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

特許第6181077号
(P6181077)

(45)発行日　平成29年8月16日(2017.8.16)　(24)登録日　平成29年7月28日(2017.7.28)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
H04L 9/14	(2006.01)	H04L	9/00	641
G06F 21/60	(2013.01)	G06F	21/60	320

請求項の数 14　(全 11 頁)

(21)出願番号	特願2014-552359 (P2014-552359)
(86)(22)出願日	平成25年1月12日 (2013.1.12)
(65)公表番号	特表2015-505225 (P2015-505225A)
(43)公表日	平成27年2月16日 (2015.2.16)
(86)国際出願番号	PCT/US2013/021344
(87)国際公開番号	WO2013/106798
(87)国際公開日	平成25年7月18日 (2013.7.18)
審査請求日	平成27年12月14日 (2015.12.14)
(31)優先権主張番号	13/350,661
(32)優先日	平成24年1月13日 (2012.1.13)
(33)優先権主張国	米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　イヴァン・ヒュー・マクリーン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】特権に基づく鍵を生成するための方法および装置

(57)【特許請求の範囲】

【請求項１】

コンピュータを使って特権に基づく鍵を生成するための方法であって、

鍵要求アプリケーションから複数の特権のうちの1つを受信するステップであって、デジタル署名が、前記鍵要求アプリケーション用の前記複数の特権およびプログラムコードに基づく、ステップと、

前記複数の特権のうちの1つが前記鍵要求アプリケーションに関連付けられていることを、前記デジタル署名を使って検証するステップと、

前記複数の特権のうちの1つが検証された場合、

第1の鍵および前記検証された複数の特権のうちの1つを使って、第2の鍵を暗号的に生成するステップと、

前記鍵要求アプリケーションから受信した特権に応じた前記第2の鍵を前記鍵要求アプリケーションに提供するステップとを含む方法。

【請求項２】

前記第1の鍵が共有秘密鍵である、請求項1に記載の方法。

【請求項３】

前記第1の鍵が、デバイスに一意のデバイス鍵である、請求項1に記載の方法。

【請求項４】

前記第2の鍵が暗号化鍵である、請求項1に記載の方法。

【請求項５】

前記第2の鍵が一時セッション鍵である、請求項1に記載の方法。
【請求項６】
前記複数の特権のうちの1つがファイルシステム許可を含む、請求項1に記載の方法。
【請求項７】
前記複数の特権のうちの1つがリソースアクセス権を含む、請求項1に記載の方法。
【請求項８】
前記複数の特権のうちの1つが32ビット整数を含む、請求項1に記載の方法。
【請求項９】
前記第1の鍵および前記検証された複数の特権のうちの1つを使って、前記第2の鍵を暗号的に生成するステップが、前記第1の鍵および前記検証された複数の特権のうちの1つを入力として使ってハッシュを実施して、前記第2の鍵を生成するステップを含む、請求項1に記載の方法。
【請求項１０】
前記第1の鍵および前記検証された複数の特権のうちの1つを使って、前記第2の鍵を暗号的に生成するステップが、前記第1の鍵および前記検証された複数の特権のうちの1つを入力として使って一方向暗号化演算を実施して、前記第2の鍵を生成するステップを含む、請求項1に記載の方法。
【請求項１１】
特権に基づく鍵を生成するための装置であって、
鍵要求アプリケーションから複数の特権のうちの1つを受信するための手段であって、デジタル署名が、前記鍵要求アプリケーション用の前記複数の特権およびプログラムコードに基づく、手段と、
前記複数の特権のうちの1つが前記鍵要求アプリケーションに関連付けられていることを、前記デジタル署名を使って検証するための手段と、
前記特権が検証された場合、第1の鍵および前記検証された複数の特権のうちの1つを使って、第2の鍵を暗号的に生成するための手段と、
前記鍵要求アプリケーションから受信した特権に応じた前記第2の鍵を前記鍵要求アプリケーションに提供するための手段とを備える装置。
【請求項１２】
前記第1の鍵および前記検証された複数の特権のうちの1つを使って、前記第2の鍵を暗号的に生成するための前記手段が、前記第1の鍵および前記検証された複数の特権のうちの1つを入力として使ってハッシュを実施して、前記第2の鍵を生成するための手段を備える、請求項11に記載の装置。
【請求項１３】
前記第1の鍵および前記検証された複数の特権のうちの1つを使って、前記第2の鍵を暗号的に生成するための前記手段が、前記第1の鍵および前記検証された複数の特権のうちの1つを入力として使って一方向暗号化演算を実施して、前記第2の鍵を生成するための手段を備える、請求項11に記載の装置。
【請求項１４】
コンピュータに請求項1から10のいずれか一項に記載の方法を実行させるためのコードを備えるコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は概して、アプリケーションへの安全な暗号化鍵の提供に関する。
【背景技術】
【０００２】
通信の分野には、たとえば、ページング、ワイヤレスローカルループ、インターネットテレフォニー、および衛星通信システムを含む多くのアプリケーションがある。例示的なアプリケーションが、モバイル加入者向けのセルラー電話システムである。(本明細書で

使用される場合、「セルラー」システムという用語は、セルラーおよびパーソナル通信サービス(PCS)システム周波数の両方を包含する。)複数のユーザが共通通信媒体にアクセスできるように設計されたワイヤレス通信システムなど、現代の通信システムが、そのようなセルラーシステム用に開発されている。これらの現代の通信システムは、符号分割多元接続(CDMA)、時分割多元接続(TDMA)、周波数分割多元接続(FDMA)、空間分割多元接続(SDMA)、偏波分割多元接続(PDMA)、または当技術分野で知られている他の変調技法などの多元接続技法に基づき得る。これらの変調技法は、通信システムの複数のユーザから受信した信号を復調し、そうすることによって、通信システムの容量の増大を可能にする。それに関連して、たとえば、改良型モバイル加入者ソフトウェア(AMPS)、モバイル通信用グローバルシステム(GSM(登録商標))、および他のワイヤレスシステムを含む様々なワイヤレス通信システムが確立されている。

【０００３】

FDMAシステムでは、総周波数スペクトルは、いくつかのより小さいサブバンドに分割され、各ユーザには、通信媒体にアクセスするための専用のサブバンドが与えられる。代替として、TDMAシステムでは、総周波数スペクトルは、いくつかのより小さいサブバンドに分割され、各サブバンドは数人のユーザの間で共有され、各ユーザは、そのサブバンドを使って、所定のタイムスロット中に送信することが認められる。CDMAシステムは、システム容量の増大を含む、他のタイプのシステムに勝る潜在的利点をもたらす。CDMAシステムでは、各ユーザは、いつでも周波数スペクトル全体を与えられるが、その送信を、一意のコードを使用して区別する。

【０００４】

安全な通信は通常、安全な鍵を使ったデータの暗号化を伴う。鍵は安全に保管されなければならないので、鍵の記憶および管理技法がもたらされる。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

したがって、安全な鍵の効果的な提供のための技法が必要である。

【課題を解決するための手段】

【０００６】

本発明の態様は、コンピュータを使って特権に基づく鍵を生成するための方法に存在し得る。この方法において、特権がアプリケーションから受けられ、アプリケーションに関連付けられているものとして検証される。コンピュータは、第1の鍵および特権を使って、第2の鍵を暗号的に生成する。第2の鍵は、アプリケーションに与えられる。

【０００７】

本発明のより詳細な態様において、第1の鍵は、共有秘密鍵、および/またはデバイスにとって一意のデバイス鍵であり得る。第2の鍵は、一時セッション鍵などの暗号化鍵であってよい。特権は、ファイルシステム許可またはリソースアクセス権を含んでよく、32ビットの整数で表すことができる。第1の鍵および特権を使って第2の鍵を暗号的に生成することは、第1の鍵および特権を入力として使って、ハッシュ、または同様の一方向暗号化演算を実施して、第2の鍵を生成することを含み得る。

【０００８】

本発明の別の態様は、特権に基づく鍵を生成するための装置であって、アプリケーションから特権を受信するための手段と、特権がアプリケーションに関連付けられていることを検証するための手段と、第1の鍵および特権を使って、第2の鍵を暗号的に生成するための手段と、第2の鍵をアプリケーションに提供するための手段とを備える装置に存在し得る。

【０００９】

本発明の別の態様は、特権に基づく鍵を生成するための装置であって、データを記憶するように構成されたメモリと、アプリケーションから特権を受信し、特権がアプリケーションに関連付けられていることを検証し、特権およびメモリに記憶された第1の鍵を使っ

て、第2の鍵を暗号的に生成し、第2の鍵をアプリケーションに与えるように構成されたプロセッサとを備える装置に存在し得る。

【００１０】

本発明の別の態様は、コンピュータに、アプリケーションから特権を受信させるためのコードと、コンピュータに、特権がアプリケーションに関連付けられていることを検証させるためのコードと、コンピュータに、特権および第1の鍵を使って、暗号的に第2の鍵を生成させるためのコードと、コンピュータに、第2の鍵をアプリケーションに提供させるためのコードとを備えるコンピュータプログラムに存在し得る。

【図面の簡単な説明】

【００１１】

【図１】ワイヤレス通信システムの一例を示すブロック図である。

【図２】本発明による、特権に基づく鍵を生成するための方法の流れ図である。

【図３】特権に基づく鍵を生成するための方法を実装するためのコンピュータの例を示すブロック図である。

【図４】本発明による、特権に基づく鍵を生成するための方法の別の流れ図である。

【発明を実施するための形態】

【００１２】

「例示的な」という言葉は、「例、事例、または例示として機能する」ことを意味するように本明細書で使用される。「例示的な」として本明細書で説明される任意の実施形態は、必ずしも他の実施形態よりも好ましいか、または有利であると解釈されるべきではない。

【００１３】

移動局(MS)、アクセス端末(AT)、ユーザ機器または加入者ユニットとしても知られる遠隔局は、モバイルであっても静止していてもよく、トランシーバ基地局(BTS)またはノードBとしても知られる1つまたは複数の基地局と通信することができる。遠隔局は、1つまたは複数の基地局を通して、無線ネットワークコントローラ(RNC)としても知られる基地局コントローラに、データパケットを送信し、受信する。基地局および基地局コントローラは、アクセスネットワークと呼ばれるネットワークの一部である。アクセスネットワークは、複数の遠隔局の間でデータパケットをトランスポートする。アクセスネットワークは、企業イントラネットまたはインターネットのような、アクセスネットワークの外部の追加のネットワークにさらに接続されてよく、各遠隔局とそのような外部のネットワークとの間でデータパケットをトランスポートすることができる。1つまたは複数の基地局とのアクティブトラフィックチャネル接続を確立した遠隔局は、アクティブ遠隔局と呼ばれ、トラフィック状態にあると言われる。1つまたは複数の基地局とのアクティブトラフィックチャネル接続を確立中である遠隔局は、接続セットアップ状態にあると言われる。遠隔局は、ワイヤレスチャネルを介して通信する任意のデータデバイスであり得る。遠隔局はさらに、限定はしないが、PCカード、コンパクトフラッシュ(登録商標)、外部もしくは内部モデム、またはワイヤレス電話を含む、いくつかのタイプのデバイスのいずれかとすることができる。遠隔局が基地局に信号を送るときに経由する通信リンクは、アップリンクと呼ばれ、逆方向リンクとしても知られる。基地局が遠隔局に信号を送るときに経由する通信リンクは、ダウンリンクと呼ばれ、順方向リンクとしても知られる。

【００１４】

図1を参照すると、ワイヤレス通信システム100は、1つまたは複数のワイヤレス遠隔局(RS)102、1つまたは複数の基地局(BS)104、1つまたは複数の基地局コントローラ(BSC)106、およびコアネットワーク108を含む。コアネットワークは、適切なバックホールを介して、インターネット110および公衆交換電話網(PSTN)112に接続することができる。典型的なワイヤレス移動局には、ハンドヘルド電話またはラップトップコンピュータが含まれ得る。ワイヤレス通信システム100は、符号分割多元接続(CDMA)、時分割多元接続(TDMA)、周波数分割多元接続(FDMA)、空間分割多元接続(SDMA)、偏波分割多元接続(PDMA)、または当技術分野で知られている他の変調技法などのいくつかの多元接続技法のうちのいずれか

1つを採用することができる。

【００１５】

図2～図4を参照すると、本発明の態様は、コンピュータ300を使って特権に基づく鍵を生成するための方法200に存在し得る。この方法において、アプリケーション430から、特権420が受けられ(ステップ210)、アプリケーションに関連付けられているものとして検証される(ステップ220)。コンピュータ300は、第1の鍵450および特権を使って、第2の鍵440を暗号的に生成する(ステップ230)。第2の鍵440は、アプリケーションに与えられる(ステップ240)。

【００１６】

本発明のより詳細な態様において、第1の鍵450は、共有秘密鍵、および/またはデバイスに一意のデバイス鍵であり得る。さらに、第1の鍵は、鍵として機能することができる識別子であり得る。第2の鍵440は、一時セッション鍵などの暗号化鍵であってよい。特権420は、ファイルシステム許可またはリソースアクセス権を含んでよく、たとえば32ビット、64ビット、128ビットの整数などの整数で表すことができる。第1の鍵および特権を使って第2の鍵を暗号的に生成することは、第1の鍵および特権を入力として使って、ハッシュまたはHMAC(ハッシュベースメッセージ認証コード)など、何らかの適切な一方向暗号化演算を実施して、第2の鍵を生成することを含み得る。

【００１７】

遠隔局102は、安全なハードウェア320を有するプロセッサ310と、メモリ(および/またはディスクドライブ)330と、ディスプレイ340と、キーパッドまたはキーボード350とを含むコンピュータ300であってよい。コンピュータは、マイクロフォン、スピーカ、カメラ、ウェブブラウザソフトウェア等も含む場合がある。さらに、遠隔局102は、インターネット110のようなネットワークを介して通信するためのUSB、イーサネット(登録商標)および類似のインターフェース360も含む場合があり、移動局であってもよい。

【００１８】

本発明の別の態様は、特権に基づく鍵を生成するための装置300であって、アプリケーション430から特権420を受けるための手段310と、特権がアプリケーションに関連付けられていることを検証するための手段310と、第1の鍵450および特権を使って、第2の鍵440を暗号的に生成するための手段310と、第2の鍵をアプリケーションに提供するための手段310とを備える装置に存在し得る。

【００１９】

本発明の別の態様は、特権に基づく鍵を生成するための装置300であって、データを記憶するように構成されたメモリ330と、アプリケーション430から特権420を受け、特権がアプリケーションに関連付けられていることを検証し、特権およびメモリに記憶された第1の鍵450を使って、第2の鍵440を暗号的に生成し、第2の鍵をアプリケーションに提供するように構成されたプロセッサ310とを備える装置に存在し得る。

【００２０】

本発明の別の態様は、コンピュータ300に、アプリケーション430から特権420を受けさせるためのコードと、コンピュータに、特権がアプリケーションに関連付けられていることを検証させるためのコードと、コンピュータに、特権および第1の鍵450を使って、暗号的に第2の鍵440を生成させるためのコードと、コンピュータに、第2の鍵をアプリケーションに提供させるためのコードとを備えるコンピュータ可読媒体330を備えるコンピュータプログラム製品に存在し得る。

【００２１】

本発明の態様では、与えられた特権420に基づいて暗号化鍵440を生成するための機構が提供される。アプリケーション430は、所与の特権を提示することによって、クライアントプラットフォーム300に対して鍵440を要求することができる。鍵440が発行される前に、要求側アプリケーションは、アプリケーションが、与えられた特権の有効な保持者であることを保証するために、プラットフォームによって認可される。コードサイニングが通常、アプリケーション430の安全性および認可と、アプリケーションに付与されている特

権420とを定着させるのに使われる。

【００２２】

生成された暗号化鍵440は、データ、ファイルまたは機密性通信を暗号化するのに使うことができる。互いとの安全な通信を確立することを望む、またはファイルもしくはデータを共有したいと思うアプリケーションは、一意の特権420を確立し、合意することによって、そうすることができる。典型的なシナリオにおいて、アプリケーション開発者は、適切な特権を宣言し、アプリケーション430は次いで、機関によってデジタル署名される。

【００２３】

特権420が鍵要求アプリケーション430に関連付けられているということの検証は、米国特許第7,743,407号に記載されているアプリケーションおよび関連特権(許可)を使って作成されたデジタル署名を使って遂行することができる。米国特許第7,743,407号は、参照によって本明細書に組み込まれている。

【００２４】

提供される機構には、従来の鍵管理/鍵記憶方式に勝るいくつかの利点がある。この機構は、従来の一元的な「安全なキーストア」の必要を本質的になくす。この機構は、アプリケーションが同じデバイス上で、それとも異なるデバイス上で稼動しているかにかかわらず、アプリケーションが情報を共有し、または安全な通信を確立するための簡単な機構を提供する。この機構は、コードサイニングの既存の安全性と、BREWなどのクライアント動作環境およびプラットフォーム460によって提供される最低限の特権セキュリティモデルとを活用する。

【００２５】

クライアント環境460は、アプリケーション430から特権420を受け(ステップ210)、特権がアプリケーションに関連付けられていることを検証することができる(ステップ220)。クライアント環境460は次いで、検証された特権を、第2の鍵440の生成(ステップ230)のために、安全なハードウェア410にフォワードすることができる(ステップ225)。

【００２６】

第2の鍵440は、与えられた特権420に対して一方向暗号化演算を実施することによって生成することができる。たとえば、第2の鍵は、与えられた特権および何らかの不変/秘密デバイス鍵または識別子450に対してハッシュを実施することによって生成することができる。より具体的には、次のようになる。

【００２７】

第2の鍵=HASH(特権+デバイス鍵)。

【００２８】

別の態様では、複数のデバイスにわたってアプリケーションの間でデータを安全に共有することができるようにするのに、共有秘密鍵450が使われ得る。この態様において、第2の鍵440は、特権420と、複数のデバイスの間で共有される秘密鍵450とに対してハッシュを実施することによって生成することができる。より具体的には、次のようになる。

【００２９】

第2の鍵=HASH(特権+共有秘密鍵)。

【００３０】

この手法の利益は、共有秘密鍵の直接使用が必要とされないことである。また、異なるデバイス上のアプリケーションのインスタンスの間で、専用鍵の確立または鍵の共有は必要とされない。

【００３１】

第2の鍵440を生成するための一方向暗号化演算は、安全なハードウェア320/410によって(および/またはメモリ保護境界内で)実施することができる。第1の鍵(たとえば、デバイス鍵または共有秘密鍵450)は、呼出し側アプリケーション430にも非システムコードにも暴露されることはない。

【００３２】

セキュリティは、最小特権およびコードサイニングの概念の上に構築することができる。アプリケーション430が、安全な鍵440へのアクセスを得ることを望む場合、アプリケーション開発者は、特権420を決定し、機関によって署名されるべきアプリケーションを提出するとき、その特権を含める。特権は、特権がこのアプリケーションに一意であり得るという理解に基づいて生成または選択することができ、他のどのアプリケーションにも決して認められることはない。

【００３３】

代替として、アプリケーション開発者が、アプリケーション430が他の信頼できるアプリケーションと情報を安全に共有することを望む場合、特権420は、確立された信頼関係に基づいて生成/選択/合意されなければならない。他のアプリケーションは、特権所有者/作成者の承認を得た、当該の特権を用いて、署名されるのに成功するだけである。特権を用いて署名されるための他のどの要求も、拒絶されることになる。

【００３４】

第2の鍵440は「オンザフライ」で生成されるので、アプリケーションが、安全なキーストアを維持する必要はない。デバイス鍵450を使うとき、生成された鍵440は、特権ごと、デバイスごとに一意である。同じデバイス上での所与の特権420をもつ鍵についての要求は、どのアプリケーションが要求を行ったか、またはいつ要求が行われるか、または時間の経過とともに何度要求が繰り返されるかにかかわらず、常に同じ第2の鍵440を戻す。鍵の不変性により、呼出し側アプリケーション430は、鍵管理または安全な鍵記憶のいかなる責任も軽減される。第2の鍵440は、アプリケーションによって使われ、次いで、破棄されてよい。

【００３５】

また、アプリケーションは、異なるが関連する目的のために、任意の数の異なる特権420または特権セットを自由に用いることもできる。したがって、たとえば、アプリケーション430は、他のどのアプリケーションとも共有したくないデータまたはファイルを保護するための1つまたは複数の特権を確保することができる。アプリケーション430は、何らかの他の情報を、所与の信頼の輪の中の限られたアプリケーションセットと安全に共有するのに使うことができる別の特権(または特権セット)に合意する場合がある。また、アプリケーション430は、何らかの他の情報を保護し、異なるセキュリティ要件または信頼レベルである異なるアプリケーションセットと共有するのに、さらに別の特権を用いることができる。

【００３６】

一例として、ゲームアプリケーション430は、そのライセンス情報を暗号化するためにのみ使われる暗号化鍵440を取り出すのに、専用の特権420を用いることができる。特権および関連付けられた鍵は、アプリケーションに一意であり、他のどのアプリケーションとも、異なるデバイス上で稼動する同じアプリケーションであっても共有されない。

【００３７】

同じゲームアプリケーション430は、クライアント証明書を暗号化するのに使われる暗号化鍵440'を取り出すのに、異なる特権420'を用いることができる。これらの証明書は、同じベンダからの他のアプリケーションと(または異なるベンダからの信頼されるアプリケーションであっても)安全に共有することができる。この場合、同じデバイス上で稼動するアプリケーションに共有が制限されることが意図される。

【００３８】

さらに、同じゲームアプリケーション430は、高得点およびゲーム状態情報を暗号化するのに使われる鍵440''を取り出すのに、さらに別の異なる特権420''を用いることができる。この場合の鍵生成は、特権420''および共有の秘密450に基づき得る。このようにして保護される情報は、同じデバイス上のアプリケーション、または異なるデバイス上で稼動する、必要な特権をもつアプリケーションの間で安全に共有することができる。

【００３９】

異なる特権420は、関連付けられた暗号化鍵440とともに、同じリソースへの異なるタイ

プのアクセスを制御するのに使うことができる。たとえば、暗号化ファイルシステムは、特権A/鍵Xが読出しアクセスを認めることができ、特権B/鍵Yが読取り/書込みアクセスを認めることができるような特権を強制し得る。

【００４０】

情報および信号は、様々な異なる技術および技法のいずれかを使用して表され得ることが、当業者には理解されよう。たとえば、上記の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁界または磁性粒子、光場または光学粒子、あるいはそれらの任意の組合せによって表され得る。

【００４１】

当業者は、本明細書で開示する実施形態に関して説明した様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップが、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることをさらに諒解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップを、上記では概してそれらの機能性に関して説明した。そのような機能性をハードウェアとして実装するか、ソフトウェアとして実装するかは、特定の適用例および全体的なシステムに課される設計制約に依存する。当業者は、説明した機能性を特定の適用例ごとに様々な方法で実装し得るが、そのような実装の決定は、本発明の範囲からの逸脱を生じるものと解釈すべきではない。

【００４２】

本明細書で開示された実施形態に関連して説明された様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または、本明細書で説明された機能を実施するように設計されたそれらの任意の組合せで、実装または実施され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であり得る。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、あるいは任意の他のそのような構成として実装され得る。

【００４３】

本明細書で開示する実施形態に関して説明した方法またはアルゴリズムのステップは、直接ハードウェアで具現化されるか、プロセッサによって実行されるソフトウェアモジュールで具現化されるか、またはその2つの組合せで具現化され得る。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体内に常駐することができる。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替として、記憶媒体はプロセッサと一体であり得る。プロセッサおよび記憶媒体はASIC中に常駐し得る。ASICはユーザ端末中に常駐し得る。代替として、プロセッサおよび記憶媒体は、ユーザ端末中に個別構成要素として常駐し得る。

【００４４】

1つまたは複数の例示的な実施形態では、説明された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実装され得る。コンピュータプログラムとしてソフトウェア中で実装した場合、機能は、1つまたは複数の命令またはコードとしてコンピュータ可読記録媒体上に記憶され得る。コンピュータ可読記録媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にするコンピュータ記憶媒体を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読記録媒体は、RAM、ROM、

EEPROM、CD-ROMまたは他の光ディスクストレージ、磁気ディスクストレージまたは他の磁気ストレージデバイス、あるいは命令またはデータ構造の形態の所望のプログラムコードを記憶するために使用でき、コンピュータによってアクセスできる、任意の他の媒体を含むことができる。本明細書で使用される場合、ディスク(disk)およびディスク(disc)は、コンパクトディスク(CD)、レーザーディスク(登録商標)、光ディスク、デジタル多用途ディスク(DVD)、フロッピー(登録商標)ディスク、およびブルーレイディスクを含み、ディスク(disk)は、通常、磁気的にデータを再生し、ディスク(disc)は、レーザーで光学的にデータを再生する。上記の組合せもコンピュータ可読記録媒体の範囲内に含めるべきである。コンピュータ可読記録媒体は、一時的な伝搬信号を含まないように非一時的であってよい。

【００４５】

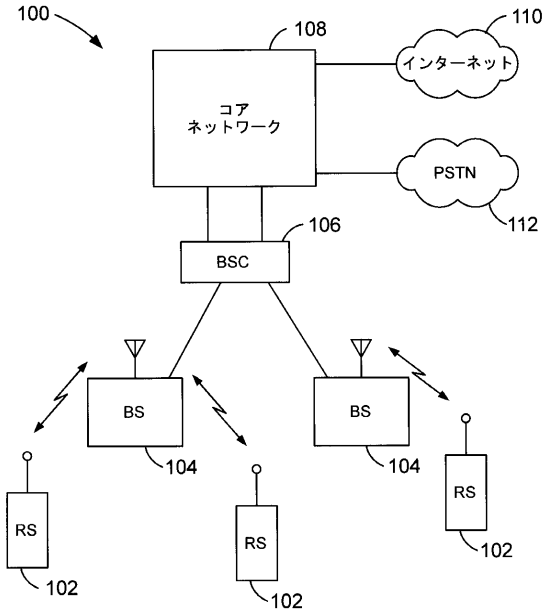
開示された実施形態の上記の説明は、いかなる当業者も本発明を作製または使用できるようにするために提供される。これらの実施形態への様々な修正が当業者には容易に明らかになり、本明細書に定義された一般原理は、本発明の趣旨または範囲を逸脱することなしに他の実施形態に適用することができる。したがって、本発明は、本明細書に示された実施形態に限定されるものではなく、本明細書で開示された原理および新規の特徴に一致する最大の範囲を与えられるものである。

【符号の説明】

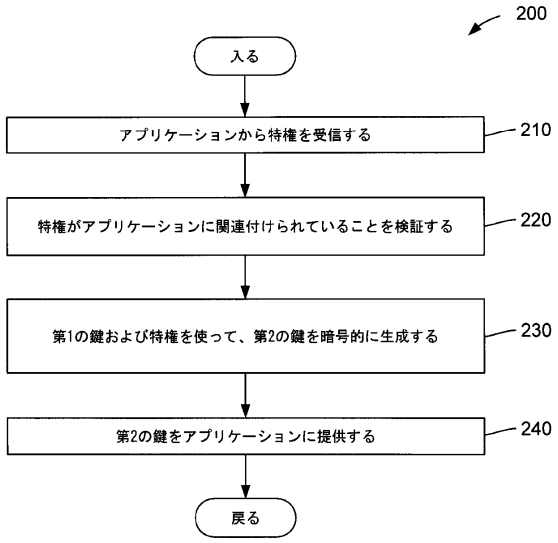
【００４６】

100　ワイヤレス通信システム
102　ワイヤレス遠隔局(RS)、遠隔局
104　基地局(BS)
106　基地局コントローラ(BSC)
108　コアネットワーク
110　インターネット
112　公衆交換電話網(PSTN)
300　コンピュータ、装置、クライアントプラットフォーム
310　プロセッサ、手段
320　安全なハードウェア
330　メモリ、コンピュータ可読記録媒体
340　ディスプレイ
350　キーパッド、キーボード
360　インターフェース

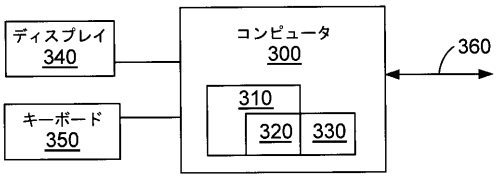
【図１】


100
108
110
インターネット
コア
ネットワーク
PSTN
112
106
BSC
BS
BS
104
104
RS
RS
RS
102
102
102

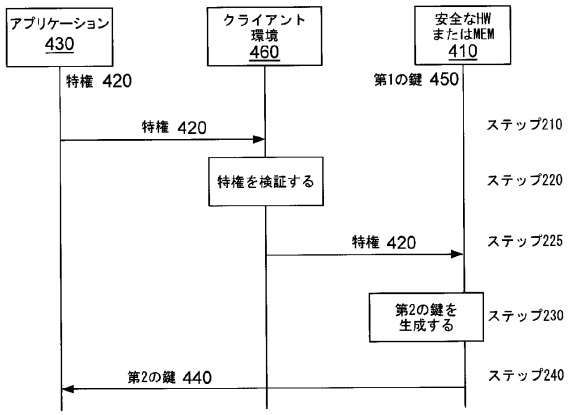
【図２】


200
入る
アプリケーションから特権を受信する
210
特権がアプリケーションに関連付けられていることを検証する
220
第1の鍵および特権を使って、第2の鍵を暗号的に生成する
230
第2の鍵をアプリケーションに提供する
240
戻る

【図３】


ディスプレイ
340
キーボード
350
コンピュータ
300
310
320
330
360

【図４】


アプリケーション
430
クライアント
環境
460
安全なHW
またはMEM
410
特権 420
第1の鍵 450
特権 420
ステップ210
特権を検証する
ステップ220
特権 420
ステップ225
第2の鍵を
生成する
ステップ230
第2の鍵 440
ステップ240

フロントページの続き

(72)発明者　ローレンス・ジー・ランドブレード
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ブライアン・ハロルド・ケリー
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ロバート・ジー・ウォーカー
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　行田　悦資

(56)参考文献　特開２０００－２４２４９１（ＪＰ，Ａ）
特開２００５－２３６９６３（ＪＰ，Ａ）
特開２００２－３００１５８（ＪＰ，Ａ）
特開２０１１－０２８６８８（ＪＰ，Ａ）
特表２００５－５１７２２０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／６０
Ｈ０４Ｌ　　９／１４