣメモリタグの自動読み出しをサポートしていることである。
【０００９】
本発明の一観点は、ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保する認証装置を提供することである。
【００１０】
いくつかの実施形態では、該認証装置は、秘密鍵を格納するように構成されたメモリーコンポーネントと、前記秘密鍵と動的変数の値とを暗号化して組み合わせる（ｃｒｙｐｔｏｇｒａｐｈｉｃａｌｌｙ　ｃｏｍｂｉｎｉｎｇ）ことによって動的認証情報を生成するように構成されたデータ処理コンポーネントと、認証装置をＮＦＣ転送装置に接続する近距離無線通信（ＮＦＣ）インターフェースとを有することができ、前記認証装置は、ＮＦＣタグとして前記ＮＦＣ転送装置に提供され、ＮＦＣタグのデータコンテンツを読み出すＮＦＣ機構を用いて前記ＮＦＣ転送装置により読み出し可能である、前記ＮＦＣタグの第一のデータコンテンツに前記生成した動的認証情報を含めることにより、該動的認証情報を前記ＮＦＣ転送装置に利用可能にするように構成することができる。
【００１１】

いくつかの実施形態では、該認証装置は、１型、２型、３型または４型の近距離無線通信（ＮＦＣ）フォーラムに準拠したタグとして提供され、前記ＮＦＣ転送装置が、ＮＦＣフォーラムに準拠したタグからＮＤＥＦメッセージを読み出すＮＦＣ機構を用いて、前記生成された動的認証情報を読み出すために、該動的認証情報を前記認証装置のＮＤＥＦファイルのＮＤＥＦメッセージにおけるＮＦＣデータ交換フォーマット（ＮＤＥＦ）のレコードに含めることによって、該動的認証情報を前記ＮＦＣ転送装置に利用可能にするように構成することができる先に説明した実施任意の実施形態の認証装置を有することができる。

【００１２】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、さらに、クロックを有し、前記動的変数は前記クロックによって提供される時刻値に基づくことができる。

【００１３】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、前記動的変数は、前記メモリーコンポーネント内に格納され、特定のイベントが発生する毎に認証装置によって更新可能なイベント関連値に基づくことができる。いくつかの実施形態では、前記特定のイベントは、前記動的認証情報の前記生成と同時に発生する。いくつかの実施形態では、前記イベント関連値は、前記特定のイベントが発生する毎に前記認証によって単調増加または単調減少され得るカウンタを有することができる。

【００１４】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、前記秘密鍵と前記動的変数とを暗号化して組み合わせる工程は、前記動的変数に対称暗号化アルゴリズムを適用する工程を有し、前記対称暗号化アルゴリズムは前記秘密鍵でパラメータ化され、また、前記秘密鍵は前記生成された動的認証情報を認証するための機関と共有される。

【００１５】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、さらに、ユーザ識別子を格納し、ＮＦＣタグのデータコンテンツを読み出すＮＦＣ機構を用いて前記ＮＦＣ転送装置により読み出し可能である、前記ＮＦＣタグのデータコンテンツ内に前記動的認証情報を含めることにより、前記ユーザ識別子を前記ＮＦＣ転送装置に利用可能にするように構成することができる。

【００１６】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、さらに、前記ユーザからの入力を取得するためのユーザ入力インターフェースを有することができ、前記動的認証情報を生成する工程および／または前記生成された認証情報を前記ＮＦＣ転送装置に利用可能にする工程に対する条件として前記ユーザからの特定の入力を要求するように構成することができる。いくつかの実施形態では、前記ユーザ入力インターフェースはアクティベーションボタンを有することができ、前記特定の入力はユーザが前記アクティベーションボタンを押す工程を有することができる。いくつかの実施形態では、該認証装置は、さらに、前記ユーザ入力インターフェースによって前記ユーザによりアクティベートされるように構成することができ、該認証装置は、前記ユーザが前記ユーザ入力インターフェースを用いて該認証装置をアクティベートさせた後でのみ、ＮＦＣタグとして前記ＮＦＣ転送装置に提供される。

【００１７】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、さらに、前記ＮＦＣ転送装置に永久的または半永久的に固定されるように構成することができる。いくつかの実施形態では、さらに、該認証装置は、前記ＮＦＣ転送装置への取り付け用に接着コンポーネントを有することができる。いくつかの実施形態では、該認証装置は、前記ＮＦＣ転送装置を有するアクセス装置の保護シェルまたは保

護カバー内に含まれる。

【００１８】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、前記動的変数は外部データに基づいており、該認証装置は、さらに、ＮＦＣタグのデータコンテンツを更新するＮＦＣ機構を用いて前記ＮＦＣ転送装置により更新された、前記ＮＦＣタグの第二のデータコンテンツから外部データを抽出することによって前記ＮＦＣ転送装置から外部データを受信するように構成することができる。いくつかの実施形態では、該認証装置は、さらに、ユーザ入力インターフェースとユーザ出力インターフェースとを有し、前記外部データは取引データを有し、該認証装置は前記取引データをユーザに提示し、前記提示された取引データに対する前記ユーザによる承諾または拒否を前記入力インターフェースで取得し、前記ユーザが前記取引データを承諾した場合にのみ、前記動的認証情報を生成し、および／または、前記生成された動的認証情報を前記ＮＦＣ転送装置に利用可能にするように構成することができる。いくつかの実施形態では、前記ユーザ入力インターフェースは前記承諾を取得するための承諾ボタンと、前記拒否を取得するための拒否ボタンとを有することができる。いくつかの実施形態では、認証装置は、さらに、前記ＮＦＣ転送装置から前記外部データを受信した後、所定の期間、ＮＦＣタグとして前記ＮＦＣ転送装置に提供されず、前記ユーザが前記提示された取引データを承諾または拒否した後にのみ、前記ＮＦＣ転送装置に提供されるように構成することができる。

【００１９】

いくつかの実施形態では、該認証装置は、先に説明した任意の実施形態の認証装置を有することができ、さらに、ＮＦＣタグのデータコンテンツを更新するＮＦＣ機構を用いて前記ＮＦＣ転送装置により更新された、前記ＮＦＣタグの第三のデータコンテンツからパスワード値を抽出することにより、前記ＮＦＣ転送装置から該パスワード値を受信し、前記受信したパスワード値が正しいかどうかを検証（例えば、受信したパスワード値を前記のメモリ部品に格納され得るパスワード基準値と比較することにより）し、かつ、前記パスワード値を受信し、かつ該パスワード値が正しいと検証した場合にのみ、前記動的認証情報を生成し、および／または前記生成した認証情報を前記ＮＦＣ転送装置に利用可能にするように構成することができる。

【００２０】

本発明の別の態様では、ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保するシステムを提供する。いくつかの実施形態では、該システムは、先に説明した任意の実施形態の認証装置を有してよい。いくつかの実施形態では、該システムは、動的認証情報を生成する認証装置と、前記アプリケーションのサーバ部をホストし、前記認証装置によって生成された前記動的認証情報を検証するアプリケーションサーバと、前記ユーザが前記コンピュータ・ベース・アプリケーションへのアクセスを許可するためのアクセス装置であって、コンピュータネットワークによって前記アプリケーションサーバに接続され、前記認証装置から前記動的認証情報を取得し、かつ前記取得した動的認証情報を検証のために前記アプリケーションサーバに転送するように構成されているものである、前記アクセス装置とを有してよい。前記アクセス装置はＮＦＣ転送装置を有してよく、前記認証装置は、秘密鍵を格納するように構成されたメモリーコンポーネントと、前記秘密鍵と第一の動的変数の第一の値とを組み合わせることによって前記動的認証情報を生成するように構成されたデータ処理コンポーネントと、該認証装置を前記ＮＦＣ転送装置に接続する近距離無線通信（ＮＦＣ）インターフェースとを有してよい。また、前記認証装置は、ＮＦＣタグとして前記ＮＦＣ転送装置に提供され、ＮＦＣタグのデータコンテンツを読み出すＮＦＣ機構を用いて前記ＮＦＣ転送装置により読み出し可能である、前記ＮＦＣタグの前記第一のデータコンテンツ内に前記動的認証情報を含めることによって、前記生成された動的認証情報を前記ＮＦＣ転送装置に利用可能にするように構成することができ、前記アクセス装置は、ＮＦＣタグのデータコンテンツを読み出すＮＦＣ機構を用いて前記ＮＦＣ転送装置により読み出し可能である、前記ＮＦＣタグの

前記データコンテンツから前記動的認証情報を抽出することにより、前記動的認証情報を取得することができ、前記アプリケーションサーバは、前記認証装置により生成され、前記アクセス装置により取得および転送された前記動的認証情報を受信し、前記受信した動的変数を第二の動的変数の第二の値と共に暗号化アルゴリズムを用いて検証するように構成することができる。

【００２１】

いくつかの実施形態では、該システムは先に説明した実施形態のうちの任意のシステムであってもよく、前記秘密鍵と前記第一の動的変数の前記第一の値とを暗号化して組み合わせる工程は、前記第一の動的変数の前記第一の値に対称暗号化アルゴリズムを実行する工程を有し、前記対称暗号化アルゴリズムは前記秘密鍵でパラメータ化され、前記秘密鍵を前記認証装置と前記アプリケーションサーバとの間で共有することができ、前記アプリケーションサーバは前記秘密鍵のサーバコピーを用いて前記動的認証情報を検証することができる。

【００２２】

いくつかの実施形態では、該システムは先に説明した実施形態のうちの任意のシステムを有してよく、前記認証装置および前記アクセス装置は結合用の秘密（ｂｉｎｄｉｎｇ　ｓｅｃｒｅｔ）を共有することができ、前記アクセス装置は、さらに、前記ＮＦＣ転送装置が、ＮＦＣタグのデータコンテンツを更新するＮＦＣ機構を用いて前記ＮＦＣタグの第二のデータコンテンツを更新することにより前記結合用の秘密から導き出された結合値を前記認証装置に通信するように構成することができ、前記アクセス装置は、前記ＮＦＣ転送装置が、ＮＦＣタグのデータコンテンツを更新するためのＮＦＣ機構を用いて前記ＮＦＣ転送装置の第二のデータコンテンツを更新することにより、該結合値を前記認証装置に通信できるようにすることができる。また、前記認証装置は、ＮＦＣタグのデータコンテンツを更新するための前記ＮＦＣ機構を用いて前記ＮＦＣ転送装置によって更新された前記ＮＦＣタグの前記第二のデータコンテンツから前記結合値を抽出することにより、前記アクセス装置から前記結合値を受信し、前記結合用の秘密を用いて前記受信した結合値を検証し、前記受信した結合値が正しいと検証した場合にのみ、前記動的認証情報を生成し、および／または、前記生成した動的認証情報を前記ＮＦＣ転送装置に利用可能にするように構成することができる。

【００２３】

本発明のさらに別の態様は、ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保する方法を提供する。いくつかの実施形態では、該方法は、先に説明した任意の実施形態の認証装置またはシステムと共に使用することが可能である。いくつかの実施形態では、該方法は、ＮＦＣ転送装置に接続するための近距離無線通信（ＮＦＣ）インターフェースを有する認証装置で、第一の動的変数の第一の値と、前記認証装置に格納されかつ前記アプリケーションのサーバ部をホストするアプリケーションサーバと共有する秘密鍵とを暗号化して組み合わせることにより動的認証情報を生成する工程であって、該認証装置はＮＦＣタグとして前記ＮＦＣ転送装置に提示されるものである、前記生成する工程と、該認証装置で、ＮＦＣタグのデータコンテンツを読み出すＮＦＣ機構を用いて前記ＮＦＣ転送装置が読み出し可能である、前記ＮＦＣタグの第一のデータコンテンツに前記動的認証情報に含めることにより、前記生成した動的認証情報を前記ＮＦＣ転送装置に利用可能にする工程と、前記ＮＦＣ転送装置を有し、コンピュータネットワークによってアプリケーションサーバに接続されたアクセス装置を用いて、前記ユーザが前記コンピュータベースのアプリケーションにアクセスするのを許可する工程と、前記アクセス装置で、ＮＦＣタグのデータコンテンツを読み出す前記ＮＦＣ転送装置を用いてＮＦＣ転送装置により読み出された、前記ＮＦＣタグの前記データコンテンツから動的認証情報を抽出することにより、前記動的認証情報を取得する工程と、前記アクセス装置で、前記動的認証情報を前記アプリケーションサーバに転送する工程と、前記アプリケーションサーバで、前記認証装置で生成され、前記アクセス装置で取得された前記動的認証情報を受信する工程と、前記アプリケーションサーバで、前記受信した動的認証情報

を検証する工程とを有することができる。

【００２４】

いくつかの実施形態では、自身を標準のパッシブＮＦＣメモリタグとしてスマートフォンに提示する認証装置が提供される。いくつかの実施形態では、スマートフォンはＮＦＣフォーラムに準拠したデバイスでよい。いくつかの実施形態では、認証装置はＮＦＣフォーラムに準拠したタグを有することができ、またはＮＦＣフォーラムに準拠したタグとして自身を提示することができる。いくつかの実施形態では、ＮＦＣリーダ／ライタを用いてもよい。いくつかの実施形態では、スマートフォンはＮＦＣリーダ／ライタの役割を持つことができる。

【００２５】

いくつかの実施形態では、スマートフォンと認証装置との間の通信の態様は、例えば、ＮＦＣデジタルプロトコル技術仕様、または、ＮＦＣ活動技術仕様ならびに、例えば、ＩＳＯ／ＩＥＣ（国際標準化機構／国際電気標準会議）１８０９０２、ＩＳＯ／ＩＥＣ１８０００－３、ＩＳＯ／ＩＥＣ１４４４３（Ａ型またはＢ型）、および日本工業規格（ＪＩＳ）Ｘ６３１９－４などの他の仕様と標準などのＮＦＣフォーラム技術仕様のうちの少なくともいくつかで定義可能である。認証装置が自身をスマートフォン（または他のＮＦＣ転送装置）に提示する方法の他の態様および認証装置とスマートフォンとの間のデータ交換の他の態様は、例えば、ＮＦＣデータ交換フォーマット（ＮＤＥＦ）技術仕様、ＮＦＣフォーラム・タグ・タイプ技術仕様（ＮＦＣフォーラムの１型、２型、３型、４型タグオペエレーション仕様など）および記録型定義技術仕様（ＮＦＣ記録型定義（ＲＴＤ）技術仕様、ＮＦＣ統一資源識別子（ＵＲＩ）ＲＴＤ技術仕様、およびＮＦＣスマートポスタＲＴＤ技術仕様）、などのＮＦＣフォーラム技術仕様のうちの少なくともいくつかで定義可能である。いくつかの実施形態では、認証装置は標準ＮＦＣの１型タグとして自身を提示することができる。いくつかの実施形態では、認証装置は標準ＮＦＣの２型タグとして自身を提示することができる。いくつかの実施形態では、認証装置は標準ＮＦＣの３型タグとして提供されれる。いくつかの実施形態では、認証装置は標準ＮＦＣの４型タグとして提供される。

【００２６】

本明細書で、用語、ＮＦＣ転送装置は、適用できるＮＦＣ仕様で定義されるようなＮＦＣリーダ／ライタの手法でオペレーション可能なＮＦＣフォーラム装置または他の類似の装置のことを指すことができる。用語、ＮＦＣタグまたはＮＦＣメモリタグ（あるいは、単にタグまたはメモリタグ）は、ＮＦＣデジタルプロトコル技術仕様およびＮＦＣフォーラム・タグ・タイプ技術仕様で定義されるようなＮＦＣタグ、すなわち、パッシブ通信を介してＮＤＥＦをサポートする非接触式タグまたは（スマート）カードのことを指すことができる。パッシブ通信は一方の装置（ＮＦＣ転送装置）がＲＦ場（無線周波数場：ＲＦ場＝磁場）を生成し、第二の装置（ＮＥＣタグ）にコマンドを送信する通信モードであり、この第二の装置は、応答するために負荷変調を使用する（すなわち、この装置は、ＲＦ場を生成しないが、ＲＦ場から多かれ少なかれ電力を引き出す）。

【００２７】

認証装置（さらに、ＮＦＣトークン装置またはＮＦＣトークンと指されることがある）は、ワン・タイム・パスワード（さらに、ＯＴＰと指されることがある）を生成し、自身をＮＦＣタグとして提示し、かつ、ＮＦＣメモリタグのコンテンツに生成したワン・タイム・パスワードを追加するように構成することができる。例えば、いくつかの実施形態では、メモリタグのコンテンツは生成されたＯＴＰを有するＮＤＥＦレコードを有するＮＤＥＦメッセージを有することができる。メモリタグのコンテンツ（ＯＴＰを有することがある）は、ＮＦＣメモリタグのコンテンツを読み出すための標準プロトコルによってＮＦＣ転送装置（スマートフォンなど）が読み出すことができる。いくつかの実施形態では、ＮＦＣトークンは、ワン・タイム・パスワードを生成することができ、ＮＦＣトークンがスマートフォンのＮＦＣ場内に持ち込まれてアクティベートされたときにタグのコンテンツに生成したＯＴＰを追加することができる。いくつかの実施形態では、ＮＦＣトークン

は、ワン・タイム・パスワードを生成し、ＮＦＣ転送装置からメモリー・タグ・コンテンツを読み出す命令を受信するとオンザフライでタグのコンテンツに追加することができる。例えば、いくつかの実施形態では、ＮＦＣトークンはＮＦＣの４型のタグでよい。また、ＮＦＣトークンはＯＴＰを生成し、生成したＯＴＰを有するＮＤＥＦメッセージを生成し、ＮＤＥＦファイルを読み出すリード・バイナリー・コマンドを受信し、かつ応答する前にＮＤＥＦファイルに追加されたＮＤＥＦファイルのコンテンツを追加するように構成することができる。いくつかの実施形態では、ＮＦＣトークンは新しいワン・タイム・パスワードを生成し、スマートフォンがタグの現在のコンテンツを読み出した後にタグのコンテンツに新しいＯＴＰを追加する。

【００２８】

ＯＴＰの生成

いくつかの実施形態では、ＮＦＣトークンは、１若しくはそれ以上のデータ処理コンポーネントを有することができ、該１若しくはそれ以上のデータ処理コンポーネントに秘密鍵を格納するように構成することができる。ＮＦＣトークンは、１若しくはそれ以上のデータ処理コンポーネントをさらに有することができ、格納された秘密鍵と動的変数を暗号化して組み合わせることによってＯＴＰを生成するようにさらに構成することができる。いくつかの実施形態では、ＮＦＣトークンは、時間ベースのＯＴＰを生成するための動的変数の値を決定するために自身が使用することができる時刻値を生成するためのクロックを有することができる。他の実施形態では、ＮＦＣトークンは、特定のイベントの際に自身が更新するイベント関連値をメモリに格納し保持することができ、このイベント関連値を用いてイベントベースのＯＴＰを生成するための動的変数の値を決定することができる。例えば、いくつかの実施形態では、ＮＦＣトークンは、自身がワン・タイム・パスワードを生成するたびにイベント関連値を更新することができる。いくつかの実施形態では、イベント関連値はカウンタでよく、イベント関連値を更新することは、カウンタを増加させる工程（または、減少させる工程）を有することができる。いくつかの実施形態では、イベント関連値を更新する工程は、ＮＦＣトークンがイベント関連値の現在の値から計算することができる新しい値にイベント関連値の現在の値を置き換えるＮＦＣトークンを有することができる。いくつかの実施形態では、ＮＦＣトークンは、例えば、イベント関連値の現在の値にハッシュ関数を適用することによってイベント関連値の新しい値を計算することができる。

【００２９】

アプリケーションでの集積化

いくつかの実施形態では、スマートフォンおよびＮＦＣトークンは、ＮＦＣトークンがスマートフォンのＮＦＣ場に持ち込まれたときに自動的にアクティベートされることができ、スマートフォンはＮＦＣトークン（通常の標準パッシブＮＦＣタグとして自身を提示できる）の存在を検出することができ、その後すぐにスマートフォンはＯＴＰを含むタグのコンテンツを読み出すことができるように構成することができる。タグのコンテンツを読み出すと、スマートフォンは自動的にタグに関連するアプリケーション（ブラウザまたは例えばモバイル・バンキング・アプリケーションなどの）を開始し、アプリケーションにタグのコンテンツを渡すことができる。いくつかの実施形態では、タグのコンテンツは、ＯＴＰに加えてＮＦＣトークンに関連するユーザを特定するデータ要素を有することもできる。かかる場合には、タグのコンテンツは、スマートフォンによって自動的に立ち上げられることによって便利で安全な立ち上げおよびログインの経験をユーザに提供する、タグに関連したアプリケーションに、例えば、ユーザＩＤ（ユーザ識別子）および動的パスワード情報を自動的に提供することができる。例えば、いくつかの実施形態では、タグのコンテンツはＮＤＥＦメッセージを有することができ、ＮＤＥＦメッセージはユーザＩＤとＯＴＰでパラメータ化されるＵＲＩを有することができるＵＲＩタイプのＮＤＥＦレコードを有することができる。ＮＤＥＦメッセージを読み出すと、スマートフォンはブラウザアプリケーションを立ち上げブラウザにＵＲＩ（ユーザＩＤとＯＴＰでパラメータ化された）を渡すことができる。その際、ブラウザはＵＲＩに指定されたアプリケーション

サーバにＵＲＩのパラメータとしてユーザＩＤとＯＴＰを渡し、それによって、ユーザがＵＲＩによって指定されたアプリケーションに自動的にログインすることができる。例えば、いくつかの実施形態では、タグのコンテンツを読み出すＮＦＣリーダ装置は、自身がタグから読み出すレコードのコンテンツ（たとえば、ＯＴＰおよび／またはユーザＩＤを有してもよい）をアプリケーションまたはアプリに渡すＮＤＥＦメッセージ内のレコードタイプのＮＤＥＦレコードに基づいてアプリケーションまたはアプリを選択することができる。いくつかの実施形態では、レコードタイプは外部タイプでよい。アプリケーションまたはアプリは、例えば、モバイル・バンキング・アプリを有することができる。

【００３０】

ユーザによるＮＦＣトークンの明示的なアクティベーション

いくつかの実施形態では、ＮＦＣトークンは初期設定ではＯＴＰをＮＦＣ転送装置に利用可能にせず、ユーザの明示的なアクションの後にのみ利用可能にする。例えば、いくつかの実施形態では、ＮＦＣトークンはユーザ入力インターフェース（ボタンなど）を有することができ、また、ユーザがユーザ入力インターフェースを用いて（例えば、ボタンを押すことによって）ＯＴＰが利用可能にされるべきだと指示したときのみＯＴＰを利用可能にするようにＮＦＣトークンを構成することができる。

【００３１】

いくつかの実施形態では、ＮＦＣトークンは生成したＯＴＰをＮＤＥＦファイルのＮＤＥＦレコード内で利用可能にするように構成することができ、また、ＯＴＰを自動的に生成し、ユーザがユーザ入力インターフェースを用いてＮＦＣトークンにそのように指示したときにＮＤＥＦファイルを新しいＯＴＰ値で更新するように該トークンを構成することができる。

【００３２】

いくつかの実施形態では、初期設定でのＮＦＣトークンは、スマートフォンのＮＦＣ場内に持ち込まれたときでもスマートフォンにＮＦＣタグを提示しない。いくつかの実施形態では、ＮＦＣトークンは、ＮＦＣトークンがスマートフォンに自身をＮＦＣタグとして提示するように促すユーザの明示的な物理的アクションを必要とする。例えば、いくつかの実施形態では、ＮＦＣトークンはユーザ入力インターフェースを有することができ、また、ユーザが該ユーザ入力インターフェースを用いてＮＦＣトークンがそうするように指示したときにのみ自身をＮＦＣタグとして提示するようにＮＦＣトークンを構成することができる。例えば、いくつかの実施形態では、ＮＦＣトークンはアクティベーションボタンを有することができる。また、ＮＦＣトークンはユーザがアクティベーションボタンを押した後で自身をＮＦＣタグとしてスマートフォンに提示するように構成することができる。いくつかの実施形態では、ＮＦＣトークンは、ＮＦＣトークンのＮＦＣアンテナが、ＮＦＣトークンの他のコンポーネントから電気絶縁されており、ユーザがアクティベーションボタンを押したときにＮＦＣトークンがＮＦＣタグとしてスマートフォンに知覚できるようになるとＮＦＣトークンの他のコンポーネントに接続可能になるように構成することができる。これは、一方ではユーザがアクティベーションボタンを明示的に押したときのみＮＦＣタグのコンテンツ（ＯＴＰおよびユーザＩＤを有することができる）が読み出しのためにアクセス可能になり、ユーザが知らないうちにある悪意のアプリケーションによってＯＴＰおよびユーザＩＤがこっそり読み取られることが防止される。また、これには、ユーザがＮＦＣトークンをアクティベートするためにＮＦＣ場の内外に移動させてＮＦＣトークンに新しいＯＴＰを生成させスマートフォンにＮＦＣタグのコンテンツを再度読み出す必要がないという追加の利点もある。ユーザがＮＦＣトークンをスマートフォンに永久的に取り付け続けることができＮＦＣトークンの行方を追い続ける必要がないことを意味する。アクティベーションボタンのさらに別の利点は、ユーザがＮＦＣトークンのアクティベーションボタンを１回だけ押してアプリケーションを立ち上げそのアプリケーションに安全にログインできるようになることである。

【００３３】

取り引きデータに署名すること

いくつかの実施形態では、ＮＦＣトークンを、ＮＦＣトークンに格納された秘密鍵とＮＦＣトークンがスマートフォンから受信できる外部データに基づいた動的変数と暗号化して組み合わせることによってＯＴＰまたは署名を生成できるように構成することができる。本明細書で使用されるとき動的変数という用語は、ＯＴＰを指すことができ、または、秘密鍵と外部データに基づいた動的変数とを暗号化して組み合わせることによって生成される署名を指すことができる。外部データは、例えば、チャレンジ（アプリケーションによって提供され得る）または取り引きデータを有することができる。いくつかの実施形態では、スマートフォン（またはＮＦＣを用いてデータ／情報を読み出しおよび／または書込むことができるＮＦＣ転送装置を有する他の装置）はＮＦＣメモリタグのコンテンツを更新するための標準の機構を用いてこれらの外部データをＮＦＣトークンに転送することができる。例えば、スマートフォンまたは他の装置はＮＦＣ転送装置を有することができ、ＮＦＣトークンのＮＤＥＦファイル内のＮＤＥＦレコードを外部データで更新することができる。いくつかの実施形態では、ＮＦＣトークンは、例えば、チャレンジまたは取り引きデータを有する外部データを受信した後で受信したチャレンジに対する応答または取り引きデータに関する署名を生成することができる。いくつかの実施形態では、ＮＦＣトークンは、メモリタグのコンテンツを生成された応答または署名で更新するように構成することができる。いくつかの実施形態では、ＮＦＣトークンは、スマートフォンに提示してスマートフォンにメモリタグの更新されたコンテンツを読み出すように促すメモリタグとの接続を切り、また、それに再接続する。すなわち、いくつかの実施形態では、ＮＦＣトークンは、外部データを受信した後、ある時間の間自身をＮＦＣタグとして提示するのを止めるように構成することができる。その時間が経過した後、ＮＦＣトークンは、ＮＦＣトークンがその間に外部データを介して生成した署名でそのＮＦＣトークンが更新され得るＮＤＥＦファイルにＮＦＣタグとして自身を再度提示することができる。いくつかの実施形態では、ＮＦＣトークンがこのようにＮＦＣ転送装置またはスマートフォンによりＮＦＣタグとして見られることができない間隔は２秒未満である。いくつかの実施形態では、この時間間隔は１秒未満である。いくつかの実施形態では、この時間間隔は０．５秒未満である。いくつかの実施形態では、この時間間隔は０．１秒未満である。いくつかの実施形態では、この時間間隔は、ＮＦＣ転送装置の近接場内でＮＦＣ転送装置がＮＦＣタグが取り外されその後再度提示されたことを認識するであろうことを保証するためにＮＦＣタグの取り外しと（再）挿入との間に経過しなければならない最少の時間間隔である。

【００３４】

いくつかの実施形態では、ＮＦＣトークンは、生成した応答または署名を外部データに基づかないＯＴＰではないタグコンテンツの別の部分に置くように構成することができる。いくつかの実施形態では、スマートフォンは自身がＮＦＣトークンに書込む外部データにセッションＩＤを含むことができ、また、ＮＦＣトークンはメモリタグを更新する生成した応答または署名と一緒にこのセッションＩＤを含むことができる。いくつかの実施形態では、ＮＦＣトークンは、生成した応答または署名と、任意選択で、セッションＩＤ、ユーザＩＤまたは別のデータ識別要素と（例えば、生成した応答または署名、および、任意選択でセッションＩＤ、ユーザＩＤまたは他のデータ識別要素）を、特殊なヘルパーアプリケーションに関連したメモリタグ内に有することができる。この特殊なヘルパーアプリケーションは、ユーザにアクセスされるモバイルアプリケーションに関連した認証サーバに該メモリタグ内に有されたデータを転送するように構成される。

【００３５】

いくつかの実施形態では、ＮＦＣ転送装置またはスマートフォンの第一のアプリケーションまたはアプリはメモリタグを外部データで更新することができる。ＮＦＣトークンは、これらの外部データを使用して動的認証情報を生成し、生成した動的認証情報で（例えば、ＮＦＣトークンのＮＤＥＦファイルのＮＤＥＦメッセージ内のＮＤＥＦレコードを更新することによって）メモリタグのコンテンツを更新することができる。ＮＦＣ転送装置またはスマートフォンは、その後、更新したコンテンツの読み出しその読み出したコンテンツを、ＮＦＣ転送装置が読み出した更新情報（例えば、ＮＤＥＦメッセージ内のＮＤＥ

ＦタイプのＮＤＥＦレコードなど）に基づいて選択したＮＦＣ転送装置上の第二のアプリケーションまたはアプリに渡すことができる。

【００３６】

いくつかの実施形態では、ＮＦＣトークンは、署名ボタンを有することができ、ユーザが該署名ボタンを押して署名を生成し、および／または署名をスマートフォンまたはＮＦＣ転送装置が読み出すことができるようにすることができる。いくつかの実施形態では、署名ボタンがＯＴＰ生成用のアクティベーションボタンと同じでよい。いくつかの実施形態では、署名ボタンがアクティベーションボタンと異なってもよい。

【００３７】

いくつかの実施形態では、ＮＦＣトークンはユーザ入力インターフェース（ディスプレイなど）を有することができ、また、ＮＦＣトークンは署名すべき外部データをユーザに提示し、ユーザが署名を生成しおよび／またはスマートフォンまたはＮＦＣ転送装置によって該署名が読み取られることができるようにする前にユーザが提示された外部データを承認するのを待つように構成することができる。いくつかの実施形態では、ＮＦＣトークンは、ユーザ入力インターフェースによる外部データのユーザ承認を取得するように構成することができる。いくつかの実施形態では、ＮＦＣトークンは、ユーザ入力インターフェースによる外部データのユーザ拒否を取得するように構成することができ、また、したがって、ＮＦＣトークンは、メモリタグのコンテンツを更新することによってユーザの拒否を伝える（例えば、ＮＦＣトークンのＮＤＥＦファイルのＮＤＥＦメッセージのＮＤＥＦレコード内に拒否の指示を含めることによって）ように構成することができる。いくつかの実施形態では、ＮＦＣトークンは、ユーザが承諾を示すアクティベーションボタンおよびユーザが拒否を示す拒否ボタンを有することができる。

【００３８】

ピンエントリー

いくつかの実施形態では、ＮＦＣトークンは、個人識別番号（ＰＩＮ）および／またはパスワードを検証するように構成することができ、例えば署名または外部データへの応答を生成するために正しいＰＩＮおよび／またはパスワードが提供されることを要求することができる。いくつかの実施形態では、ユーザはスマートフォン上のＰＩＮおよび／またはパスワードに入ることができ、スマートフォンは例えば外部データと一緒にまたは外部データの一部として該ＰＩＮおよび／またはパスワードをＮＦＣトークンに提供することができる。例えば、いくつかの実施形態では、検証すべきＰＩＮまたはパスワードはＮＦＣ転送装置（例えば、スマートフォン内のＮＦＣ転送装置）によって、ＮＦＣトークンのＮＤＥＦファイル内のＮＤＥＦレコードを更新するＮＦＣ転送装置によるＮＦＣトークンに通信されることができる。いくつかの実施形態では、ＮＦＣトークンは１若しくはそれ以上のメモリーコンポーネントを有することができ、該１若しくはそれ以上のメモリーコンポーネント内にＰＩＮ参照値および／またはパスワード参照値を格納するように構成することができる。また、ＮＦＣトークンは、例えばスマートフォンから受信したＰＩＮおよび／またはパスワードを格納したＰＩＮ参照値および／またはパスワード参照値と比較することによって検証するように構成することができる。いくつかの実施形態では、ＰＩＮは一連の１０進法数字を有することができる。いくつかの実施形態では、パスワードは英数字文字を有することができる。

【００３９】

いくつかの実施形態では、ＮＦＣトークンは、正当なユーザの生物測定的測定を検証するように構成することができ、例えば、署名または外部データに対する応答を生成するためにＮＦＣトークンに関連した正当なユーザの生物測定的測定が提供されることを要求することができる。いくつかの実施形態では、スマートフォン（またはＮＦＣ転送装置を有する他の装置）はユーザの生物測定的測定を取得する（例えば、スマートフォン上の生物測定センサを用いることによって）ことができ、スマートフォンは例えば外部データと一緒にまたはその一部として該生物測定的測定をＮＦＣトークンに提供することができる。いくつかの実施形態では、ＮＦＣトークンは、１若しくはそれ以上のメモリーコンポーネ

ントを有することができ、該１若しくはそれ以上のメモリーコンポーネント内に生物測定的参照データを格納するように構成することができる。また、ＮＦＣトークンは、受信した生物測定的測定を格納した生物測定的参照データと比較することによって例えばスマートフォンから受信した生物測定的測定を検証するように構成することができる。

【００４０】

ＮＦＣトークンのＮＦＣ転送装置への結合

いくつかの実施形態では、ＮＦＣトークンは、特別なＮＦＣ転送装置に結合させることができる。いくつかの実施形態では、ＮＦＣ読み出し装置とＮＦＣトークンは、ＮＦＣトークンがＮＦＣ転送装置と共に使用される最初に結合させることができる。いくつかの実施形態では、結合はＮＦＣトークンとＮＦＣ読み出し装置に共有された結合用の秘密を用いてなされることができる。いくつかの実施形態では、ＮＦＣ読み出し装置は、結合用の秘密の値を一回（例えば、ＮＦＣトークンがＮＦＣ転送装置に最初に使用されたとき）受信することができ、将来の使用のために結合用の秘密を格納することができる。いくつかの実施形態では、ＮＦＣトークンは、結合用の秘密の正しい値が署名またはＯＴＰなどの動的認証情報を生成するための条件としてＮＦＣトークンに提供（例えば、ＰＩＮまたはパスワード値が提供されることができた上記した方法と同じ方法で）されることを要求することができ、また、結合用の秘密が正しいかどうかを検証することができる。いくつかの実施形態では、ＮＦＣ読み出し装置は、結合用の秘密を暗号化アルゴリズムと共に使用して暗号の結合値を生成し、ＮＦＣ転送装置は、生成した結合値をＮＦＣトークンに提供する（例えば、ＰＩＮまたはパスワード値が提供されることができた上記した方法と同じ方法で）ことができ、ＮＦＣトークンは結合値が暗号的に正しいかどうかを検証し、結合値の暗号的な正しさを動的認証情報を生成するための条件として使用することができる。

【００４１】

フォームファクタ

いくつかの実施形態では、ＮＦＣトークンは、ユーザがＮＦＣトークン（または、ＮＦＣトークンを有する対象）をアクセス装置から外す明示的な行動をとるまでＮＦＣトークンをアクセス装置に固定したままにするようにＮＦＣ読み出し装置（例えば、スマートフォン）を有するアクセス装置に永久的または半永久的にＮＦＣトークンを容易に固定可能にするフォームファクタを有することができる。例えば、いくつかの実施形態では、ＮＦＣトークンは、ＮＦＣトークンをアクセス装置に差し込みまたは貼り付け可能にする接着部を有することができる。いくつかの実施形態では、ＮＦＣトークンは最大厚が２ｍｍでよい。いくつかの実施形態では、ＮＦＣトークンは最大厚が１ｍｍでよい。いくつかの実施形態では、ＮＦＣトークンは最大幅が５４ｍｍ、最大長が８６ｍｍでよい。いくつかの実施形態では、ＮＦＣトークンは最大幅と最大長が３ｃｍでよい。いくつかの実施形態では、ＮＦＣトークンはスマートフォンに取り付け可能なステッカ内に有することができる。いくつかの実施形態では、ＮＦＣトークンはスマートフォンのシェルまたは保護カバー内に有することができる。いくつかの実施形態では、ＮＦＣトークンはポータブルでよい。いくつかの実施形態では、ＮＦＣは重さ１０グラム未満でよい。

【００４２】

いくつかの実施形態では、ＮＦＣトークンは、例えば、ＮＦＣトークンがスマートフォンまたはＮＦＣ転送装置を有する他の装置のＮＦＣ場から（十分な）電力を得ることができない場合にＮＦＣトークンに電力を供給するための自律的な電気エネルギー源を有することができる。いくつかの実施形態では、該自律的な電気エネルギー源は再充電可能なものでよい。いくつかの実施形態では、ＮＦＣトークンはスマートフォンまたはＮＦＣ転送装置を有する他の装置のＮＦＣ場から取得したエネルギーを使用して自律的な電気エネルギー源を再充電するように構成することができる。いくつかの実施形態では、ＮＦＣトークンはバッテリーを有することができる。いくつかの実施形態では、該バッテリーは再充電可能でよい。いくつかの実施形態では、ＮＦＣトークンはスマートフォンまたはＮＦＣ転送装置を有する他の装置のＮＦＣ場から取得したエネルギーを使用してバッテリーを再充電するように構成することができる。いくつかの実施形態では、ＮＦＣトークンはＮＦ

Ｃトークンのエレクトニクスに電気エネルギーを供給するためのコンデンサを有することができる。いくつかの実施形態では、ＮＦＣトークンはスマートフォンまたはＮＦＣ転送装置を有する他の装置のＮＦＣ場から取得したエネルギーを使用して該コンデンサを再充電することができる。

【００４３】

本発明の前記その他の目的および利点は、添付図面に例示する下記の、より詳細な本発明の実施形態の記載から明らかである。

【図面の簡単な説明】

【００４４】

【図１】図１は、本発明の一態様による例示的な装置を概略的に示す図である。

【図２】図２は、本発明の一態様による例示的なシステムを概略的に示す図である。

【図３】図３は、本発明の態様によるユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保するための方法のフローチャートである。

【発明を実施するための形態】

【００４５】

本発明のいくつかの実装形態を以下に説明する。具体的な実装形態が説明されるが、この説明は説明の目的のためだけになされることを理解すべきである。関連する技術分野の当業者なら、他の構成要素および構成が本発明の精神と範囲から離れることなく使用できることが分かるであろう。

【００４６】

図１は本発明の一態様による発明の例示的装置（１００）を概略的に示す。いくつかの実施形態では、該装置（１００）は本明細書の他の箇所で説明した認証装置および／またはＮＦＣトークンのうちの任意のものを有することができる。

【００４７】

図示した装置は、ＮＦＣアンテナ／インターフェース（１１０）と、秘密鍵を格納、およびＮＦＣメモリタグのコンテンツを（少なくとも一時的に）格納するための１若しくはそれ以上のコンポーネント（１２０）と、１若しくはそれ以上の処理コンポーネント（１３０）と、アクティベーションボタン（１４０）と、署名ボタン（１５０）とを有することができる。いくつかの実施形態では、該装置はＯＴＰおよび／または署名または外部データへの応答を生成し、上記で説明したＮＦＣトークンとして機能するように構成することができる。

【００４８】

いくつかの実施形態では、該装置は、スマートフォン（またはＮＦＣ転送装置を有する他の装置）にＮＦＣメモリタグとして提供されるように構成することができる。いくつかの実施形態では、該装置は１若しくはそれ以上のメモリーコンポーネントに格納された秘密鍵を使用するワン・タイム・パスワードを生成するように構成することができ、また、該装置は、生成したワン・タイム・パスワードを含むようにメモリタグのコンテンツを追加しまたは更新するように構成することができる。いくつかの実施形態では、該装置は標準ＮＦＣメモリー・タグ・オペレーションを用いてワン・タイム・パスワードを有するメモリタグのコンテンツを読み出し可能に構成することができる。

【００４９】

いくつかの実施形態では、１若しくはそれ以上の処理コンポーネントはワン・タイム・パスワードを生成するように構成することができる。いくつかの実施形態では、１若しくはそれ以上の処理コンポーネントは秘密鍵とワン・タイム・パスワードを生成するための動的変数を用いてパラメータ化された暗号計算を実行するように構成することができる。いくつかの実施形態では、暗号計算は、例えば、秘密鍵と動的変数を用いてパラメータ化された対称暗号化アルゴリズムを実行することを含む。いくつかの実施形態では、この暗号計算はＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ：高度暗号化標準）などの対称暗号化／復号化アルゴリズムまたはＨＭＡＣ（Ｈａｓｈ－ｂａｓｅｄ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ：ハッシュベースのメッ

セージ認証コード）などの鍵付きハッシュアルゴリズムを含む。
【００５０】
いくつかの実施形態では、該装置はＮＦＣトークンが時刻ベースのＯＴＰを生成するのに使用することができる時刻値を提供することができるクロック（１６０）を有することができる。
【００５１】
図２は、本発明の一態様による例示的なシステム（２００）を概略的に示す。いくつかの実施形態では、該システムは、ＮＦＣトークン（２１０）と、クライアント装置（２２０）と、アプリケーションサーバ（２３０）とを有することができる。
【００５２】
いくつかの実施形態では、ＮＦＣトークン（２１０）は本明細書の他の箇所で記載したＮＦＣトークンのうちの任意のものを有することができる。
【００５３】
いくつかの実施形態では、クライアント装置（２２０）はパーソナル通信装置を有することができる。いくつかの実施形態では、該クライアント装置はスマートフォン（または、タブレットなどのＮＦＣ転送装置を有する他の装置）を有することができる。いくつかの実施形態では、クライアントアプリケーションは、ユーザ（２４０）によりインターフェースによって操作されると共にインターフェースに対して操作されるように構成することができる。いくつかの実施形態では、クライアント装置はユーザに情報を提供するためのユーザ出力インターフェース（ディスプレイなど）を有することができる。いくつかの実施形態では、クライアント装置はユーザから入力および情報を受信するためのユーザ入力インターフェース（キーボードまたはタッチスクリーンなど）を有することができる。いくつかの実施形態では、クライアント装置は、例えば、ユーザがクライアント装置のユーザ入力インターフェースおよびユーザ出力インターフェースを用いることによってアプリケーションとインタラクトするために使用することができるクライアントアプリケーションおよびクライアントアプリ（ｃｌｉｅｎｔ　ａｐｐ）を動作させるように構成することができる。いくつかの実施形態では、クライアントアプリのクライアントアプリケーションはウェブベースのアプリケーションとインタラクトするためのウェブブラウザを有することができる。
【００５４】
いくつかの実施形態では、アプリケーションサーバ（２３０）は１若しくはそれ以上のコンピュータを有することができる。いくつかの実施形態では、該アプリケーションサーバは、アプリケーションのサーバ部をホストするように構成することができる。該アプリケーションは、例えば、ウェブ・バンキング・アプリケーションを有することができる。いくつかの実施形態では、クライアント装置およびアプリケーションサーバは、例えば、インターネットおよび／または無線データネットワークおよび／または電話ネットワークなどのコンピュータネットワーク（２５０）および／または通信ネットワーク（２５０）を介して接続することができる。
【００５５】
図３は、本発明の一態様による、ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保するための工程のフローチャート３００を示す。
【００５６】
工程３１０では、動的認証情報が認証装置によって生成される。該動的認証情報は認証装置１００によって生成されてよい。該認証装置は、近距離無線通信（ＮＦＣ）転送装置（例えば、クライアント装置２２０などのアクセス装置の）と接続するための近距離無線通信（ＮＦＣ）インターフェースを含む。該認証装置１００は、第一の動的変数の第一の値と認証装置１００（例えば、メモリー１２０内）に格納された秘密鍵とを暗号化して組み合わせることによって、（例えば、データ処理コンポーネント１３０を用いて）動的認証情報を生成することができる。認証装置１００内の秘密鍵は、コンピュータベースのアプリケーションのサーバ部をホストするアプリケーションサーバ（例えば、アプリケーシ

ョンサーバ２３０）と共有されてよい。いくつかの実施形態では、認証装置１００はＮＦＣタグとしてＮＦＣ転送装置に提供される。

【００５７】

工程３２０では、動的認証情報が認証装置によってＮＦＣ転送装置に利用可能になる。該ＮＦＣ転送装置はＮＦＣを介して通信可能な装置（例えば、クライアント装置２２０／スマートフォン／タブレット／読み出し装置、またはかかる装置内のコンポーネント）でよい。該認証装置は、ＮＦＣ転送装置がＮＦＣタグのデータコンテンツを読み出すためのＮＦＣ機構を使用して読み出すことができるＮＦＣタグの第一のデータコンテンツ内に（例えば工程３１０で）生成した動的認証情報を含めることによって該認証情報をＮＦＣ転送装置に利用可能にすることができる。

【００５８】

工程３３０では、アクセス装置が動的認証情報を取得する。該アクセス装置はＮＦＣ転送装置を有するスマートフォンなどの装置でよい。アクセス装置は、コンピュータネットワークによってコンピュータベースのアプリケーションのサーバ部をホストするアプリケーションサーバに接続することができる。アクセス装置は、ＮＦＣタグのデータコンテンツを読み出すためのＮＦＣ機構を用いてＮＦＣ転送装置が読み出すＮＦＣタグのデータコンテンツから動的認証情報を抽出することによって動的認証情報を取得することができる。

【００５９】

工程３４０では、該アクセス装置が動的認証情報をアプリケーションサーバに転送し、該アプリケーションサーバは、認証装置によって生成され、アクセス装置によって取得された動的認証情報を受信する。

【００６０】

工程３５０では、該アプリケーションサーバは、受信した動的認証情報を検証する。アプリケーションサーバは、例えば、動的認証情報を生成するのに使用された動的変数の値を決定しかつ、認証装置と共有される秘密鍵を用いて、例えば、参照値を生成し、次に受信された動的認証情報と該参照値を比較することによって動的認証情報を検証するように構成することができる。

【００６１】

工程３６０では、ユーザがアクセス装置を使用してコンピュータベースのアプリケーションへのアクセスを許可される。該ユーザは、アプリケーションサーバが受信した動的認証情報を検証したことに応答してコンピュータベースのアプリケーションへのアクセスの許可を受けることができる。

【００６２】

多数の実装形態を説明してきたが、様々な修正を加えることができることは理解されるであろう。例えば、１若しくはそれ以上の実装形態の要素が組み合わされ、削除され、修正され、または補足されてさらなる実装形態を形成することができる。したがって、他の実装形態も添付の請求項の範囲内である。加えて、数個の実装形態のうちのただ１つに対してだけ特別な特徴が開示される一方で、かかる特徴は、任意の所与のまたは特別なアプリケーションに望ましいかまたは有利になり得るような他の実装形態の１若しくはそれ以上の他の特徴と組み合わされてよい。様々な実施形態が上記で説明されてきたが、これらは説明のためだけに提示されたのであり、限定するものではない。もちろん、請求された主題を説明するために、コンポーネントまたは方法のすべての考えられる組み合わせを説明することは不可能であるが、しかし、当技術分野の当業者なら、多くのさらなる組み合わせおよび置き換えが可能であることを理解することができる。すなわち、本明細書の教示の幅および範囲は、上記で説明した例示的な実施形態のいかなるものにも限定されるべきでなく、以下の特許請求の範囲およびそれらの均等物によってのみ規定されるべきである。

【図１】

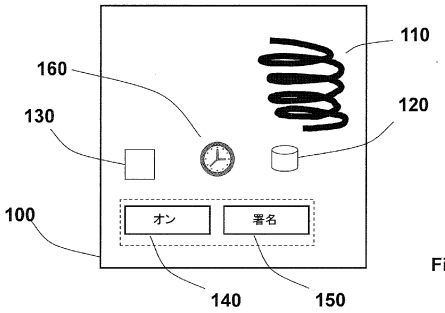

Figure 1

【図２】

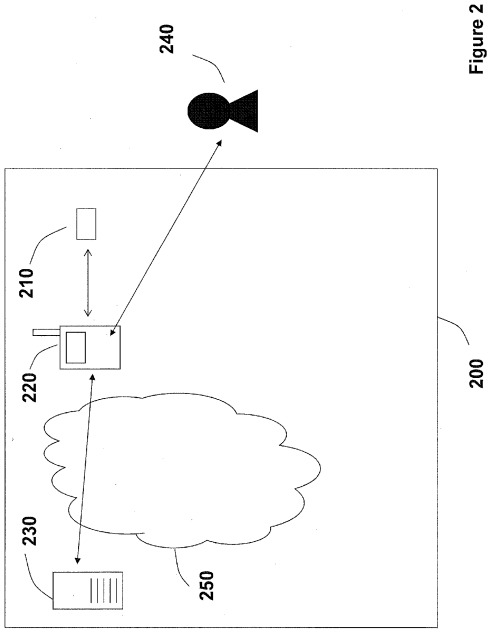

Figure 2

【図３】

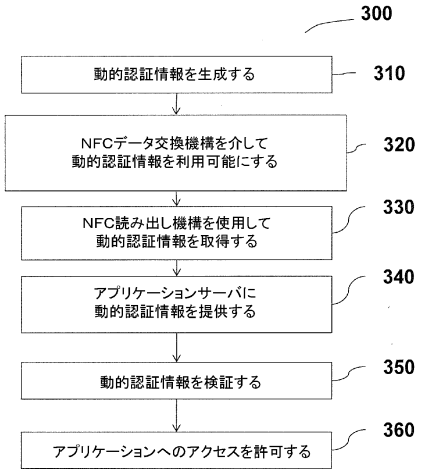

Figure 3

フロントページの続き

(56)参考文献 国際公開第２０１３／０３４６８１（WO，Ａ１）
特開２０１２－０７３９５５（ＪＰ，Ａ）
特開２００８－１０４１６９（ＪＰ，Ａ）
国際公開第２０１０／０４３９７４（WO，Ａ１）
米国特許第０８４１２９２８（ＵＳ，Ｂ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／３５