(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2008-131652
(P2008-131652A)
(43)公開日　平成20年6月5日(2008.6.5)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	G09C	1/00	640D	

審査請求 有　請求項の数 28　ＯＬ　（全 22 頁）

(21)出願番号　特願2007-300825 (P2007-300825)
(22)出願日　平成19年11月20日 (2007.11.20)
(31)優先権主張番号　06124600.5
(32)優先日　平成18年11月22日 (2006.11.22)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　500043574
リサーチ　イン　モーション　リミテッド
Ｒｅｓｅａｒｃｈ　Ｉｎ　Ｍｏｔｉｏｎ　Ｌｉｍｉｔｅｄ
カナダ国　エヌ２エル　３ダブリュー８　オンタリオ，　ウォータールー，　フィリップ　ストリート　２９５
２９５　Ｐｈｉｌｌｉｐ　Ｓｔｒｅｅｔ，　Ｗａｔｅｒｌｏｏ，　Ｏｎｔａｒｉｏ　Ｎ２Ｌ　３Ｗ８　Ｃａｎａｄａ
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明

最終頁に続く

(54)【発明の名称】モバイルユーザ証明書の共有知識を用いる安全な記録プロトコルのためのシステムおよび方法

(57)【要約】
【課題】モバイルユーザ証明書の共有知識を用いる安全な記録プロトコルのための方法を提供すること。
【解決手段】サーバとクライアントとを有するシステムにおける安全な記録プロトコルのための方法であって、モバイルユーザ証明書をサーバキージェネレータ、クライアントキージェネレータへの入力として利用するステップであって、該モバイルユーザ証明書は、サーバとクライアントとの双方に既知である、ステップと、該サーバキージェネレータを利用して、該モバイルユーザ証明書入力に基づく１つまたは２つの公開キー－秘密キーのペアを生成するステップと、該クライアントキージェネレータを利用して、該モバイルユーザ証明書入力に基づく１つまたは２つの公開キー－秘密キーのペアを生成するステップと、該秘密キーのうちの一つを用いて、署名されたメッセージを送信するステップとを包含する、方法。
【選択図】図１

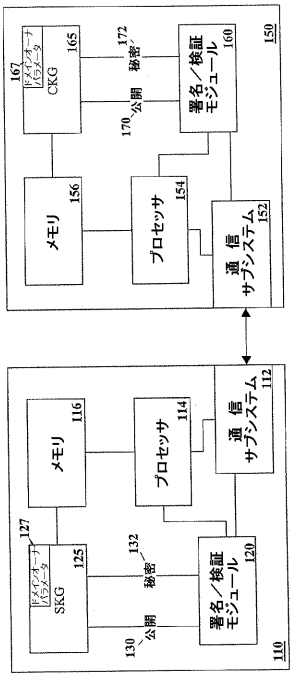

FIG. 1

【特許請求の範囲】
【請求項１】
サーバキージェネレータ（１２５；２２５）を有するサーバ（１１０；２１０）と、クライアントデバイスキージェネレータ（１６５；２６５）を有するクライアントデバイス（１５０；２５０）とを有するシステムにおける安全な記録プロトコルのための方法であって、
モバイルユーザ証明書を該サーバキージェネレータ（１２５；２２５）、該クライアントデバイスキージェネレータ（１６５；２６５）への入力として利用するステップであって、該モバイルユーザ証明書は、該サーバ（１１０；２１０）と該クライアントデバイス（１５０；２５０）との双方に既知である、ステップと、
該サーバキージェネレータ（１２５；２２５）を利用して、該モバイルユーザ証明書入力に基づく１つまたは２つの公開キー－秘密キーのペアを生成するステップと、
該クライアントデバイスキージェネレータ（１６５；２６５）を利用して、該モバイルユーザ証明書入力に基づく１つまたは２つの公開キー－秘密キーのペアを生成するステップと、
該秘密キーのうちの一つを用いて署名されたメッセージを、送信するステップと
を包含する、方法。
【請求項２】
前記モバイルユーザ証明書は、パスワードである、請求項１に記載の方法。
【請求項３】
前記入力は、安全なハッシュ関数を用いて、ノンスを用いてハッシュされたパスワードである、請求項１または請求項２に記載の方法。
【請求項４】
前記入力は、前記クライアントデバイスと前記サーバとによって共有されるパラメータを用いるパスワード変換である、請求項１～請求項３のいずれか１項に記載の方法。
【請求項５】
前記サーバキージェネレータ（１２５；２２５）およびクライアントデバイスキージェネレータ（１６５；２６５）は、１つの公開キー－秘密キーのペアのみを生成する、請求項１～請求項４のいずれか１項に記載の方法。
【請求項６】
前記サーバキージェネレータ（１２５；２２５）およびクライアントデバイスキージェネレータ（１６５；２６５）は、クライアントデバイスの公開キー－秘密キーのペアおよびサーバの公開キー－秘密キーのペアを生成する、請求項１～請求項４のいずれか１項に記載の方法。
【請求項７】
前記サーバキージェネレータ（１２５；２２５）およびクライアントデバイスキージェネレータ（１６５；２６５）は、前記クライアントデバイス秘密キーまたは前記サーバ秘密キーを隠す、請求項６に記載の方法。
【請求項８】
前記送信するステップは、さらに、前記公開キーのうちの一つを用いて、メッセージを暗号化する、請求項１～請求項７のいずれか１項に記載の方法。
【請求項９】
同一の入力を利用すると、前記生成するステップが前記クライアントデバイス（１５０；２５０）上で実行されるときは、該生成するステップが前記サーバ（１１０；２１０）上で実行されるときと、同一の公開キー－秘密キーのペアを生成する、請求項１～請求項８のいずれか１項に記載の方法。
【請求項１０】
前記利用するステップは、さらに、セッション識別子を組み込んで、入力を生成する、請求項１～請求項９のいずれか１項に記載の方法。
【請求項１１】

前記生成するステップは、ドメインオーナによって提供されるパラメータをさらに備える、請求項１～請求項１０のいずれか１項に記載の方法。
【請求項１２】
前記ドメインオーナによって提供される前記パラメータは、該ドメインオーナの秘密キーを用いて自動生成される、請求項１１に記載の方法。
【請求項１３】
前記クライアントデバイスは、無線デバイスである、請求項１～請求項１２のいずれか１項に記載の方法。
【請求項１４】
モバイルユーザ証明書を使用する安全な記録プロトコルのためのシステムであって、該システムは、
クライアントデバイス（１５０；２５０）であって、
通信サブシステム（１５２；２５２）と、
該通信サブシステム（１５２；２５２）と通信するように適合されているプロセッサ（１５４；２５４）と、
該モバイルユーザ証明書から生成された入力を格納するように適合されているメモリ（１５６；２５６）と、
クライアントデバイスキージェネレータ（１６５；２６５）であって、該クライアントデバイスキージェネレータは、該入力を提供され、１つまたは２つの公開キー－秘密キーのペアを生成するように適合されている、クライアントデバイスキージェネレータ（１６５；２６５）と、
署名／検証モジュール（１６０；２６０）であって、該署名／検証モジュールは、該クライアントデバイスキージェネレータ（１６５；２６５）によって生成された該秘密キーのうちの一つを用いて、メッセージに署名するように適合されている、署名／検証モジュール（１６０；２６０）と
を有する、クライアントデバイス（１５０；２５０）と、
サーバ（１１０；２１０）であって、
該クライアントデバイス通信サブシステム（１５２；２５２）と通信するように適合されている通信サブシステム（１１２；２１２）と、
該サーバ通信サブシステムと通信するように適合されているプロセッサ（１１４；２１４）と、
該モバイルユーザ証明書から生成された入力を格納するように適合されているメモリ（１１６；２１６）と、
サーバキージェネレータ（１２５；２２５）であって、該サーバキージェネレータは、該入力を提供され、１つまたは２つの公開キー－秘密キーのペアを生成するように適合されている、サーバキージェネレータ（１２５；２２５）と、
署名／検証モジュール（１２０；２２０）であって、該署名／検証モジュールは、該サーバキージェネレータによって生成された該秘密キーのうちの一つを用いて、メッセージに署名するように適合されている、署名／検証モジュール（１２０；２２０）と
を有する、サーバ（１１０；２１０）と
を備え、
該クライアントデバイスキージェネレータおよび該サーバキージェネレータは、同一の入力に対して、同一の秘密キー－公開キーのペアを生成するように適合されている、システム。
【請求項１５】
前記モバイルユーザ証明書は、パスワードを備える、請求項１４に記載のシステム。
【請求項１６】
前記サーバでの前記入力および前記クライアントデバイスでの前記入力は、ノンスを用いてハッシュされたパスワードを備える、請求項１４または請求項１５に記載のシステム。

【請求項１７】
前記サーバでの前記入力および前記クライアントデバイスでの前記入力は、該クライアントデバイスと該サーバとによって共有されるパラメータを用いるパスワード変換を備える、請求項１４～請求項１６のいずれか１項に記載のシステム。
【請求項１８】
前記クライアントデバイスキージェネレータ（１６５；２６５）および前記サーバキージェネレータ（１２５；２２５）は、同一の単一の公開キー－秘密キーのペアを生成するように適合されている、請求項１４～請求項１６のいずれか１項に記載のシステム。
【請求項１９】
前記クライアントデバイスキージェネレータ（１６５；２６５）および前記サーバキージェネレータ（１２５；２２５）は、クライアント公開キー－秘密キーのペアと、サーバ公開キー－秘密キーのペアとの双方を生成するように適合されている、請求項１４～請求項１７のいずれか１項に記載のシステム。
【請求項２０】
前記クライアントデバイスキージェネレータ（１６５；２６５）は、前記サーバ秘密キーを隠し、前記サーバキージェネレータ（１２５；２２５）は、前記クライアントデバイス秘密キーを隠す、請求項１９に記載のシステム。
【請求項２１】
前記クライアントデバイス署名／検証モジュールは、さらに、前記公開キーのうちの一つを用いて、前記メッセージを暗号化する、請求項１４～請求項２０のいずれか１項に記載のシステム。
【請求項２２】
前記サーバ署名／検証モジュールは、さらに、前記公開キーのうちの一つを用いて、前記メッセージを暗号化する、請求項１４～請求項２１のいずれか１項に記載のシステム。
【請求項２３】
前記入力は、セッション識別子を備える、請求項１４～請求項２２のいずれか１項に記載のシステム。
【請求項２４】
前記クライアントデバイスキージェネレータ（１６５；２６５）および前記サーバキージェネレータ（１２５；２２５）は、ドメインオーナによって提供されるパラメータを前記入力と結合して、利用するように適合されている、請求項１４～請求項２３のいずれか１項に記載のシステム。
【請求項２５】
前記ドメインオーナによって提供される前記パラメータは、該ドメインオーナの秘密キーを用いて自動生成される、請求項２４に記載のシステム。
【請求項２６】
前記クライアントデバイスは、無線デバイスである、請求項１４～請求項２５のいずれか１項に記載のシステム。
【請求項２７】
計算デバイスまたはシステムのプロセッサによって、該計算デバイスまたはシステムに、請求項１～請求項１３のいずれか１項に記載の方法を実行させるために使用するプログラムコードを格納する、コンピュータ読み取り可能な媒体。
【請求項２８】
請求項１４～請求項２６のいずれか１項に記載のシステムを備える通信システムであって、複数のクライアントデバイスが、該システムの前記サーバと通信するように適合されている、通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概して、安全な記録プロトコルに関し、特に、クライアントとサーバとの間

の通信のための安全な記録プロトコルに関する。
【背景技術】
【０００２】
クライアントとサーバとの間で、多数のタイプの情報を送信するとき、安全な通信は、重要である。たとえば、とりわけ、金融情報、健康情報、電子メールは、データ認証および保全性の双方を保証することによって、およびデータの暗号化を介して保護される必要がある。
【０００３】
このような安全な通信を提供するために、様々なソリューションが存在する。一つの例は、クライアントおよびサーバの証明書を使用することを含む。しかしながら、当業者によって理解されるように、キャリアまたは企業のようなドメインオーナにとって、クライアントデバイス上のクライアント証明書を管理することは、特に、クライアントデバイスがモバイルデバイスであるときに、困難である。さらに、モバイルデバイスにこれらのクライアント証明書をインストールすることは、難解なロジスティックスを要する。
【０００４】
代替のソリューションは、共有秘密（ｓｈａｒｅｄ　ｓｅｃｒｅｔ）を使用することを含み、この共有秘密またはその一部は、安全なチャネルが確立される前に、クライアントとサーバとの間で無線を介して流れる。理解されるように、この共有秘密の無線を介する転送は、結果として、データ保全性を危うくし得る。
【発明の開示】
【課題を解決するための手段】
【０００５】
（概要）
本システムおよび方法は、デバイスクライアントと一般的なモバイルサーバとの間で、安全に認証された記録プロトコルを確立するための軽量なセキュリティモデルを提供し得る。本方法は、デバイスまたはモバイルのユーザ登録時に、オフラインで提供されるユーザパスワードまたは任意の他の安全なパラメータのようなモバイルユーザ証明書の共有知識に基づき得る。
【０００６】
本システムは、クライアントキージェネレータ（ＣＫＧ）を含み得、該ＣＫＧは、所定のセキュリティアルゴリズムを用いて、シングルキーペア暗号化方法論において、公開および秘密キーを入力トークンから生成するか、あるいはデュアルキーペアソリューションにおいて、デバイスクライアント公開および秘密キーと、サーバ公開キーとを入力トークンから生成する。サーバ公開キーを生成するために、シーケンスの一部として生成されたサーバ秘密キーが、クライアントランタイム環境にさらされない（ＮＯＴ　ｅｘｐｏｓｅｄ）ことが、留意されるべきである。
【０００７】
本システムは、サーバキージェネレータ（ＳＫＧ）をさらに含み得、該ＳＫＧは、クライアントキージェネレータのマッチングセキュリティアルゴリズムに、マッチングセキュリティアルゴリズムを用いて、シングルキーペアソリューションにおいて、公開および秘密キーを入力トークンから生成し、あるいはデュアルキーペアソリューションにおいて、サーバ公開キーおよびデバイスクライアント公開キーを入力トークンから生成する。クライアント公開キーを生成するために、シーケンスの一部として生成されたクライアント秘密キーが、サーバランタイム環境にさらされない（ＮＯＴ　ｅｘｐｏｓｅｄ）ことが、留意されるべきである。
【０００８】
したがって、本開示は、サーバおよびクライアントを有するシステムにおける安全な記録プロトコルに対する方法を提供し得、該方法は、キージェネレータへの入力としてモバイルユーザ証明書を利用するステップであって、該モバイルユーザ証明書は該サーバと該クライアントとの双方に既知である、ステップと、該モバイルユーザ証明書入力に基づい

て、１つまたは２つの公開キー－秘密キーのペアを生成するステップと、秘密キーを用いて署名されたメッセージを送信するステップとを包含する。

【０００９】

本開示は、さらに、モバイルユーザ証明書を使用する安全な記録プロトコルのためのシステムを提供し得、該システムは、クライアントであって、通信サブシステムと、該通信サブシステムと通信するように適合されているプロセッサと、該モバイルユーザ証明書から生成された入力を格納するように適合されているメモリと、クライアントキージェネレータであって、該クライアントキージェネレータは、該入力を提供され、１つまたは２つの公開キー－秘密キーのペアを生成するように適合されている、クライアントキージェネレータと、署名／検証モジュールであって、該署名／検証モジュールは、該クライアントキージェネレータによって生成された該秘密キーのうちの一つを用いて、メッセージに署名するように適合されている、署名／検証モジュールとを有する、クライアントと；サーバであって、該クライアント通信サブシステムと通信するように適合されている通信サブシステムと、該サーバ通信サブシステムと通信するように適合されているプロセッサと、該モバイルユーザ証明書から生成された入力を格納するように適合されているメモリと、サーバキージェネレータであって、該サーバキージェネレータは、該入力を提供され、１つまたは２つの公開キー－秘密キーのペアを生成するように適合されている、サーバキージェネレータと、署名／検証モジュールであって、該署名／検証モジュールは、該サーバキージェネレータによって生成された該秘密キーのうちの一つを用いて、メッセージに署名するように適合されている、署名／検証モジュールとを有する、サーバとを備え、該クライアントキージェネレータおよび該サーバキージェネレータは、同一の入力に対して、同一の秘密キー－公開キーのペアを生成するように適合されている。

【００１０】

本発明は、さらに、以下の手段を提供する。

【００１１】

（項目１）

サーバキージェネレータ（１２５；２２５）を有するサーバ（１１０；２１０）と、クライアントデバイスキージェネレータ（１６５；２６５）を有するクライアントデバイス（１５０；２５０）とを有するシステムにおける安全な記録プロトコルのための方法であって、

モバイルユーザ証明書を該サーバキージェネレータ（１２５；２２５）、該クライアントデバイスキージェネレータ（１６５；２６５）への入力として利用するステップであって、該モバイルユーザ証明書は、該サーバ（１１０；２１０）と該クライアントデバイス（１５０；２５０）との双方に既知である、ステップと、

該サーバキージェネレータ（１２５；２２５）を利用して、該モバイルユーザ証明書入力に基づく１つまたは２つの公開キー－秘密キーのペアを生成するステップと、

該クライアントデバイスキージェネレータ（１６５；２６５）を利用して、該モバイルユーザ証明書入力に基づく１つまたは２つの公開キー－秘密キーのペアを生成するステップと、

該秘密キーのうちの一つを用いて署名されたメッセージを、送信するステップと

を包含する、方法。

【００１２】

（項目２）

上記モバイルユーザ証明書は、パスワードである、項目１に記載の方法。

【００１３】

（項目３）

上記入力は、安全なハッシュ関数を用いて、ノンスを用いてハッシュされたパスワードである、項目１または項目２に記載の方法。

【００１４】

（項目４）

上記入力は、上記クライアントデバイスと上記サーバとによって共有されるパラメータを用いるパスワード変換である、項目１～項目３のいずれか１項に記載の方法。

【００１５】

（項目５）

上記サーバキージェネレータ（１２５；２２５）およびクライアントデバイスキージェネレータ（１６５；２６５）は、１つの公開キー－秘密キーのペアのみを生成する、項目１～項目４のいずれか１項に記載の方法。

【００１６】

（項目６）

上記サーバキージェネレータ（１２５；２２５）およびクライアントデバイスキージェネレータ（１６５；２６５）は、クライアントデバイスの公開キー－秘密キーのペアおよびサーバの公開キー－秘密キーのペアを生成する、項目１～項目４のいずれか１項に記載の方法。

【００１７】

（項目７）

上記サーバキージェネレータ（１２５；２２５）およびクライアントデバイスキージェネレータ（１６５；２６５）は、上記クライアントデバイス秘密キーまたは上記サーバ秘密キーを隠す、項目６に記載の方法。

【００１８】

（項目８）

上記送信するステップは、さらに、上記公開キーのうちの一つを用いて、メッセージを暗号化する、項目１～項目７のいずれか１項に記載の方法。

【００１９】

（項目９）

同一の入力を利用すると、上記生成するステップが上記クライアントデバイス（１５０；２５０）上で実行されるときは、該生成するステップが上記サーバ（１１０；２１０）上で実行されるときと、同一の公開キー－秘密キーのペアを生成する、項目１～項目８のいずれか１項に記載の方法。

【００２０】

（項目１０）

上記利用するステップは、さらに、セッション識別子を組み込んで、入力を生成する、項目１～項目９のいずれか１項に記載の方法。

【００２１】

（項目１１）

上記生成するステップは、ドメインオーナによって提供されるパラメータをさらに備える、項目１～項目１０のいずれか１項に記載の方法。

【００２２】

（項目１２）

上記ドメインオーナによって提供される上記パラメータは、該ドメインオーナの秘密キーを用いて自動生成される、項目１１に記載の方法。

【００２３】

（項目１３）

上記クライアントデバイスは、無線デバイスである、項目１～項目１２のいずれか１項に記載の方法。

【００２４】

（項目１４）

モバイルユーザ証明書を使用する安全な記録プロトコルのためのシステムであって、該システムは、

クライアントデバイス（１５０；２５０）であって、

通信サブシステム（１５２；２５２）と、

該通信サブシステム（１５２；２５２）と通信するように適合されているプロセッサ（１５４；２５４）と、
該モバイルユーザ証明書から生成された入力を格納するように適合されているメモリ（１５６；２５６）と、
クライアントデバイスキージェネレータ（１６５；２６５）であって、該クライアントデバイスキージェネレータは、該入力を提供され、１つまたは２つの公開キー－秘密キーのペアを生成するように適合されている、クライアントデバイスキージェネレータ（１６５；２６５）と、
署名／検証モジュール（１６０；２６０）であって、該署名／検証モジュールは、該クライアントデバイスキージェネレータ（１６５；２６５）によって生成された該秘密キーのうちの一つを用いて、メッセージに署名するように適合されている、署名／検証モジュール（１６０；２６０）と
を有する、クライアントデバイス（１５０；２５０）と、
サーバ（１１０；２１０）であって、
該クライアントデバイス通信サブシステム（１５２；２５２）と通信するように適合されている通信サブシステム（１１２；２１２）と、
該サーバ通信サブシステムと通信するように適合されているプロセッサ（１１４；２１４）と、
該モバイルユーザ証明書から生成された入力を格納するように適合されているメモリ（１１６；２１６）と、
サーバキージェネレータ（１２５；２２５）であって、該サーバキージェネレータは、該入力を提供され、１つまたは２つの公開キー－秘密キーのペアを生成するように適合されている、サーバキージェネレータ（１２５；２２５）と、
署名／検証モジュール（１２０；２２０）であって、該署名／検証モジュールは、該サーバキージェネレータによって生成された該秘密キーのうちの一つを用いて、メッセージに署名するように適合されている、署名／検証モジュール（１２０；２２０）と
を有する、サーバ（１１０；２１０）と
を備え、
該クライアントデバイスキージェネレータおよび該サーバキージェネレータは、同一の入力に対して、同一の秘密キー－公開キーのペアを生成するように適合されている、システム。

【００２５】
（項目１５）
上記モバイルユーザ証明書は、パスワードを備える、項目１４に記載のシステム。

【００２６】
（項目１６）
上記サーバでの上記入力および上記クライアントデバイスでの上記入力は、ノンスを用いてハッシュされたパスワードを備える、項目１４または項目１５に記載のシステム。

【００２７】
（項目１７）
上記サーバでの上記入力および上記クライアントデバイスでの上記入力は、該クライアントデバイスと該サーバとによって共有されるパラメータを用いるパスワード変換を備える、項目１４～項目１６のいずれか１項に記載のシステム。

【００２８】
（項目１８）
上記クライアントデバイスキージェネレータ（１６５；２６５）および上記サーバキージェネレータ（１２５；２２５）は、同一の単一の公開キー－秘密キーのペアを生成するように適合されている、項目１４～項目１６のいずれか１項に記載のシステム。

【００２９】
（項目１９）

上記クライアントデバイスキージェネレータ（１６５；２６５）および上記サーバキージェネレータ（１２５；２２５）は、クライアント公開キー－秘密キーのペアと、サーバ公開キー－秘密キーのペアとの双方を生成するように適合されている、項目１４～項目１７のいずれか１項に記載のシステム。

【００３０】

（項目２０）

上記クライアントデバイスキージェネレータ（１６５；２６５）は、上記サーバ秘密キーを隠し、上記サーバキージェネレータ（１２５；２２５）は、上記クライアントデバイス秘密キーを隠す、項目１９に記載のシステム。

【００３１】

（項目２１）

上記クライアントデバイス署名／検証モジュールは、さらに、上記公開キーのうちの一つを用いて、上記メッセージを暗号化する、項目１４～項目２０のいずれか１項に記載のシステム。

【００３２】

（項目２２）

上記サーバ署名／検証モジュールは、さらに、上記公開キーのうちの一つを用いて、上記メッセージを暗号化する、項目１４～項目２１のいずれか１項に記載のシステム。

【００３３】

（項目２３）

上記入力は、セッション識別子を備える、項目１４～項目２２のいずれか１項に記載のシステム。

【００３４】

（項目２４）

上記クライアントデバイスキージェネレータ（１６５；２６５）および上記サーバキージェネレータ（１２５；２２５）は、ドメインオーナによって提供されるパラメータを上記入力と結合して、利用するように適合されている、項目１４～項目２３のいずれか１項に記載のシステム。

【００３５】

（項目２５）

上記ドメインオーナによって提供される上記パラメータは、該ドメインオーナの秘密キーを用いて自動生成される、項目２４に記載のシステム。

【００３６】

（項目２６）

上記クライアントデバイスは、無線デバイスである、項目１４～項目２５のいずれか１項に記載のシステム。

【００３７】

（項目２７）

計算デバイスまたはシステムのプロセッサによって、該計算デバイスまたはシステムに、項目１～項目１３のいずれか１項に記載の方法を実行させるために使用するプログラムコードを格納する、コンピュータ読み取り可能な媒体。

【００３８】

（項目２８）

項目１４～項目２６のいずれか１項に記載のシステムを備える通信システムであって、複数のクライアントデバイスが、該システムの上記サーバと通信するように適合されている、通信システム。

【００３９】

（摘要）

サーバとクライアントとを有するシステムにおける安全な記録プロトコルのための方法および装置であって、該方法は、キージェネレータへの入力としてモバイルユーザ証明書

を利用するステップであって、該モバイルユーザ証明書は該サーバと該クライアントとの双方に既知である、ステップと、該モバイルユーザ証明書入力に基づいて、１つまたは２つの公開キー－秘密キーのペアを生成するステップと、秘密キーを用いて署名されたメッセージを送信するステップとを有する。

【発明を実施するための最良の形態】

【００４０】

本開示は、図面を参照することによって、より良く理解される。

【００４１】

（好ましい実施形態の説明）

図１に、参照がなされる。図１は、シングルキーペア暗号化スキームで使用されるように適合された簡略化されたサーバおよびクライアントのブロック図である。システムは、サーバ１１０およびクライアント１５０を含む。サーバ１１０は、クライアント１５０と、特に、クライアント１５０上の通信サブシステム１５２と、ネットワークを介して、通信するように適合された通信サブシステム１１２を含む。当業者には理解されるように、通信が発生するネットワークは、有線ネットワークまたは無線ネットワークを含む任意のネットワークであり得る。一つの例において、通信サブシステム１５２は、基地局またはアクセスポイントを有するセルラネットワークまたは無線ローカルエリアネットワーク（ＷＬＡＮ）のような無線ネットワークを介して通信するように適合される。次いで、この基地局またはアクセスポイントが、パケットデータサービングノードのような一連のシステムコンポーネントを介して、インターネットを介して、サーバ１１０に接続する。通信の他の例は、当業者に公知であり、本出願は、任意の特定のモードの通信に限定されることを意図しない。

【００４２】

サーバ１１０は、通信サブシステム１１２と通信するように適合されたプロセッサ１１４を含む。

【００４３】

プロセッサ１１４はまた、様々なアプリケーションおよびデータを格納するために使用されるメモリ１１６と通信する。メモリ１１６は、コンピュータシステムおよびデバイスに適用される任意の形式のメモリを含み得る。

【００４４】

プロセッサ１１４は、さらに、署名／検証モジュール１２０と通信する。図１のシステムにおいて、署名／検証モジュール１２０は、シングルキーペア署名／検証モジュールである。

【００４５】

サーバキージェネレータ１２５は、署名／検証モジュール１２０に署名／検証キーを提供するように適合される。この署名／検証キーは、発信メッセージに署名するためか、あるいは着信メッセージを検証するためかのいずれかに必要なものである。サーバキージェネレータ（ＳＫＧ）１２５は、さらに、メモリ１１６からの入力トークンを受信するために、メモリ１１６と通信するように適合される。

【００４６】

ＳＫＧ１２５に対する入力トークンは、サーバとクライアントとの双方に既知であるモバイルユーザ証明書を備える。これは、デバイス登録時に、オフラインで提供されるユーザパスワードまたは安全コードのような証明書を含み得る。モバイルユーザ証明書の他の例は、当業者に公知である。

【００４７】

好ましい実施形態において、ＳＫＧ１２５は、メモリ１１６からの入力トークンを利用し、公開キーおよび秘密キーの双方を生成する。好ましい実施形態において、秘密キーは、着信メッセージを解読するために使用され、公開キーは、発信メッセージを暗号化するために使用される。

【００４８】

ＳＫＧ１２５は、好ましくは、自身の中に構築されたドメインオーナパラメータをさらに含む。キャリアまたは企業のような無線ドメインオーナは、ＳＫＧを配備する前に、これらのドメインオーナパラメータを設定する。ＳＫＧ１２５は、公開キー１３０および秘密キー１３２を生成するために、ドメインオーナパラメータ１２７をメモリ１１６から受信された入力トークンと結合する。

【００４９】

入力トークンとドメインオーナパラメータとの結合は、エントロピを増加させ、セキュリティを向上させる。これらのパラメータを混合するには、種々の方法が存在する。一つは、例えば、ＤＳＡ（デジタル署名アルゴリズム）キーを用いるドメインオーナパラメータからのパラメータの生成である。ＤＳＡキー生成メカニズムは、ウィキペディアのウェブサイト上で、「Ｄｉｇｉｔａｌ＿Ｓｉｇｎａｔｕｒｅ＿Ａｌｇｏｒｉｔｈｍ」の項目に見出され得る。

【００５０】

上述の項目に記載されているように、（ｐ，ｑ，ｇ，ｙ）は、公開キーで、（ｘ）は、秘密キーであり、ここで

ｐは、巡回グループＺｐ＊のオーダであり、

ｑは、Ｚｐ＊の巡回サブグループＺｑ＊のオーダであり（ｑがｐを分割する）、

ｇは、巡回サブグループＺｑ＊のジェネレータであり、

ｙは、$g^x = y$であるようなＺｑ＊における要素である。

【００５１】

理解されるように、ｐ、ｑ、およびｇは、アルゴリズムパラメータを規定し、ｙは、公開キーを規定するものである。

【００５２】

通常、ｐ、ｑ、およびｇは、公開されている。しかしながら、上述のように、ｐ、ｑ、およびｇは、ドメインオーナ証明書から導出されて設定された秘密アルゴリズムのパラメータであり得る。次いで、ｘ（秘密キー）は、加入者パスワードから導出され、ｙは、$y = g^x$として、計算される。ｐ、ｑ、およびｇは、両方の側で同じはずであることに留意されたい。

【００５３】

別の例において、二段階処理が、ＣＫＧおよびＳＫＧ内で使用され得る。ここで、第一段階で、処理は、ドメインオーナパラメータから導出されたキーを用いて、入力トークンに変換を適用する。また、このキーは、デバイス上にＣＫＧを配備する前に、安全にＣＫＧの中に設定され得る。第一段階で、このアプローチを用いて、処理は、（より良いエントロピで）新たな入力キーを生成し、第二段階におけるキーペア生成に、このキーを供給する。

【００５４】

当業者に理解されるように、他の可能なシナリオも存在する。

【００５５】

クライアント側において、クライアント１５０は、上述のように、通信サブシステム１５２を含む。クライアント１５０は、プロセッサ１５４をさらに含む。プロセッサ１５４は、通信サブシステム１５２を介して通信を送信するように適合され、さらに、メモリ１５６と相互作用する。

【００５６】

署名／検証モジュール１６０は、発信メッセージに署名し、着信メッセージを検証するために利用される。署名／検証モジュール１６０は、クライアントキージェネレータ１６５と通信し、クライアントキージェネレータ１６５は、キーを生成するように適合される。特に、好ましい実施形態において、公開キー１７０および秘密キー１７２が生成される。公開キー１７０は、公開キー１３０と同一であるべきであり、秘密キー１７２は、秘密キー１３２と同一であるべきである。

【００５７】

動作において、メモリ１５６に格納された入力トークンは、ＣＫＧ１６５に入力される。好ましくは、ドメインオーナパラメータ１６７は、メモリ１５６からの入力トークンと結合され、クライアントキージェネレータ１６５は、これらの２つのパラメータに基づいて、キーを生成する。これは、上述と同様に、幾つかの方法で行われ得る。

【００５８】

また、ＳＫＧ１２５と署名／検証モジュール１２０との一方または双方は、プロセッサ１１４の一部であり得る。代替として、これらのコンポーネントは、サーバ１１０上のプロセッサ１１４と別個であり得る。

【００５９】

同様に、ＣＫＧ１６５は、プロセッサ１５４の一部を形成し得、署名／検証モジュール１６０もまた、プロセッサ１５４の一部を形成し得る。代替として、ＳＫＧ１６５と署名／検証モジュール１６０との一方または双方は、クライアントデバイス１５０上の別個のコンポーネントでもあり得る。

【００６０】

図１の実施形態により良い保護を提供するために、デュアルキーペアシステムが使用され得る。ここで、図２に参照がなされる。図２は、サーバ２１０およびクライアント２５０を有する例示的なクライアント／サーバシステムを示す。

【００６１】

図１のシステムと同様に、サーバ２１０は、通信サブシステム２１２を含み、通信サブシステム２１２は、クライアント２５０と、特に、クライアント２５０上の通信サブシステム２５２と、ネットワークを介して通信するように適合されている。

【００６２】

サーバ２１０は、さらに、通信サブシステム２１２を介して通信を送受信するように適合されたプロセッサ２１４を含み、さらに、メモリ２１６および署名／検証モジュール２２０と通信する。メモリ２１６は、共有の証明書を備える入力トークンを格納し、メモリ２１６は、任意の形式のメモリであり得る。

【００６３】

図２のシステムにおいて、署名／検証モジュール２２０は、非対称な署名／検証モジュールである。換言すれば、サーバ２１０上で、クライアント秘密キーは、発信メッセージに署名するために使用され、サーバ公開キーは、クライアントから受信されたメッセージを検証するために使用される。以下に記載されるように、クライアント公開キーはまた、暗号化のために使用され得、サーバ秘密キーは、検証のために使用され得る。

【００６４】

サーバキージェネレータ２２５は、メモリ２１６からの入力トークンを受信するように適合されている。好ましくは、ＳＫＧ２２５は、アルゴリズムパラメータ２２７をさらに含み、アルゴリズムパラメータ２２７は、メモリ２１６からサーバキージェネレータ２２５に対する入力である入力トークンと結合する。

【００６５】

ＳＫＧ２２５は、サーバ公開キー２３０、サーバ秘密キー２３２、クライアント公開キー２３４、およびクライアント秘密キー（図示せず）を生成する。ＳＫＧ２２５は、デバイスクライアント秘密キーを出力する能力を提供しないことが期待される。

【００６６】

同様に、クライアントデバイス２５０は、上述のように、通信サブシステム２５２を含む。さらに、クライアント２５０は、通信サブシステム２５２を介して通信を送受信するように適合されているプロセッサ２５４を含み、メモリ２５６と通信するように適合されている。非対称な署名／検証モジュール２６０は、プロセッサおよび通信サブシステム２５２と通信し、さらに、クライアントキージェネレータ（ＣＫＧ）２６５からのキーを受信する。

【００６７】

ＣＫＧ２６５は、メモリ２５６から共有の証明書を受信し、好ましい実施形態において

、ＣＫＧ２６５はまた、入力トークンを生成して、キーを生成するために、アルゴリズムパラメータ２６７を使用する。ＣＫＧ２６５は、クライアント公開キー２７０、クライアント秘密キー２７２、サーバ公開キー２７４、およびサーバ秘密キー（図示せず）を生成する。ＣＫＧは、サーバ秘密キーを出力する能力を提供しないことが期待される。

【００６８】

したがって、上述のシステムは、クライアントキージェネレータ２６５を含み、クライアントキージェネレータ２６５は、所定のセキュリティアルゴリズムを用いて、デバイスクライアント公開および秘密キー２７０および２７２それぞれを、さらに、入力トークンからサーバ公開キー２７４を生成する。上記システムは、サーバキージェネレータ２２５をさらに含み、マッチングセキュリティアルゴリズムを用いて、サーバ公開および秘密キー２３０および２３２それぞれと、入力トークンに基づくデバイスクライアント公開キー２３４とを生成する。同一の入力トークンが使用されるとき、ＣＫＧ２６５およびＳＫＧ２２５は、以下の条件：

ａ）ＣＫＧ２６５によって生成されたサーバ公開キーは、ＳＫＧ２２５によって生成されたサーバ公開キーと同一であるべきで、ＳＫＧ２２５によって生成されたサーバ秘密キー２３２と合致するべきであることと、

ｂ）ＳＫＧ２２５によって生成されたデバイスクライアント公開キー２３４は、ＣＫＧ２６５によって生成されたクライアント公開キー２７０と同一であるべきで、ＣＫＧ２６５によって生成されたクライアント秘密キー２７２と合致するべきであることと

を満足させるべきである。

【００６９】

ＳＫＧ２２５およびＣＫＧ２６５において使用されるアルゴリズムに対する入力パラメータは、機密であり、ドメインオーナによって管理される。無線ドメインにおいて、ドメインオーナは、キャリアまたは企業であり得る。ＳＫＧ２２５およびＣＫＧ２６５のモジュールは、サーバ２１０およびデバイス２５０上に、これらのモジュールを配備する前に、ドメインオーナ証明書を設定する能力をドメインオーナに提供するべきである。これらのドメインオーナ証明書は、ドメインオーナの保護された秘密であり、クライアント証明書が危険に晒される場合、追加的なセキュリティを提供する。一つの実施形態において、これらのパラメータは、ドメインオーナ秘密キーを用いて自動生成され得る。

【００７０】

ここで、図３に参照がなされる。図３は、好ましい方法に従うデータフロー図を示す。クライアント３１０は、サーバ３２０と通信する。クライアント３１０は、ステップ３２２で、バージョンネゴシエーションの際に、モバイルユーザのアイデンティティを提供する活性化メッセージを送信する。ノンス（ｎｏｎｃｅ）が、この活性化メッセージに提供される。

【００７１】

代替のフローにおいて、クライアント３１０は、代わりに、ステップ３４２で、クライアント活性化メッセージを送信し、ステップ３４４で、ノンスを含み得るチャレンジを受信する。クライアント３１０は、次いで、チャレンジ応答３４６を送信し、ここで、モバイルユーザのアイデンティティは、オプションとして、ステップ３４４からのノンスを用いてハッシュされる。

【００７２】

サーバ３２０は、３４６の中のメッセージからモバイルユーザのアイデンティティを検索し、サーバキージェネレータ（図２からのＳＫＧ２２５）を用いて、サーバ秘密公開キーのペアと、入力トークンとして、モバイルユーザのパスワードを用いるクライアント公開キーとを生成する。オプションとして、ＳＫＧ２２５に対する入力トークンは、クライアントが活性化メッセージの中にノンスを提供した場合、ノンスを用いる安全なハッシュ関数でハッシュされたパスワードを用いて生成され得る。さらなる代替において、クライアントとサーバとによって共有されるパラメータを用いる任意のパスワード変換が、実行され得る。

【００７３】
サーバは、次いで、ステップ３５２で、サーバ秘密キーで署名された活性化確認応答メッセージを送信し得る。
【００７４】
ステップ３５４で、クライアントキージェネレータは、サーバ公開キーと、入力トークンとして、モバイルユーザのパスワードを用いるクライアント秘密公開キーとのペアとを生成する。オプションとして、ＣＫＧに対する入力トークンは、ノンスが活性化メッセージの中に送信された場合、ノンスを用いる安全なハッシュ関数でハッシュされたパスワードを用いて、あるいはクライアントとサーバとの双方で共有されるパラメータを用いる任意のパスワード変換を用いて、生成され得る。
【００７５】
クライアント３１０は、次いで、ステップ３５６で、サーバ公開キーを用いて、メッセージを検証し、オプションとして、クライアント公開キーを用いて、そのメッセージを解読する。
【００７６】
クライアントとサーバとの間での後続のメッセージは、記録プロトコルに対する自身の公開／秘密キーの一部を用いて、メッセージに署名して、暗号化する。
【００７７】
よりシンプルな活性化を用いると、クライアント活性化メッセージ３２２は、モバイルユーザ識別子と、オプションで、ノンスとを含む。
【００７８】
ステップ３２４で、サーバ３２０は、モバイルユーザ識別子に基づいて、ＳＫＧからキーを得る。上述のように、サーバは、モバイルユーザのパスワードを検索し、サーバキージェネレータを用いて、サーバ秘密／公開キーのペアを生成し、入力トークンとして、モバイルユーザのパスワードを用いるクライアント／公開キーを生成する。オプションとして、ＳＫＧに対する入力トークンは、クライアントが活性化メッセージの中にノンスを提供した場合、ノンスを用いてハッシュされたパスワードを用いて、あるいはクライアントとサーバとの双方で共有されるパラメータを用いる任意のパスワード変換を用いて、生成され得る。
【００７９】
サーバ３２０は、次いで、サーバの秘密キーで署名されたクライアント活性化メッセージ３２８を送信し、また、必要に応じて、クライアントの公開キーを暗号化し得る。ステップ３２８でのメッセージは、好ましくは、セッション識別子と、クライアント３１０によって要求される任意の他のパラメータとを含む。
【００８０】
クライアント３１０は、クライアントキージェネレータを用いて、サーバ公開キーと、入力トークンとして、モバイルユーザのパスワードを用いるクライアント公開／秘密キーを生成する。オプションとして、ＣＫＧに対する入力トークンは、ノンスが活性化メッセージの中に送信された場合、ノンスを用いてハッシュされたパスワードを用いて、あるいはクライアントとサーバとで共有される秘密パラメータを用いる任意のパスワード変換を用いて、生成され得る。これは、ステップ３３０で行われる。
【００８１】
ステップ３３２で、クライアントは、サーバ公開キーを用いて、メッセージのデジタル署名を検証し、オプションとして、クライアント秘密キーを用いて、そのメッセージを解読する。
【００８２】
任意の後続のメッセージに対して、クライアントおよびサーバは、記録プロトコルに対する自身の秘密／公開キーのペアを用いて、メッセージに署名し、暗号化する。
【００８３】
ここで、図４に参照がなされる。図４は、代替のデータフロー図を示す。

【００８４】
クライアント４１０は、サーバ４２０と通信する。図４に示されるように、様々なフローが、通信に対して可能である。第一のフローにおいて、クライアント４１０は、ステップ４２２で、クライアントの活性化メッセージを生成する。このメッセージは、モバイルユーザ識別子と、オプションで、ノンスを含む。
【００８５】
ステップ４２４で、サーバ４２０は、クライアント活性化メッセージを受信し、該サーバは、モバイルユーザのパスワードを検索し、サーバキージェネレータを使用して、公開／秘密キーのペアと、入力トークンとして、モバイルユーザのパスワードを用いて、クライアント公開キーとを生成する。オプションとして、ＳＫＧに対する入力トークンは、クライアントが活性化メッセージの中にノンスを提供した場合、ノンスを用いてハッシュされたパスワードを用いて、あるいは、クライアントとサーバとの双方によって共有されるパラメータを用いる任意のパスワード変換を用いて、生成され得る。
【００８６】
サーバは、次いで、一意的な識別子を生成し、モバイルユーザのパスワードと、活性化メッセージからのノンスがある場合は、ノンスと、オプションとして、生成されたセッションＩＤとの所定の組み合わせに基づいて、新たな共有秘密を生成する。これは、ステップ４２８で実行される。
【００８７】
サーバ４２０は、次いで、ステップ４３０で、活性化確認を示すメッセージを送信し、サーバ秘密キーで署名されて、生成されたセッションＩＤを含む。
【００８８】
クライアントは、ステップ４３２で、クライアントキージェネレータを用いて、モバイルユーザのパスワードおよび入力トークンを用いるサーバ公開キーを生成する。さらに、クライアントキージェネレータは、クライアント公開／秘密キーのペアを生成するために使用され得る。ここでも、オプションとして、ＣＫＧに対する入力トークンは、ノンスが活性化メッセージで送信された場合、ノンスを用いてハッシュされたパスワードを用いて、あるいはクライアントとサーバとによって共有されたパラメータを用いる任意のパスワード変換を用いて、生成され得る。メッセージが暗号化される場合、クライアントは、ＣＫＧを用いて、クライアント秘密キーを生成し、メッセージを解読するべきである。
【００８９】
処理は、次いで、ステップ４３４で、サーバ公開キーを用いて、メッセージを検証する。クライアントは、オプションとして、クライアント秘密キーを用いて、メッセージを解読し、セッションＩＤを検索する。
【００９０】
ステップ４３６で、クライアントは、モバイルユーザのパスワードと、活性化メッセージからのノンスがある場合は、ノンスと、生成されたセッションＩＤとの所定の組み合わせに基づいて、サーバの共有秘密と同一の新たな共有秘密を生成する。
【００９１】
クライアントは、ＣＫＧを用いて、共有秘密に基づいて、サーバ公開キーと、クライアント秘密公開キーのペアとを生成する。
【００９２】
サーバは、ステップ４３８で、同じ情報を用いて、共有秘密に基づくクライアント公開キーと、サーバ公開秘密キーのペアとを生成する。
【００９３】
次いで、クライアントおよびサーバは、記録プロトコルに対して、自身の公開キーと秘密キーとのペアを使用し、メッセージに署名して、暗号化する。
【００９４】
当業者に理解されるように、上述のアプローチのメリットは、パスワードから導出されたキーは、決して無線で移動しないということである。キーが無線で移動することの問題

は、キーを信頼することである。キーは、各パーティによって独立して生成され、これらのキーは信頼されるので、証明書は、公開キー検証に対して要求されない。

【００９５】

当業者には、さらに理解されるように、上述は、任意のクライアントデバイス上に配備され得る。しかしながら、一つの実施形態において、上述は、無線データデバイス上に配備される。企業またはキャリアは、販売されている各デバイス上に、モジュールをプロビジョニングすることによって、ＣＫＧモジュールを管理し得る。結果として、そのソリューションは、配備の容易さのために、軽量である。なぜなら、展開することが容易だからである。さらに、上記モジュールは、デバイスに追加されるので、他に何も行われる必要はなく、モジュールの追加は、デバイスのプロビジョニングの間に行われ得る。

【００９６】

図３および図４を参照すると、当業者によって理解されるように、シングルキーペアスキームが使用される簡略化されたモデルに対するオプションとして、シングルキーペアが使用され得る。

【００９７】

上述は、さらに、ＣＫＧインプリメンテーションセキュリティによって制約される否認防止（ｎｏｎ－ｒｅｐｕｄｉａｔｉｏｎ）を提供する。アルゴリズムパラメータは、１つのパーティにのみ知られている。なぜなら、アルゴリズムパラメータは、キャリアまたはドメインによって設定され、パスワードまたは他の証明書を用いて結合され、公開／秘密キーのペアを生成するからである。

【００９８】

ここで、図５に参照がなされる。図５は、本方法およびシステムと関連して使用され得る例示的なモバイルデバイスのより詳細なブロック図を示す。図５の装置は、限定することを意味するのではなく、使用され得るデバイスのタイプの例としてのみ表される。

【００９９】

図５は、本出願の装置および方法の好ましい実施形態で使用されやすいモバイルデバイスを示すブロック図である。モバイルデバイス５００は、少なくとも音声およびデータ通信能力を有する双方向無線通信デバイスであることが好ましい。モバイルデバイス５００は、インターネット上の他のコンピュータシステムと通信する能力を有することが好ましい。この無線デバイスは、提供される正確な機能性に依存して、例えば、データメッセージ伝達デバイス、双方向ページャ、無線ｅメールデバイス、データメッセージ伝達能力を有するセルラ電話、無線インターネット機器、あるいはデータ通信デバイスと称され得る。

【０１００】

モバイルデバイス５００は、双方向通信が可能な場合、通信サブシステム５１１を組み込む。通信サブシステム５１１は、受信機５１２と送信機５１４との双方と、関連コンポーネントとを含む。関連コンポーネントは、例えば、好ましくは１つ以上の内蔵または内部のアンテナ素子５１６および５１８、ローカルオシレータ（ＬＯ）５１３、デジタル信号プロセッサ（ＤＳＰ）５２０のような処理モジュールである。通信分野の当業者に明らかなように、通信サブシステム５１１の特定の設計は、そのデバイスが動作するように意図される通信ネットワークに依存する。

【０１０１】

ネットワークアクセス要求もまた、ネットワーク５１９のタイプに依存しても変化する。一部のＣＤＭＡネットワークにおいて、例えば、ネットワークアクセスは、モバイルデバイス５００の加入者またはユーザに関連する。ＣＤＭＡモバイルデバイスは、ＣＤＭＡネットワーク上で動作するために、取り外し可能なユーザ識別モジュール（ＲＵＩＭ）または加入者識別モジュール（ＳＩＭ）カードを必要とし得る。ＳＩＭ／ＲＵＩＭインターフェース５４４は、通常はカードスロットに似ており、この中に、ディスケットまたはＰＣＭＣＩＡカードのように、ＳＩＭ／ＲＵＩＭカードが挿入および排出され得る。ＳＩＭ／ＲＵＩＭカードは、約６４Ｋのメモリを有し得、多数のキー構成５５１と、ＩＤおよび

加入者関連情報のような他の情報５５３を保持し得る。

【０１０２】

要求されるネットワーク登録または活性化手順が完了したとき、モバイルデバイス５００は、ネットワーク５１９を介して、通信信号を送受信し得る。図５に示されるように、ネットワーク５１９は、モバイルデバイスと通信する複数の基地局からなり得る。例えば、ハイブリッドＣＤＭＡ　１ｘＥＶＤＯシステムにおいて、ＣＤＭＡ基地局およびＥＶＤＯ基地局は、モバイルデバイスと通信し、そのモバイルデバイスは同時に両者と接続される。ＥＶＤＯ基地局およびＣＤＭＡ　１ｘ基地局は、異なるページングスロットを用いて、モバイルデバイスと通信する。

【０１０３】

通信ネットワーク５１９を介してアンテナ５１６によって受信された信号は、受信機５１２に入力され、受信機５１２は、信号増幅、周波数下方変換、フィルタリング、チャネル選択など、および、図５に示される例示的なシステムにおけるアナログデジタル（Ａ／Ｄ）変換のような一般的な受信機の機能を実行し得る。受信信号のＡ／Ｄ変換によって、ＤＳＰ５２０において実行される復調および復号化などのより複雑な通信機能が可能になる。同様に、送信されるべき信号は、例えば、ＤＳＰ５２０による変調および符号化を含む処理がなされ、デジタルアナログ変換、周波数上方変換、フィルタリング、増幅、アンテナ５１８を介した通信ネットワーク５１９を介する送信のために、送信機５１４に入力される。ＤＳＰ５２０は、通信信号を処理するだけでなく、受信機および送信機の制御も提供する。例えば、受信機５１２および送信機５１４における通信信号に付与される利得は、ＤＳＰ５２０内でインプリメントされる自動利得制御アルゴリズムを介して適合するように制御され得る。

【０１０４】

モバイルデバイス５００は、デバイスの動作全体を制御するマイクロプロセッサ５３８を含むことが好ましい。少なくともデータおよび音声通信を含む通信機能は、通信サブシステム５１１を介して実行される。マイクロプロセッサ５３８はまた、ディスプレイ５２２、フラッシュメモリ５２４、ランダムアクセスメモリ（ＲＡＭ）５２６、補助入力／出力（Ｉ／Ｏ）サブシステム５２８、シリアルポート５３０、１つ以上のキーボードまたはキーパッド５３２、スピーカ５３４、マイク５３６、短距離通信サブシステムのような他の通信サブシステム５４０、および、全体的に５４２で示される任意の他のデバイスサブシステムなどの追加デバイスサブシステムと相互作用する。シリアルポート５３０は、ＵＳＢポート、または当業者には公知の他のポートを含み得る。

【０１０５】

図５に示されるサブシステムの一部は、通信関連の機能を実行するのに対して、他のサブシステムは「常駐」機能またはオンデバイス機能を提供し得る。とりわけ、キーボード５３２およびディスプレイ５２２などの一部のサブシステムは、例えば、通信ネットワークを介する送信のためのテキストメッセージの入力などの通信関連機能と、計算器またはタスクリストのようなデバイス常駐機能との双方のために用いられ得る。

【０１０６】

マイクロプロセッサ５３８によって用いられるオペレーティングシステムソフトウェアは、フラッシュメモリ５２４などの永続的な記憶装置に格納されることが好ましい。フラッシュメモリ５２４は、代替として、読み出し専用メモリ（ＲＯＭ）または同様のストレージ素子（図示せず）であり得る。オペレーティングシステム、特定のデバイスアプリケーション、またはそのパーツが、ＲＡＭ５２６のような揮発性メモリの中に一時的にロードされ得ることが、当業者には理解される。受信された通信信号もまた、ＲＡＭ５２６の中に格納され得る。

【０１０７】

図示されるように、フラッシュメモリ５２４は、コンピュータプログラム５５８と、プログラムデータストレージ５５０、５５２、５５４および５５６との双方に対して、異なるエリアの中に分離され得る。これらの異なるストレージタイプは、これら自身のデータ

ストレージ要求のために、各プログラムがフラッシュメモリ５２４の一部分に割り当てられ得ることを示す。マイクロプロセッサ５３８は、そのオペレーティングシステム機能に加えて、モバイルデバイス上でソフトウェアアプリケーションの実行を可能にすることが好ましい。例えば、少なくともデータおよび音声の通信アプリケーションを含む基本的な動作を制御する所定のアプリケーションのセットは、通常は製造中にモバイルデバイス５００にインストールされる。他のアプリケーションも、引き続き、あるいは動的にインストールされ得る。

【０１０８】

好ましいソフトウェアアプリケーションは、モバイルデバイスのユーザに関連するデータ項目を編成および管理する能力を有する個人情報マネージャ（ＰＩＭ）アプリケーションであり得る。ユーザに関連するデータ項目としては、ｅメール、カレンダーイベント、音声メール、アポイントメント、タスク項目などが挙げられるが、これらに限定されない。当然、１つ以上のメモリ記憶装置が、モバイルデバイス上で利用可能であり、ＰＩＭデータ項目のストレージを容易にする。このようなＰＩＭアプリケーションは、無線ネットワーク５１９を介してデータ項目を送受信する能力を有することが好ましい。好ましい実施形態において、ＰＩＭデータ項目は、無線ネットワーク５１９を介して、ホストコンピュータシステムに格納または関連付けされたモバイルデバイスユーザの、対応するデータ項目を用いて、シームレスに統合、同期および更新される。さらなるアプリケーションはまた、ネットワーク５１９、補助Ｉ／Ｏサブシステム５２８、シリアルポート５３０、短距離通信サブシステム５４０、または任意の他の適切なサブシステム５４２を介してモバイルデバイス５００上にロードされ得、マイクロプロセッサ５３８による実行のために、ＲＡＭ５２６、または好ましくは不揮発性記憶装置（図示せず）内に、ユーザによってインストールされ得る。アプリケーションのインストールにおけるそのような柔軟性は、デバイスの機能性を向上し、オンデバイス機能、通信関連機能、またはその双方の強化を提供し得る。例えば、安全な通信アプリケーションによって、モバイルデバイス５００を用いて実行される電子商取引機能および他のそのような金融取引が可能となり得る。

【０１０９】

データ通信モードにおいて、テキストメッセージまたはウェブページダウンロードのような受信信号は、通信サブシステム５１１によって処理され、マイクロプロセッサ５３８に入力される。マイクロプロセッサ５３８は、ディスプレイ５２２、あるいは代替として、補助Ｉ／Ｏデバイス５２８への出力のために、受信信号をさらに処理することが好ましい。

【０１１０】

ＣＫＧ１６５およびＣＫＧ２６５に相当し得るクライアントキージェネレータ５６０は、マイクロプロセッサ５３８に鍵を掛ける（ｋｅｙ）。

【０１１１】

モバイルデバイス５００のユーザはまた、例えば、ディスプレイ５２２およびおそらく補助Ｉ／Ｏデバイス５２８と接続するキーボード５３２を用いてｅメールメッセージのようなデータ項目を構成し得る。キーボード５３２は、完全な文字数字キーボードまたは電話タイプのキーパッドであることが好ましい。このように構成された項目は、次いで、通信サブシステム５１１を介して通信ネットワーク上に送信され得る。

【０１１２】

音声通信に対して、受信信号は、好ましくはスピーカ５３４に出力され、送信のための信号は、マイク５３６によって生成されるという点は除いて、モバイルデバイス５００の動作全体は、類似している。代替の音声またはオーディオＩ／Ｏサブシステムもまた、例えば、音声メッセージ記録サブシステムなどは、モバイルデバイス５００上でインプリメントされ得る。音声またはオーディオ信号出力は主にスピーカ５３４を介して達成されることが好ましいが、ディスプレイ５２２もまた用いられて、例えば、呼び出し相手のアイデンティティの表示、音声呼び出しの継続時間、あるいは他の音声呼び出し関連情報を提供するために用いられ得る。

【０１１３】
図５におけるシリアルポート５３０は、通常、パーソナルデジタルアシスタンツ（ＰＤＡ）タイプのモバイルデバイスにおいて、インプリメントされる。このモバイルデバイスが、ユーザのデスクトップコンピュータ（図示せず）と同期することは望ましいことであり得るが、これは、オプションのデバイスコンポーネントである。このようなポート５３０によって、ユーザは、外部デバイスまたはソフトウェアプリケーションを介して優先度を設定でき、無線通信ネットワーク以外を介して、モバイルデバイス５００に情報またはソフトウェアのダウンロードを提供することによって、モバイルデバイス５００の能力を拡張する。代替のダウンロード経路は、例えば、直接それゆえ確実で信頼性ある接続を介して、デバイスに暗号化キーをロードし、それによって安全なデバイス通信を可能にするために使用され得る。当業者には理解されるように、シリアルポート５３０は、さらに、モバイルデバイスをコンピュータに接続し、モデムとして機能するように使用され得る。
【０１１４】
短距離通信サブシステムのような他の通信サブシステム５４０は、さらなるオプションのコンポーネントであり、モバイルデバイス５００と、様々なシステムまたはデバイスとの間での通信を提供し得る。この様々なシステムまたはデバイスは、必ずしも同様のデバイスである必要はない。例えば、サブシステム５４０は、同様に有効化されたシステムおよびデバイスとの通信を提供するために、赤外線デバイス、ならびに関連回路およびコンポーネント、あるいはＢｌｕｅｔｏｏｔｈ™通信モジュールを含み得る。
【０１１５】
本明細書に記載された実施形態は、本出願の技術の要素に対応する要素を有する構造、システムまたは方法の例である。この書面による記載によって、当業者は、本出願の技術のエレメントと同様に対応する代替のエレメントを有する実施形態を実施し、使用することが可能となり得る。本出願の技術の意図される範囲は、したがって、本明細書に記載されたような本出願の技術と異ならない他の構造、システムまたは方法を含み、本明細書に記載されたような本出願の技術と実質的でない差を有する他の構造、システムまたは方法をさらに含む。
【図面の簡単な説明】
【０１１６】
【図１】図１は、クライアントキージェネレータおよびサーバキージェネレータを利用するシングルキーペアソリューションを示す例示的なデバイスのブロック図である。
【図２】図２は、クライアントキージェネレータおよびサーバキージェネレータを利用するデュアルキーペアソリューションを示す例示的なデバイスのブロック図である。
【図３】図３は、セッションの活性化のための、クライアントとサーバとの間でのサンプルデータフローのデータフロー図である。
【図４】図４は、セッションの活性化のための、クライアントとサーバとの間でのサンプルデータフローのデータフロー図である。
【図５】図５は、例示的なモバイルデバイスのブロック図である。
【符号の説明】
【０１１７】
１１０、２１０、３２０、４２０　サーバ
１１２、１５２、２１２、２５２　通信サブシステム
１１４、１５４、２１４、２５４　プロセッサ
１１６、１５６、２１６、２５６　メモリ
１２５、２２５　サーバキージェネレータ
１２０、１６０、２２０、２６０　署名／検証モジュール
１５０、２５０、３１０、４１０　クライアント
１６５、２６５　クライアントキージェネレータ

【図１】

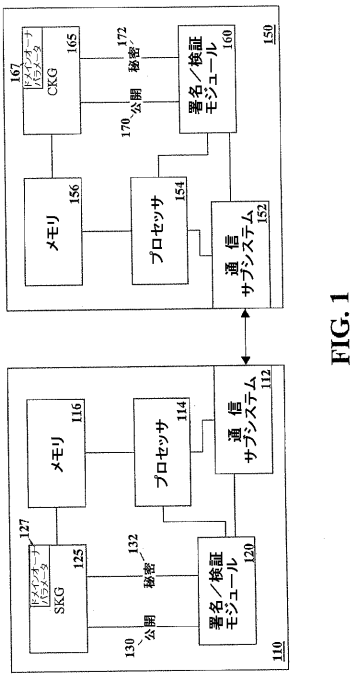

FIG. 1

【図２】

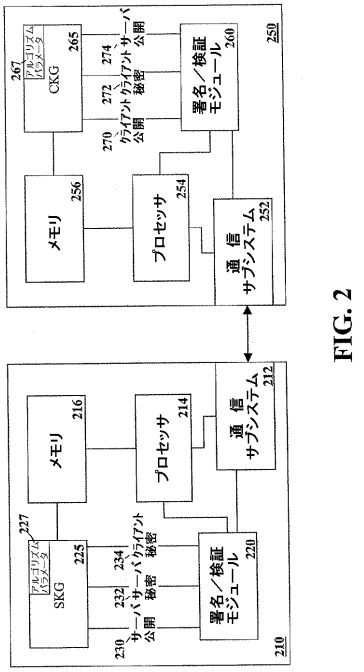

FIG. 2

【図３】

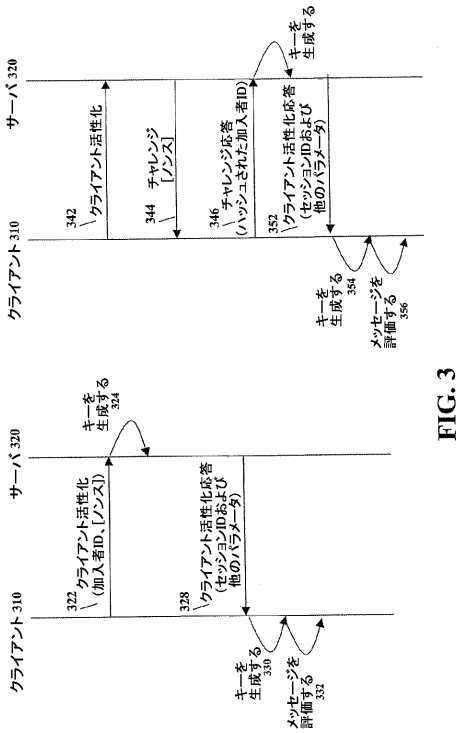

FIG. 3

【図４】

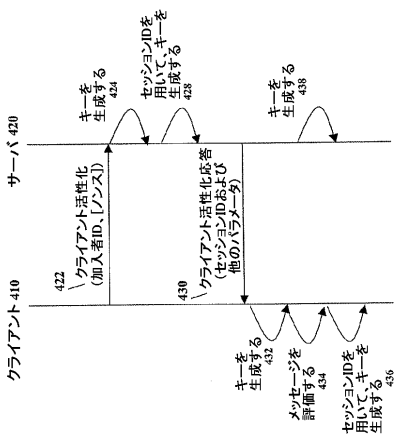

FIG. 4

【図５】

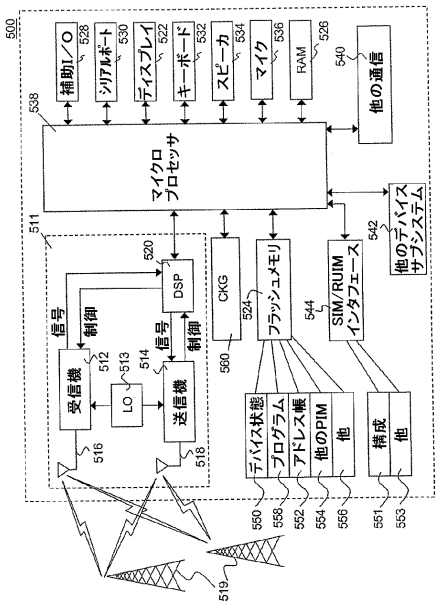
500
補助I／O
528
シリアルポート
530
ディスプレイ
522
キーボード
532
スピーカ
534
マイク
536
RAM
526
他の通信
540
538
マイクロプロセッサ
511
他のデバイスサブシステム
542
520
DSP
信号
制御
信号
制御
受信機
512
513
LO
514
送信機
516
518
519
CKG
560
フラッシュメモリ
524
SIM/RUIM インタフェース
544
デバイス状態
プログラム
アドレス帳
他のPIM
他
構成
他
550
558
552
554
556
551
553

FIG. 5

フロントページの続き

(74)代理人 100113413
弁理士 森下 夏樹
(72)発明者 マイケル シェンフィールド
カナダ国 エル４シー ３エス９ オンタリオ, リッチモンド ヒル, ストックデール クレセント ３８
(72)発明者 アレキサンダー シャーキン
カナダ国 エル３エックス ２ジェイ２ オンタリオ, ニューマーケット, ヘデル クレセント ４３０

Ｆターム(参考) 5J104 AA08 AA09 JA21 LA03 LA06 NA02 NA05 NA27 NA37