(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7189856号
(P7189856)

(45)発行日　令和4年12月14日(2022.12.14)

(24)登録日　令和4年12月6日(2022.12.6)

(51)国際特許分類

H04L 9/32 (2006.01)	H04L	9/32	200B
G06F 21/33 (2013.01)	G06F	21/33	
G06F 21/31 (2013.01)	G06F	21/31	
G06F 21/62 (2013.01)	G06F	21/62	

FI

請求項の数　20　（全26頁）

(21)出願番号　特願2019-190731(P2019-190731)
(22)出願日　令和1年10月18日(2019.10.18)
(65)公開番号　特開2020-78067(P2020-78067A)
(43)公開日　令和2年5月21日(2020.5.21)
審査請求日　令和4年10月14日(2022.10.14)
(31)優先権主張番号　16/184,811
(32)優先日　平成30年11月8日(2018.11.8)
(33)優先権主張国・地域又は機関
米国(US)
早期審査対象出願

(73)特許権者　504407000
パロ アルト リサーチ センター インコーポレイテッド
アメリカ合衆国 カリフォルニア州 ９４３０４ パロ アルト カイオーテ ヒル ロード ３３３３
(74)代理人　100094569
弁理士　田中 伸一郎
(74)代理人　100109070
弁理士　須田 洋之
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100086771
弁理士　西島 孝喜
(74)代理人　100109335

最終頁に続く

(54)【発明の名称】　モバイルデバイスを有するユーザがスタンドアロンコンピューティングデバイスの能力にアクセスすることをセキュアに可能にするためのシステム及び方法

(57)【特許請求の範囲】

【請求項１】

スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするためのコンピュータ実装方法であって、

前記スタンドアロンコンピューティングデバイスによって、ユーザに関連付けられたモバイルコンピューティングデバイスから、前記スタンドアロンコンピューティングデバイスの能力にアクセスする第１のコマンドを受信することであって、

前記第１のコマンドが、短命なユーザ識別子を含み、

前記短命なユーザ識別子が、短命な鍵とユーザ固有のメタデータとを含み、

前記短命な鍵が、前記第１のコマンドに対して固有であり、前記短命な鍵が、前記スタンドアロンコンピューティングデバイスによって直接アクセス可能ではないネットワークサービスによって前記第１のコマンドに対して生成され、

前記ユーザ固有のメタデータが、ユーザによって前もって登録されるとともに、前記ネットワークサービスによって記憶され、

前記短命なユーザ識別子が、前記ネットワークサービスの秘密鍵でデジタル署名される、ことと、

前記スタンドアロンコンピューティングデバイスによって、前記ネットワークサービスの公開鍵を使用して、前記デジタル署名された短命なユーザ識別子が前記ネットワークサービスによって生成されたことを検証することと、

前記スタンドアロンコンピューティングデバイスによって、前記スタンドアロンコンピ

ューティングデバイスの前記能力にアクセスすることによって前記ユーザ固有のメタデータに基づいて前記第１のコマンドを実行することで前記スタンドアロンコンピューティングデバイスへのユーザアクセスを引き起こすことと、を含む、方法。

【請求項２】

前記スタンドアロンコンピューティングデバイスによって、前記モバイルコンピューティングデバイスに、前記第１のコマンドの成功した実行を示す通知を送信することを更に含み、

前記モバイルコンピューティングデバイスが、前記通知を前記ネットワークサービスに送信し、これにより、前記ネットワークサービスにデータ構造内のエントリを更新させ、

前記エントリが、前記ユーザ固有のメタデータに対応する、請求項１に記載の方法。

【請求項３】

前記スタンドアロンコンピューティングデバイスによって、

ＷｉＦｉ－Ｄｉｒｅｃｔと、

Ｂｌｕｅｔｏｏｔｈと、

近距離無線通信（ＮＦＣ）と、

無線プロトコルと、

無線アクセスポイント又は無線ルータを伴わない無線プロトコルと、のうちの１つ以上に基づいて無線で前記モバイルコンピューティングデバイスとペアリングすることを更に含む、請求項１に記載の方法。

【請求項４】

前記デジタル署名された短命なユーザ識別子は、前記スタンドアロンコンピューティングデバイスが前記第１のコマンドを受信する前に、前記モバイルコンピューティングデバイスによって受信され、

前記ユーザが前記デジタル署名された短命なユーザ識別子を受信する前に、前記ユーザは、

前記モバイルコンピューティングデバイス上のアプリケーションと、

ウェブサイトと、

前記モバイルコンピューティングデバイスの構成要素を介した生体認識の形態と、

前記アプリケーション又は前記ウェブサイトにアクセスするための前記ユーザのパスワードと、のうちの１つ以上に基づいて前記ネットワークサービスによって認証される、請求項１に記載の方法。

【請求項５】

前記短命なユーザ識別子が、前記ネットワークサービスから前記モバイルコンピューティングデバイスにネットワークを介して送信され、

前記第１のコマンドを前記スタンドアロンコンピューティングデバイスに送信する前に、前記短命なユーザ識別子は、前記モバイルコンピューティングデバイスによって前記ネットワークサービスの前記公開鍵を使用して更に検証され、

前記第１のコマンドが、前記モバイルコンピューティングデバイスによって前記スタンドアロンコンピューティングデバイスに送信され、

前記ユーザ固有のメタデータが、前記ネットワークサービスによって記憶され、これにより、前記スタンドアロンコンピューティングデバイスは、前記モバイルコンピューティングデバイスが前記ネットワークサービスによって既に許可されているユーザに関連付けられていることを検証することが可能になる、請求項１に記載の方法。

【請求項６】

前記短命なユーザ識別子が、前記短命なユーザ識別子及びメッセージ認証コードの暗号化に基づいて前記モバイルコンピューティングデバイスから隠され、

前記暗号化は、前記スタンドアロンコンピューティングデバイスと前記ネットワークサービスとの間のセキュアな暗号ハンドシェイクプロトコルに基づいて導き出されたセッション鍵を使用して実行され、

前記セキュアな暗号ハンドシェイクプロトコルは、前記モバイルコンピューティングデ

バイスを信頼されていないリレーとして利用する、請求項１に記載の方法。
【請求項７】
前記ネットワークサービスが、クラウドベースのサーバを含み、前記スタンドアロンコンピューティングデバイスが、いかなるネットワーク又はいかなる無線アクセスポイントを介しても前記クラウドベースのサーバに接続されていない、請求項１に記載の方法。
【請求項８】
前記ネットワークサービスが前記デジタル署名された短命なユーザ識別子を前記モバイルコンピューティングデバイスに送信する前に、前記方法は、前記モバイルコンピューティングデバイスと前記ネットワークサービスとの間に第１のセキュア接続をトランスポート層セキュリティプロトコルに基づいて確立することを更に含み、
前記スタンドアロンコンピューティングデバイスが前記第１のコマンドを受信する前に、前記方法は、前記モバイルコンピューティングデバイスと前記スタンドアロンコンピューティングデバイスとの間に第２のセキュア接続を前記トランスポート層セキュリティプロトコルに基づいて確立することを更に含む、請求項１に記載の方法。
【請求項９】
前記スタンドアロンコンピューティングデバイスが、
多機能プリンタと、
モノのインターネット（ＩｏＴ）対応デバイスと、
ロボットと、のうちの１つ以上である、請求項１に記載の方法。
【請求項１０】
スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするためのコンピュータシステムであって、
プロセッサと、
前記プロセッサによって実行されると、前記プロセッサに方法を実行させる命令を記憶する記憶デバイスと、を含み、前記方法が、
前記スタンドアロンコンピューティングデバイスによって、ユーザに関連付けられたモバイルコンピューティングデバイスから、前記スタンドアロンコンピューティングデバイスの能力にアクセスする第１のコマンドを受信することであって、
前記第１のコマンドが、短命なユーザ識別子を含み、
前記短命なユーザ識別子が、短命な鍵とユーザ固有のメタデータとを含み、
前記短命な鍵が、前記第１のコマンドに対して固有であり、前記短命な鍵が、前記スタンドアロンコンピューティングデバイスによって直接アクセス可能ではないネットワークサービスによって前記第１のコマンドに対して生成され、
前記ユーザ固有のメタデータが、ユーザによって前もって登録されるとともに、前記ネットワークサービスによって記憶され、
前記短命なユーザ識別子が、前記ネットワークサービスの秘密鍵でデジタル署名される、ことと、
前記スタンドアロンコンピューティングデバイスによって、前記ネットワークサービスの公開鍵を使用して、前記デジタル署名された短命なユーザ識別子が前記ネットワークサービスによって生成されたことを検証することと、
前記スタンドアロンコンピューティングデバイスによって、前記スタンドアロンコンピューティングデバイスの前記能力にアクセスすることによって前記ユーザ固有のメタデータに基づいて前記第１のコマンドを実行することで前記スタンドアロンコンピューティングデバイスへのユーザアクセスを引き起こすことと、を含む、コンピュータシステム。
【請求項１１】
前記スタンドアロンコンピューティングデバイスによって、前記モバイルコンピューティングデバイスに、前記第１のコマンドの成功した実行を示す通知を送信することを更に含み、
前記モバイルコンピューティングデバイスが、前記通知を前記ネットワークサービスに送信し、これにより、前記ネットワークサービスにデータ構造内のエントリを更新させ、

前記エントリが、前記ユーザ固有のメタデータに対応する、請求項１０に記載のコンピュータシステム。
【請求項１２】
前記方法が、
前記スタンドアロンコンピューティングデバイスによって、
ＷｉＦｉ－Ｄｉｒｅｃｔと、
Ｂｌｕｅｔｏｏｔｈと、
近距離無線通信（ＮＦＣ）と、
無線プロトコルと、
無線アクセスポイント又は無線ルータを伴わない無線プロトコルと、のうちの１つ以上に基づいて無線で前記モバイルコンピューティングデバイスとペアリングすることを更に含む、請求項１０に記載のコンピュータシステム。
【請求項１３】
前記デジタル署名された短命なユーザ識別子は、前記スタンドアロンコンピューティングデバイスが前記第１のコマンドを受信する前に、前記モバイルコンピューティングデバイスによって受信され、
前記ユーザが前記デジタル署名された短命なユーザ識別子を受信する前に、前記ユーザは、
前記モバイルコンピューティングデバイス上のアプリケーションと、
ウェブサイトと、
前記モバイルコンピューティングデバイスの構成要素を介した生体認識の形態と、
前記アプリケーション又は前記ウェブサイトにアクセスするための前記ユーザのパスワードと、のうちの１つ以上に基づいて前記ネットワークサービスによって認証される、請求項１０に記載のコンピュータシステム。
【請求項１４】
前記短命なユーザ識別子が、前記ネットワークサービスから前記モバイルコンピューティングデバイスにネットワークを介して送信され、
前記第１のコマンドを前記スタンドアロンコンピューティングデバイスに送信する前に、前記短命なユーザ識別子は、前記モバイルコンピューティングデバイスによって前記ネットワークサービスの前記公開鍵を使用して更に検証され、
前記第１のコマンドが、前記モバイルコンピューティングデバイスによって前記スタンドアロンコンピューティングデバイスに送信され、
前記ユーザ固有のメタデータが、前記ネットワークサービスによって記憶され、これにより、前記スタンドアロンコンピューティングデバイスは、前記モバイルコンピューティングデバイスが前記ネットワークサービスによって既に許可されているユーザに関連付けられていることを検証することが可能になる、請求項１０に記載のコンピュータシステム。
【請求項１５】
前記短命なユーザ識別子が、前記短命なユーザ識別子及びメッセージ認証コードの暗号化に基づいて前記モバイルコンピューティングデバイスから隠され、
前記暗号化は、前記スタンドアロンコンピューティングデバイスと前記ネットワークサービスとの間のセキュアな暗号ハンドシェイクプロトコルに基づいて導き出されたセッション鍵を使用して実行され、
前記セキュアな暗号ハンドシェイクプロトコルは、前記モバイルコンピューティングデバイスを信頼されていないリレーとして利用する、請求項１０に記載のコンピュータシステム。
【請求項１６】
前記ネットワークサービスが、クラウドベースのサーバを含み、前記スタンドアロンコンピューティングデバイスが、いかなるネットワーク又はいかなる無線アクセスポイントを介しても前記クラウドベースのサーバに接続されていない、請求項１０に記載のコンピュータシステム。

【請求項１７】
前記ネットワークサービスが前記デジタル署名された短命なユーザ識別子を前記モバイルコンピューティングデバイスに送信する前に、前記方法は、前記モバイルコンピューティングデバイスと前記ネットワークサービスとの間に第１のセキュア接続をトランスポート層セキュリティプロトコルに基づいて確立することを更に含み、
前記スタンドアロンコンピューティングデバイスが前記第１のコマンドを受信する前に、前記方法は、前記モバイルコンピューティングデバイスと前記スタンドアロンコンピューティングデバイスとの間に第２のセキュア接続を前記トランスポート層セキュリティプロトコルに基づいて確立することを更に含む、請求項１０に記載のコンピュータシステム。
【請求項１８】
前記スタンドアロンコンピューティングデバイスが、
多機能プリンタと、
モノのインターネット（ＩｏＴ）対応デバイスと、
ロボットと、のうちの１つ以上である、請求項１０に記載のコンピュータシステム。
【請求項１９】
スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための装置であって、
前記スタンドアロンコンピューティングデバイスによって、ユーザに関連付けられたモバイルコンピューティングデバイスから、前記スタンドアロンコンピューティングデバイスの能力にアクセスする第１のコマンドを受信するように構成された通信モジュールであって、
前記第１のコマンドが、短命なユーザ識別子を含み、
前記短命なユーザ識別子が、短命な鍵とユーザ固有のメタデータとを含み、
前記短命な鍵が、前記第１のコマンドに対して固有であり、前記短命な鍵が、前記スタンドアロンコンピューティングデバイスによって直接アクセス可能ではないネットワークサービスによって前記第１のコマンドに対して生成され、
前記ユーザ固有のメタデータが、ユーザによって前もって登録されるとともに、前記ネットワークサービスによって記憶され、
前記短命なユーザ識別子が、前記ネットワークサービスの秘密鍵でデジタル署名される、通信モジュールと、
前記スタンドアロンコンピューティングデバイスによって、前記ネットワークサービスの公開鍵を使用して、前記デジタル署名された短命なユーザ識別子が前記ネットワークサービスによって生成されたことを検証するように構成された検証モジュールと、
前記スタンドアロンコンピューティングデバイスによって、前記スタンドアロンコンピューティングデバイスの前記能力にアクセスすることによって前記ユーザ固有のメタデータに基づいて前記第１のコマンドを実行することで前記スタンドアロンコンピューティングデバイスへのユーザアクセスを引き起こすように構成されたコマンド実行モジュールと、を含む、装置。
【請求項２０】
前記短命なユーザ識別子が、前記ネットワークサービスから前記モバイルコンピューティングデバイスにネットワークを介して送信され、
前記第１のコマンドを前記スタンドアロンコンピューティングデバイスに送信する前に、前記短命なユーザ識別子は、前記モバイルコンピューティングデバイスによって前記ネットワークサービスの前記公開鍵を使用して更に検証され、
前記第１のコマンドが、前記モバイルコンピューティングデバイスによって前記スタンドアロンコンピューティングデバイスに送信され、
前記ユーザ固有のメタデータが、前記ネットワークサービスによって記憶され、これにより、前記スタンドアロンコンピューティングデバイスは、前記モバイルコンピューティングデバイスが前記ネットワークサービスによって既に許可されているユーザに関連付けられていることを検証することが可能になる、請求項１９に記載の装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、一般に、電子通信に関連する。より具体的には、本開示は、モバイルデバイスを有するユーザがスタンドアロンコンピューティングデバイスの能力にアクセスすることをセキュアに可能にするためのシステム及び方法に関する。
【０００２】
インターネット及び電子商取引の急増により、膨大な量のデジタルコンテンツが作成され続けている。従来のシステムでは、ユーザが、ユーザのモバイルデバイスを介して、コンピューティングデバイス上のデジタルコンテンツ又はコンピューティングデバイスの能力にアクセスすることを所望するとき、アクセスされるコンピューティングデバイスは、典型的にはネットワーク上にあり、そのネットワーク上のコンピューティングデバイスへのインターフェースを介してアクセス可能である。例えば、ユーザが多機能プリンタの能力にアクセスする（例えば、多機能プリンタ上で文書を印刷する）ことを所望する場合、ユーザのモバイルデバイス及び多機能プリンタの両方は、同じネットワークを介してアクセス可能でなければならない。しかしながら、この多機能プリンタがネットワーク上にない場合、ユーザは多機能プリンタにアクセスすることはできない。
【０００３】
更に、特定のアプリケーション固有の動作は、典型的にはネットワークサービスを介して達成され、ネットワークサービスは、様々なコンピューティングデバイスの動作を管理することができる。例えば、ユーザを認証すること、特定のコンピューティングデバイスの能力にアクセスする権限をユーザに与えること、ユーザのアカウント特権を更新すること、及びユーザ固有のパーソナライゼーションを提供することは、典型的には、ネットワークサービスによって管理及び監視されるタスクである。ネットワークサービスは、クラウドベースのサーバ、又は複数の他のデバイスを管理することができる任意の他のコンピューティングデバイス若しくはコンピューティングエンティティを含むことができ、これらの例示的なタイプのアプリケーション固有の動作を実行することができる。
【０００４】
従来のシステムでは、モバイルデバイスを有するユーザは、コンピューティングデバイス（例えば、多機能プリンタ）が、モバイルデバイスからもアクセス可能であるネットワーク上にある場合にのみ、そのコンピューティングデバイスの機能にアクセスすることができる。ユーザは、これらのアプリケーション固有の動作を実行するために、他のコンピューティングデバイスに頼る必要があり得、こうした他のコンピューティングデバイスは、特定のコンピューティングデバイスの機能にアクセスするユーザの能力を限定又は制限することができる。この依存を軽減することへのいくつかの現在の解決策は、コンピューティングデバイスに接続された管理コンピューティングエンティティの存在を想定しており、管理コンピューティングエンティティは、上述のアプリケーション固有の動作を実行する。一例は、コンピューティングデバイスが、管理されているデバイスのフリート（例えば、多機能プリンタのフリート）の一部である場合である。しかしながら、モバイルデバイスを有するユーザが、管理コンピューティングエンティティを使用せずに、「スタンドアロン」コンピューティングデバイス（すなわち、ネットワークサービス又はクラウドベースのサーバを介してアクセスすることができないコンピューティングデバイス）の能力にアクセスすることができる機構は、現在存在しない。
【０００５】
一実施形態は、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にする。動作中、システムは、スタンドアロンコンピューティングデバイスによって、ユーザに関連付けられたモバイルコンピューティングデバイスから、スタンドアロンコンピューティングデバイスの能力にアクセスする第１のコマンドを受信し、第１のコマンドは、短命な鍵を含み、かつユーザ固有のメタデータを示す、短命なユーザ識別子を含んでおり、短命なユーザ識別子は、第１のコマンドに固有であり、短命な鍵は、ネットワークサ

ービスによって生成されており、短命なユーザ識別子は、ネットワークサービスの秘密鍵でデジタル署名されており、スタンドアロンコンピューティングデバイスは、ネットワークサービスによって直接アクセス可能ではない。システムは、スタンドアロンコンピューティングデバイスによって、ネットワークサービスの公開鍵を使用して、デジタル署名された短命なユーザ識別子がネットワークサービスによって生成されたことを検証する。システムは、スタンドアロンコンピューティングデバイスによって、スタンドアロンコンピューティングデバイスの能力にアクセスすることによってユーザ固有のメタデータに基づいて第１のコマンドを実行する。

【０００６】

いくつかの実施形態では、システムは、スタンドアロンコンピューティングデバイスによって、モバイルコンピューティングデバイスに、第１のコマンドの成功した実行を示す通知を送信し、モバイルコンピューティングデバイスは、通知をネットワークサービスに送信し、これにより、ネットワークサービスにデータ構造内のエントリを更新させ、エントリは、ユーザ固有のメタデータに対応する。

【０００７】

いくつかの実施形態では、システムは、スタンドアロンコンピューティングデバイスによって、ＷｉＦｉ－Ｄｉｒｅｃｔと、Ｂｌｕｅｔｏｏｔｈ（登録商標）と、近距離無線通信（ＮＦＣ）と、無線プロトコルと、無線アクセスポイント又は無線ルータを伴わない無線プロトコルと、のうちの１つ以上に基づいて無線でモバイルコンピューティングデバイスとペアリングする。

【０００８】

いくつかの実施形態では、デジタル署名された短命なユーザ識別子は、スタンドアロンコンピューティングデバイスが第１のコマンドを受信する前に、モバイルコンピューティングデバイスによって受信され、ユーザは、ユーザがデジタル署名された短命なユーザ識別子を受信する前に、モバイルコンピューティングデバイス上のアプリケーションと、ウェブサイトと、モバイルコンピューティングデバイスの構成要素を介した生体認識の形態と、アプリケーション又はウェブサイトにアクセスするためのユーザのパスワードと、のうちの１つ以上に基づいて（ｂａｓｅｄ　ｏｎ　ｏｒ　ｍｏｒｅ　ｏｆ）ネットワークサービスによって認証される。

【０００９】

いくつかの実施形態では、短命なユーザ識別子は、ネットワークサービスからモバイルコンピューティングデバイスにネットワークを介して送信され、短命なユーザ識別子は、第１のコマンドをスタンドアロンコンピューティングデバイスに送信する前に、モバイルコンピューティングデバイスによってネットワークサービスの公開鍵を使用して更に検証され、第１のコマンドは、モバイルコンピューティングデバイスによってスタンドアロンコンピューティングデバイスに送信され、ユーザ固有のメタデータは、ネットワークサービスによって記憶され、これにより、スタンドアロンコンピューティングデバイスは、モバイルコンピューティングデバイスがネットワークサービスによって既に許可されているユーザに関連付けられていることを検証することが可能になる。

【００１０】

いくつかの実施形態では、短命なユーザ識別子は、短命なユーザ識別子及びメッセージ認証コードの暗号化に基づいてモバイルコンピューティングデバイスから隠され、暗号化は、スタンドアロンコンピューティングデバイスとネットワークサービスとの間のセキュアな暗号ハンドシェイクプロトコルに基づいて導き出されたセッション鍵を使用して実行され、セキュアな暗号ハンドシェイクプロトコルは、モバイルコンピューティングデバイスを信頼されていないリレーとして利用する。

【００１１】

いくつかの実施形態では、ネットワークサービスは、クラウドベースのサーバを含み、スタンドアロンコンピューティングデバイスは、いかなるネットワーク又はいかなる無線アクセスポイントを介してもクラウドベースのサーバに接続されていない。

【００１２】
いくつかの実施形態では、ネットワークサービスがデジタル署名された短命なユーザ識別子をモバイルコンピューティングデバイスに送信する前に、システムは、モバイルコンピューティングデバイスとネットワークサービスとの間に第１のセキュア接続をトランスポート層セキュリティプロトコルに基づいて確立する。スタンドアロンコンピューティングデバイスが第１のコマンドを受信する前に、システムは、モバイルコンピューティングデバイスとスタンドアロンコンピューティングデバイスとの間に第２のセキュア接続をトランスポート層セキュリティプロトコルに基づいて確立する。
【００１３】
いくつかの実施形態では、スタンドアロンコンピューティングデバイスは、多機能プリンタと、モノのインターネット（ＩｏＴ）対応デバイスと、ロボットと、のうちの１つ以上である。
【図面の簡単な説明】
【００１４】
【図１Ａ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための例示的な環境を示す。
【図１Ｂ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための例示的な環境を示す。
【図１Ｃ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための例示的な環境を示す。
【図２】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするためのテーブルをユーザ固有のメタデータも含めて提示する。
【図３Ａ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャートを提示する。
【図３Ｂ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャートを提示する。
【図３Ｃ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャートを提示する。
【図３Ｄ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャートを提示する。
【図３Ｅ】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャートを提示する。
【図４】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするためのスタンドアロンコンピューティングデバイスによる方法を示すフローチャートを提示する。
【図５】本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にする例示的な分散コンピュータ及び通信システムを示す。
【図６】本出願の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にする例示的な装置を示す。
【００１５】
図面において、同様の参照番号は、同様の図要素を指す。
【発明を実施するための形態】
【００１６】
本明細書に記載される実施形態は、モバイルデバイスを有するユーザがスタンドアロンコンピューティングデバイスの能力にアクセスすることを可能にする問題を解決するシステムを提供する。
【００１７】
従来のシステムでは、ユーザが、ユーザのモバイルデバイスを介して、コンピューティングデバイス上のデジタルコンテンツ又はコンピューティングデバイスの能力にアクセスすることを所望するとき、アクセスされるコンピューティングデバイスは、典型的にはネ

ットワーク上にあり、そのネットワーク上のコンピューティングデバイスへのインターフェースを介してアクセス可能である。例えば、ユーザが多機能プリンタの能力にアクセスする（例えば、多機能プリンタ上で文書を印刷する）ことを所望する場合、ユーザのモバイルデバイス及び多機能プリンタの両方は、同じネットワークを介してアクセス可能でなければならない。しかしながら、この多機能プリンタがネットワーク上にない場合、ユーザは多機能プリンタにアクセスすることはできない。

【００１８】

更に、特定のアプリケーション固有の動作は、典型的にはネットワークサービスを介して達成され、ネットワークサービスは、様々なコンピューティングデバイスの動作を管理することができる。例えば、ユーザを認証すること、特定のコンピューティングデバイスの能力にアクセスする権限をユーザに与えること、ユーザのアカウント特権を更新すること、及びユーザ固有のパーソナライゼーションを提供することは、典型的には、ネットワークサービスによって管理及び監視されるタスクである。ネットワークサービスは、クラウドベースのサーバ、又は複数の他のデバイスを管理することができる任意の他のコンピューティングデバイス若しくはコンピューティングエンティティを含むことができ、これらの例示的なタイプのアプリケーション固有の動作を実行することができる。

【００１９】

従来のシステムでは、モバイルデバイスを有するユーザは、コンピューティングデバイス（例えば、多機能プリンタ）が、モバイルデバイスからもアクセス可能であるネットワーク上にある場合にのみ、そのコンピューティングデバイスの機能にアクセスすることができる。ユーザは、これらのアプリケーション固有の動作を実行するために、他のコンピューティングデバイスに頼る必要があり得、こうした他のコンピューティングデバイスは、特定のコンピューティングデバイスの機能にアクセスするユーザの能力を限定又は制限することができる。この依存を軽減することへのいくつかの現在の解決策は、コンピューティングデバイスに接続された管理コンピューティングエンティティの存在を想定しており、管理コンピューティングエンティティは、上述のアプリケーション固有の動作を実行する。一例は、コンピューティングデバイスが、管理されているデバイスのフリート（例えば、多機能プリンタのフリート）の一部である場合である。しかしながら、モバイルデバイスを有するユーザが、管理コンピューティングエンティティを使用せずに、「スタンドアロン」コンピューティングデバイス（すなわち、ネットワークサービス又はクラウドベースのサーバを介してアクセスすることができないコンピューティングデバイス）の能力にアクセスすることができる機構は、現在存在しない。

【００２０】

本明細書に記載される実施形態は、モバイルデバイスを有するユーザがスタンドアロンコンピューティングデバイスの能力にアクセスすることを可能にする問題を解決するシステムを提供する。例示的な一実施形態では、スタンドアロンコンピューティングデバイスはスタンドアロン多機能プリンタ（ＭＦＰ）であり、ユーザのモバイルデバイスは、データ接続を有するスマートフォン（「モバイルデバイス」）であり、ネットワークサービスは、スマートフォンと通信するが、ＭＦＰとは通信しない、クラウド有効化デバイス（「クラウドベースのサーバ」）である。ユーザのモバイルデバイスは、任意の既知の方法を介してクラウドベースのサーバの公開鍵を取得することができる。スタンドアロンコンピューティングデバイスは、例えば、製造時又はファームウェアアップグレード時に含まれているものを介してクラウドベースのサーバの公開鍵を取得することができる。

【００２１】

ユーザは、クラウドベースのサーバに登録し、ユーザがクラウドベースのサーバに対して認証を行うことができるアカウントクレデンシャルをセットアップすることができる。例えば、ユーザは、ユーザ名、パスワード、及び生体認識の形態をセットアップすることができる。続いて、ユーザは（ユーザのモバイルデバイスを介して）、ユーザのアカウントクレデンシャルに基づき、クラウドベースのサーバとの認証プロセスを介してＭＦＰへのアクセスを要求することができる。クラウドベースのサーバは、短命なユーザ識別子を

生成することができ、短命なユーザ識別子は、短命な鍵（固有のものであり、特定のコマンドに対して生成される）及びユーザ固有のメタデータ（クラウドベースのサーバによって記憶されたデータ構造から取得することができ、ユーザの好み／設定を含むことができる）を含むことができる。クラウドベースのサーバのそれ自身の秘密鍵を使用して、クラウドベースのサーバは、生成された短命なユーザ識別子にデジタル署名し、デジタル署名された短命なユーザ識別子をユーザのモバイルデバイスに送信することができる。

【００２２】

続いて、ユーザのモバイルデバイスは、クラウドベースのサーバの公開鍵を使用して、短命なユーザ識別子がクラウドベースのサーバによって署名されたことを検証することによって、デジタル署名された短命なユーザ識別子を検証することができる。次いで、ユーザのモバイルデバイスは、適切なコマンドをＭＦＰに送信することができ、このコマンドは、デジタル署名された短命なユーザ識別子を含むことができる。ＭＦＰもまた、デジタル署名された短命なユーザ識別子を同じ方法で（すなわち、クラウドベースのサーバの公開鍵を使用することによって）検証することができ、検証に成功した場合、コマンドを実行することができる。

【００２３】

ユーザのモバイルデバイスとクラウドベースのサーバとの間の第１のセキュア接続は、例えば、ロングタームエボリューション（ＬＴＥ）、５Ｇ、４Ｇ、３Ｇ、又はＷｉＦｉプロトコルを介して、第１のトランスポート層セキュリティ（ＴＬＳ）プロトコルハンドシェイクに基づくことができる。この第１の接続は、登録プロセス及び／又はＭＦＰへのアクセス要求の前に確立することができる。ユーザのモバイルデバイスとＭＦＰとの間の第２のセキュア接続は、例えば、Ｗｉ Ｆｉ－Ｄｉｒｅｃｔ又はＢｌｕｅｔｏｏｔｈ（登録商標）又はＮＦＣチャネル上で、第２のＴＬＳプロトコルハンドシェイクに基づくことができる。この第２の接続は、ユーザのモバイルデバイスがＭＦＰにコマンドを送信する前に確立することができる。ＴＬＳハンドシェイク又は鍵共有プロトコルを確立することの先駆者として、スタンドアロンコンピューティングデバイス、モバイルデバイス、及びクラウドサービスはそれぞれ、公開暗号鍵及び秘密復号鍵を含む鍵ペアと、適切な認証局によって割り当てられた証明書と、を有することは理解される。認証局は、所与のエンティティに割り当てられた鍵を認証するために必須である。当該技術分野において既知であるように、３つのデバイスのそれぞれは、同じ認証局によって又は異なる認証局によって署名された鍵を使用することができる。以下の全ての実施形態では、公開鍵暗号方式に基づく鍵共有が記載される場合は常に、鍵が鍵認証局によって割り当てられたものであり、鍵認証局によって発行された証明書を伴うものとする。例示的な通信は、図１Ｂ及び図３Ａ～図３Ｅに関連して以下に記載される。

【００２４】

本明細書に記載される実施形態では、システムは、クレデンシャルをクラウドベースのサーバからスタンドアロンコンピューティングデバイスにユーザのモバイルデバイスを介してリレーするネットワーク接続を使用している間、ユーザのモバイルデバイスが、ユーザを認証する信頼のルートになることを可能にする。更に、記載されたシステムの実施形態は、このフリート内のデバイスを管理する、常に存在する管理コンピューティングサービスの複雑性、保守、及び費用を排除することによって、従来のシステムを改善する。システムは、必要に応じて、この機能を、フリートのユーザとのみ通信するクラウドベースのサーバに移す。結果として、システムはまた、コンピューティングデバイスがユーザのモバイルデバイスと日和見的にペアリングすることができる限り、フリート内のコンピューティングデバイスが、常に存在するネットワークに接続されている必要性も排除する。

【００２５】

システムは更に、フリート内のコンピューティングデバイスが、特定のユーザクレデンシャル及び特定のユーザ情報を管理コンピューティングサービスに渡すことができるように構成されなければならない、複雑なセットアップ段階を排除する。代わりに、フリート内の新しいコンピューティングデバイスは、ユーザのモバイルデバイスと通信することが

できさえすればよい。システムはまた、ユーザがフリート内のコンピューティングデバイスと同じネットワーク内にいる必要性も排除する。

【００２６】

したがって、本明細書に記載される実施形態は、スタンドアロンコンピューティングデバイス（ＭＦＰなど）の能力にアクセスするためのユーザのモバイルデバイスの能力を改善するコンピュータシステムを提供する。ユーザのモバイルデバイスが信頼のルートになることを可能にすることによって、システムは、コンピューティングデバイスのフリートを管理する、常に存在する管理コンピューティングサービスの必要性を排除することができる。システムは、本明細書に記載されるように、ユーザのモバイルデバイスがスタンドアロンコンピューティングデバイスにアクセスすることができる方法に改善をもたらす。したがって、システムは、常に存在する管理エンティティのオーバーヘッド又はそのような常に存在する管理エンティティとフリート内のコンピューティングデバイスとの間のネットワーク接続のいずれかを必要とせずに、ユーザが、スタンドアロンコンピューティングデバイスの物理的（又は他の）能力にアクセスすることを可能にすることによって、データアクセスの技術領域を強化及び改善する。

【００２７】

特許請求されるシステムは、技術的な問題（スタンドアロンコンピューティングデバイス内のデジタルデータにアクセスすること、及びネットワークを介したデジタル通信の効率を改善すること）に対する技術的な解決策（本明細書に記載されるように、デジタル署名された短命なユーザ識別子をシステム内で使用すること）である。更に、改善は基本的に技術的なものであり、より効率的なデジタル通信をもたらすことができ、本明細書に記載されるように、様々な実用的で具体的かつ実体的な用途に適用することができる。

【００２８】

用語「ネットワークサービス」は、例えば、ＬＴＥ、５Ｇ、４Ｇ、３Ｇ、又はＷｉＦｉプロトコルを介してアクセス可能であるサーバ又はコンピューティングデバイス又はコンピューティングエンティティを指す。ネットワークサービスは、認証、許可、及び課金を含むアプリケーション固有の動作を提供することができる。ネットワークサービスはまた、複数のユーザ（例えば、ユーザ固有のメタデータ）に関連付けられた情報（例えば、メタデータ）を記憶することもできる。「クラウドベースのサーバ」は、ネットワークサービスの一例であり得る。

【００２９】

用語「モバイルデバイス」及び「モバイルコンピューティングデバイス」は、本開示において互換的に使用され、また、例えば、スマートフォン、タブレット、ラップトップ、及びコンピュータを含むことができる。

【００３０】

用語「スタンドアロンコンピューティングデバイス」は、無線アクセスポイント又は無線ルータを伴う無線プロトコルを介してアクセスすることができない任意のコンピューティングデバイスを指すことができる。ユーザのモバイルデバイスは、例えば、ＷｉＦｉ－Ｄｉｒｅｃｔ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、無線プロトコル、及び無線アクセスポイント又は無線ルータを伴わない無線チャネルの上でペアリングプロトコルを使用してスタンドアロンコンピューティングデバイスとペアリングすることができる。スタンドアロンコンピューティングデバイスの例としては、多機能プリンタ、モノのインターネット（ＩｏＴ）対応デバイス、及びロボットが挙げられる。

【００３１】

図１Ａは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための例示的な環境１００を示す。環境１００は、クラウドベースのサーバ１０２、ユーザ１０４に関連付けられたモバイルコンピューティングデバイス１０６、及びスタンドアロンコンピューティングデバイス１０８を含むことができる。クラウドベースのサーバ１０２は、無線アクセスポイント又は無線ルータを伴う無線プロトコルを介して、例えば、ＬＴＥ／５Ｇ／４Ｇ／３Ｇ／ＷｉＦｉプロトコル１１０を

介して、モバイルコンピューティングデバイス１０６と通信することができる。具体的には、クラウドベースのサーバ１０２及びモバイルコンピューティングデバイス１０６は、ネットワーク１２０を介して互いに通信することができる。モバイルコンピューティングデバイス１０６はまた、無線アクセスポイント又は無線ルータを伴わない無線プロトコルを介して、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）／ＷｉＦｉ－Ｄｉｒｅｃｔ／ＮＦＣプロトコル１１２を介して、スタンドアロンコンピューティングデバイス１０８と通信することもできる。スタンドアロンコンピューティングデバイス１０８は、ネットワーク１２０に、又は任意の他のネットワークに接続されていない。

【００３２】

モバイルコンピューティングデバイス１０６は、無線能力を有する任意のコンピューティングデバイス又はクライアントコンピューティングデバイス、例えば、ラップトップ、タブレット、スマートフォン、モバイルデバイス、及びコンピュータであり得る。スタンドアロンコンピューティングデバイス１０８は、例えば、多機能プリンタ（ＭＦＰ）、モノのインターネット（ＩｏＴ）対応デバイス、又はロボットであり得る。スタンドアロンコンピューティングデバイス１０８は、例えば、モバイルコンピューティングデバイス１０６上の特定のアプリケーションにおいて、（モバイルコンピューティングデバイス１０６のディスプレイ上で）利用可能なＭＦＰのメニューの一部としてユーザ１０４に提示され得る。特定のアプリケーションは、民間企業アプリケーション、顧客アプリケーション、又は雇用者アプリケーションであり得る。スタンドアロンコンピューティングデバイス１０８はまた、ユーザ１０４がスタンドアロンコンピューティングデバイス１０８の「近く」にいるときはいつでも、モバイルコンピューティングデバイス１０６のロック画面上に自動的に現れることによって、ユーザ１０４に提示されてもよい。この自動表示は、モバイルコンピューティングデバイス１０６とスタンドアロンコンピューティングデバイス１０８との間にセキュア接続（例えば、図１Ｂに関連して以下に記載されるＴＬＳハンドシェイク１４６）が確立された後に発生することができる。スタンドアロンコンピューティングデバイス１０８の「近く」は、スタンドアロンコンピューティングデバイス１０８から所定の距離、例えば、モバイルコンピューティングデバイス１０６とＢｌｕｅｔｏｏｔｈ（登録商標）又はＮＦＣ又はＷｉ－Ｆｉ　Ｄｉｒｅｃｔ接続を確立することができる距離内の物理的空間又は領域として定義され得ることに留意されたい。

【００３３】

図１Ｂは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための例示的な環境１３０を示す。環境１３０は、環境１００と同様であり、３つの図示されたエンティティ（すなわち、クラウドベースのサーバ１０２、モバイルコンピューティングデバイス１０６、及びスタンドアロンコンピューティングデバイス１０８）の間の特定の通信を含む。

【００３４】

動作中、ユーザ１０４は（モバイルコンピューティングデバイス１０６を介して）、クラウドベースのサーバ１０２とのユーザ登録１３２プロセスを実行することができ、このプロセスの間、ユーザ１０４は、ユーザプリファレンス、ユーザ名、パスワード、及び生体情報（すなわち、生体認識の形態）などの情報を登録することができる。生体認識（例えば、体測定値及び計算値）は、個人を標識及び記述するために使用される特徴的で測定可能な特性を指すことができ、これには、体の形状に関連する生理学的特性（例えば、指紋、手のひら静脈、顔認識、ＤＮＡ、掌紋、掌形、虹彩認識、網膜、及び臭気／香気）、及び人の行動パターンに関連する行動特性（例えば、タイピングリズム、歩容、及び音声）を含むことができる。

【００３５】

ユーザ１０４はまた、特定のマシン又はアカウントに対して残高を増加又は減少させることもでき（例えば、接続されたバンキングアプリケーション又は他の金融アプリケーションを介して預け入れ又は払い戻しを行うことによる）、また、他の登録関連タスクを実行することもできる。クラウドベースのサーバ１０２は、図２に関連して後述するように

、登録されたユーザ情報をユーザ固有のメタデータ１０５テーブル内に記憶及び維持することができる。ユーザ１０４は（モバイルコンピューティングデバイス１０６を介して）、クラウドベースのサーバ１０２とのＴＬＳハンドシェイク１３４を開始することによって、クラウドベースのサーバ１０２とのセキュア接続を確立することができる。

【００３６】

続いて、ユーザ１０４は（モバイルコンピューティングデバイス１０６を介して）、短命なユーザ識別子を要求することができる（通信１３６）。ユーザ１０４は、アプリケーション又はウェブサイトを介してこの要求１３６を実行することができ、また、正しいパスワード及び／又は生体情報を入力要求に応じて（例えば、モバイルコンピューティングデバイス１０６のユーザインターフェースディスプレイを介して）提供することもできる。要求１３６を受信すると、クラウドベースのサーバ１０２は、短命な鍵を生成し（機能１３８）、ユーザ１０４のユーザ固有のメタデータ（すなわち、ユーザ１０４に関連付けられ、ユーザ１０４によって以前に登録された、テーブル１０５からのメタデータ）を取得することができる。メタデータ１４０はまた、ユーザ１０４が許可されている役割のリスト、ユーザ１０４のアカウント番号、及び同様の補助情報を含むこともできる。役割のリストは、ユーザ１０４によって（例えば、スタンドアロンコンピューティングデバイス１０８とのペアリング成功後に）続いてアクセスすることができる機能を制限又は定義するために使用することができる。

【００３７】

クラウドベースのサーバ１０２は、クラウドベースのサーバ１０２の秘密鍵ＳｅｃｒｅｔＫｅｙ$_{ｃｓ}$を使用して、生成された短命な鍵及び取得されたユーザ固有のメタデータにデジタル署名することができ（機能１４０）、その結果、短命なユーザ識別子１４２が得られる。次いで、クラウドベースのサーバ１０２は、短命なユーザ識別子１４２を（モバイルコンピューティングデバイス１０６を介して）ユーザ１０４に返送することができる。

【００３８】

短命なユーザ識別子１４２を受信すると、モバイルコンピューティングデバイス１０６は、短命なユーザ識別子１４２が実際にクラウドベースのサーバ１０２によって署名され、送信されたことを保証するために、クラウドベースのサーバ１０２の公開鍵（すなわち、ＰｕｂｌｉｃＫｅｙ$_{ｃｓ}$）を使用して、デジタル署名を検証することができる（機能１４４）。モバイルコンピューティングデバイス１０６は、ユーザ登録１３２の前、その間、又はその後に、クラウドベースのサーバ１０２の公開鍵を取得することができる。クラウドベースのサーバ１０２の公開鍵は、この情報を取得することを所望する任意のエンティティによって容易に利用可能かつ取得可能である。デジタル署名を成功裏に検証し、それにより、短命なユーザ識別子１４２が、実際に、（悪意のある又は不正なエンティティに対立するものとしての）クラウドベースのサーバ１０２によって署名され、送信されたことを確認すると、モバイルコンピューティングデバイス１０６は、スタンドアロンコンピューティングデバイス１０８とのＴＬＳハンドシェイク１４６を開始することによって、スタンドアロンコンピューティングデバイス１０８とセキュア接続を確立することができる。

【００３９】

続いて、モバイルコンピューティングデバイス１０６は、コマンド１４８（短命なユーザ識別子１４２を含む）を生成し、コマンド１４８をスタンドアロンコンピューティングデバイス１０８に送信することができる。コマンド１４８を受信すると、スタンドアロンコンピューティングデバイス１０８は、短命なユーザ識別子１４２を抽出し、短命なユーザ識別子１４２が実際にクラウドベースのサーバ１０２によって署名され、送信されたことを保証するために、クラウドベースのサーバ１０２の公開鍵（すなわち、ＰｕｂｌｉｃＫｅｙ$_{ｃｓ}$）を使用して、デジタル署名を検証することができる（機能１５０）。検証に成功すると、スタンドアロンコンピューティングデバイス１０８は、コマンド１４８を実行し（機能１５２）、実行されたコマンドに関連付けられたトランザクション情報を示す通知メッセージを生成し（機能１５４）、モバイルコンピューティングデバイス１０６に

通知１５６を返送することができる。この実施形態は、スタンドアロンコンピューティングデバイス１０８に記憶される復号鍵を必要としない。スタンドアロンコンピューティングデバイス１０８は、短命なユーザＩＤ１４２を平文で受信することができ、クラウドベースのサーバ１０２の公開鍵を使用して、クラウドベースのサーバ１０２の関連する署名を検証することができる。一実施形態では、そのような復号鍵をスタンドアロンコンピューティングデバイス１０８にセキュアに記憶することができる場合、短命なユーザ識別子１４２は、上記のように平文で送信される必要はないが、代わりに、スタンドアロンコンピューティングデバイス１０８にのみ既知の復号鍵を使用してクラウドベースのサーバ１０２によって暗号化されることができる。別の実施形態では、モバイルコンピューティングデバイス１０６を信頼されていないリレーとして使用した、クラウドベースのサーバ１０２とのＴＬＳ型のハンドシェイクを使用して、復号鍵がスタンドアロンコンピューティングデバイス１０８によって導き出されることができる場合、この場合もやはり、短命なユーザ識別子１４２は、上記のように平文で送信される必要はないが、代わりに、（図１Ｃに関連して後述するように）ＴＬＳ型のハンドシェイクを介して、スタンドアロンコンピューティングデバイス１０８によって導き出された復号鍵を使用して、クラウドベースのサーバ１０２によって暗号化されることができる。

【００４０】

通知１５６を受信すると、モバイルコンピューティングデバイスは、通知１５８をクラウドベースのサーバ１０２に送信することができ、通知１５８は、通知１５６に示されているのと同様のトランザクション情報を伝える。トランザクション情報は、例えば、印刷されたページの数、印刷されたページの数に関連した金額又はコスト、及びトランザクションに関連した任意の他の関連情報を含むことができる。続いて、クラウドベースのサーバ１０２は、受信したトランザクション情報に基づいてユーザ固有のメタデータ１０５を更新することができる。

【００４１】

図１Ｃは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための例示的な環境１６０を示す。環境１６０は、環境１００と同様であり、３つの図示されたエンティティ（すなわち、クラウドベースのサーバ１０２、モバイルコンピューティングデバイス１０６、及びスタンドアロンコンピューティングデバイス１０８）の間の特定の通信を含む。

【００４２】

動作中、ユーザ１０４は（モバイルコンピューティングデバイス１０６を介して）、図１Ｂで上述したように、クラウドベースのサーバ１０２とのユーザ登録１３２プロセスを実行することができる。ユーザ１０４は（モバイルコンピューティングデバイス１０６を介して）、クラウドベースのサーバ１０２とのＴＬＳハンドシェイク１３４を開始することによって、クラウドベースのサーバ１０２とのセキュア接続を確立することができる。モバイルコンピューティングデバイス１０６はまた、スタンドアロンコンピューティングデバイス１０８とのＴＬＳハンドシェイク１４６を開始することによって、スタンドアロンコンピューティングデバイス１０８とのセキュア接続を確立することもできる。ユーザ１０４は（モバイルコンピューティングデバイス１０６を介して）、短命なユーザ識別子を要求することができ（通信１６１）、及び／又はコマンド１６２をスタンドアロンコンピューティングデバイス１０８に送信することができる。要求１６１を受信すると、クラウドベースのサーバ１０２は、短命なユーザ識別子を生成する前にセッション暗号文を受信するのを待つことができる。

【００４３】

コマンド１６２を受信すると、スタンドアロンコンピューティングデバイス１０８は、セッション鍵を生成し（機能１６４）、スタンドアロンコンピューティングデバイス１０８の秘密鍵を使用してセッション鍵を署名することによって「ＣＯＭＢＯ＿１」を生成することができる（例えば、ＣＯＭＢＯ＿１＝ＳＩＧ（セッション鍵，ＳｅｃｒｅｔＫｅｙＳＡＣＤ））（機能１６６）。スタンドアロンコンピューティングデバイス１０８は、クラ

ウドベースのサーバの公開鍵を使用してＣＯＭＢＯ＿１を暗号化することによって「セッション暗号文」を生成することができる（例えば、ＥＮＣ（ＣＯＭＢＯ＿１，ＰｕｂｌｉｃＫｅｙ$_{ＣＳ}$））（機能１６８）。スタンドアロンコンピューティングデバイス１０８は、セッション暗号文１７０をモバイルコンピューティングデバイス１０６に送信することができる。モバイルコンピューティングデバイス１０６は、クラウドベースのサーバ１０２の秘密鍵を有しないため、モバイルコンピューティングデバイス１０６は、セッション暗号文１７０を解読することができない。代わりに、モバイルコンピューティングデバイス１０６は、セッション暗号文１７０を（セッション暗号文１７２として）クラウドベースのサーバ１０２に転送することができる。

【００４４】

セッション暗号文１７２を受信すると、クラウドベースのサーバ１０２は、クラウドベースのサーバ１０２の秘密鍵を使用してセッション暗号文１７２を復号して（例えば、ＤＥＣ（ＥＮＣ（ＣＯＭＢＯ＿１，ＰｕｂｌｉｃＫｅｙ$_{ＣＳ}$），ＳｅｃｒｅｔＫｅｙ$_{ＣＳ}$））、ＣＯＭＢＯ＿１＝Ｓｉｇ（セッション鍵，ＳｅｃｒｅｔＫｅｙ$_{ＳＡＣＤ}$）を得ることができる（機能１７４）。クラウドベースのサーバ１０２は、セッション鍵がスタンドアロンコンピューティングデバイス１０８によって生成されたことを検証するために、スタンドアロンコンピューティングデバイス１０８の公開鍵「ＰｕｂｌｉｃＫｅｙ$_{ＳＡＣＤ}$」を使用して署名を検証することができる（機能１７６）。続いて、クラウドベースのサーバ１０２は、短命なユーザ識別子（ＥＵＩＤ）を生成することができる（機能１７８）。例えば、クラウドベースのサーバは、短命な鍵（Ｅ／Ｋ）を生成し、ユーザ固有のメタデータ（Ｍ／Ｄ）を取得し、生成したＥ／Ｋ及び取得したユーザ固有のＭ／Ｄをクラウドベースのサーバ１０２の秘密鍵でデジタル署名することによって、短命なユーザ識別子を生成することができる（例えば、ＥＵＩＤ＝Ｅ／Ｋ＋Ｍ／Ｄ｜｜ＳＩＧ（Ｅ／Ｋ＋Ｍ／Ｄ，ＳｅｃｒｅｔＫｅｙ$_{ＣＳ}$））。クラウドベースのサーバ１０２はまた、ＥＵＩＤのためのメッセージ認証コード（ＭＡＣ）を生成することができ、セッション鍵を使用してＥＵＩＤ及びＭＡＣを暗号化することによって「ＣＯＭＢＯ＿２」を生成することもできる（例えば、ＥＮＣ（ＥＵＩＤ＋ＭＡＣ，セッション鍵）（機能１８０）。

【００４５】

クラウドベースのサーバ１０２は、ＣＯＭＢＯ＿２　１８２をモバイルコンピューティングデバイス１０６に送信することができる。この場合もやはり、モバイルコンピューティングデバイス１０６はセッション鍵を有しないため、モバイルコンピューティングデバイス１０６は、ＣＯＭＢＯ＿２　１８２を解読することができない。代わりに、モバイルコンピューティングデバイス１０６は、ＣＯＭＢＯ＿２　１８２を（ＣＯＭＢＯ＿２　１８４として）スタンドアロンコンピューティングデバイス１０８に転送することができる。

【００４６】

ＣＯＭＢＯ＿２　１８４を受信すると、スタンドアロンコンピューティングデバイス１０８は、セッション鍵を使用してＣＯＭＢＯ＿２を復号して、ＥＵＩＤ及びＭＡＣを得ることができる（例えば、ＤＥＣ（（ＥＮＣ（ＥＵＩＤ＋ＭＡＣ，セッション鍵）），セッション鍵））（機能１８６）。スタンドアロンコンピューティングデバイス１０８は、ＥＵＩＤが改ざんされていないことを保証するために、ＭＡＣを使用してＥＵＩＤを検証することができる（機能１８８）。ＥＵＩＤを成功裏に検証すると、スタンドアロンコンピューティングデバイス１０８は、以前に受信したコマンド１６２を実行し（機能１９０）、実行されたコマンドに関連付けられたトランザクション情報を示す通知メッセージを生成し（機能１９２）、モバイルコンピューティングデバイス１０６に通知１９４を返送することができる。通知１９４を受信すると、モバイルコンピューティングデバイス１０６は、通知１９６をクラウドベースのサーバ１０２に送信することができ、通知１９６は、通知１９４に示されているのと同様のトランザクション情報を伝える。

【００４７】

したがって、図１Ｂの環境１３０で上述した検証通信とは対照的に、環境１６０は、検証工程を実行する異なる方法を示しており、システムが短命なユーザ識別子をモバイルデ

バイスから隠すことを可能にする。

【００４８】

図２は、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするためのテーブル２１０及び２３０をユーザ固有のメタデータも含めて提示する。テーブル２１０は、マシンタイプ２１１に対応するデータを有するテーブルであり得る。テーブル２１０は、ユーザ名２１２、現金残高２１４、ページ残数２１６、及びユーザプリファレンス２１８などの列を有するエントリを含むことができる。例えば、テーブル２１０は、前述の列に対して「ｊｏｅ．ｙ．ｓｍｉｔｈ」、「＄２６．２０」、「２６０ページ」、及び「｛縦、両面、黒／白｝」の値を有するエントリ２２０を含むことができる。

【００４９】

同様に、テーブル２３０は、マシンタイプ２３１に対応するデータを有するテーブルであり得る。テーブル２３０は、ユーザ名２３２、現金残高２３４、ページ残数２３６、及びユーザプリファレンス２３８などの列を有するエントリを含むことができる。例えば、テーブル２３０は、前述の列に対して「ｊｏｅ．ｙ．ｓｍｉｔｈ」、「＄１５８．８８」、「ｎ／ａ」、及び「｛横、片面、カラー｝」の値を有するエントリ２４０を含むことができる。

【００５０】

テーブル２１０及び２３０は、単に例示的なテーブルにすぎず、図示されていない他の列及び値を含み得ることに留意されたい。例えば、ユーザ固有のメタデータ２００は、複数のマシンタイプに対する情報を組み込む１つのテーブルを含むことができる。ユーザ固有のメタデータ２００はまた、アカウント番号、支払いタイプ、支払いの頻度、照合順序プリファレンス、ニックネーム、ユーザを識別する情報、及びスタンドアロンコンピューティングデバイスに関連した任意のオプションを含む、他のユーザプリファレンスを含むこともできる。

【００５１】

テーブル２１０及び２３０は、クラウドベースのサーバ（例えば、図１Ｂのクラウドベースのサーバ１０２）に記憶された例示的なユーザアカウント及びプリファレンス情報を表す。ユーザ固有のメタデータ２００は、ユーザの名前、アカウント番号、ニックネーム、及びユーザを識別する情報など、いくらかの個人を特定できる情報（ＰＩＩ）を含んでもよい。上述したように、いくつかの実施形態では、短命なユーザ識別子は、署名検証と共に平文で送信される。これらの事例では、ＰＩＩが通信チャネルの上で（すなわち、図１Ａの通信プロトコル１１０及び１１２の上で）送信されないことを保証するために、クラウドベースのサーバ１０２は、テーブル２１０及び２３０のユーザ固有のメタデータ（任意のＰＩＩを含む）に基づいて、数字列として、短命なユーザ識別子を生成又は導出することができる（例えば、図１Ｂの機能１３８及び１４０）。続いて、この数字列は、図１Ｂの短命なユーザ識別子１４２としてモバイルコンピューティングデバイス１０６に送信される。したがって、テーブル２１０及び２３０の列はＰＩＩを示すが、ＰＩＩから導き出されたランダムな文字列は、ＰＩＩを示すものとはならない。

【００５２】

図３Ａは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャート３００を提示する。動作中、ユーザは、ネットワークサービスに登録し、ユーザ固有のメタデータを含める（動作３０２）。ユーザは、ユーザのモバイルコンピューティングデバイスを介して、又は必要なアカウントクレデンシャルを入力として受け入れることができる別のクライアントコンピューティングデバイスを介して、登録してもよい。例えば、必要なクレデンシャルが、モバイルコンピューティングデバイス上での入力としてのみ受け入れられることができる生体認識の形態を含む場合、ユーザは、適切なモバイルコンピューティングデバイスを使用しなければならない。しかしながら、必要なクレデンシャルが、テキストベースのエディタ又はアプリケーションを介して入力されることができるユーザ名又はパスワードを含

む場合、ユーザは、登録を実行するために任意のクライアントコンピューティングデバイスを使用してもよい。ユーザ固有のメタデータは、例えば、図２に関連して上に示したように、特定のタイプのマシンに印刷するためのユーザプリファレンス、支払いプリファレンスなどを含むことができる。

【００５３】

ユーザは、モバイルコンピューティングデバイスのユーザインターフェースディスプレイ上で、スタンドアロンコンピューティングデバイスへのアクセスを取得するためのアプリケーション又はウェブサイトを開く（動作３０４）。ユーザは、モバイルコンピューティングデバイスのユーザインターフェースディスプレイを介してネットワークサービスに、スタンドアロンコンピューティングデバイスへのアクセスを取得するための認証を提供する（動作３０６）。認証はパスワード、又はモバイルコンピューティングデバイスの構成要素を介した生体認識の形態であり得る。

【００５４】

ユーザがネットワークサービスによって認証されない場合（判定３０８）、動作は戻る。ユーザがネットワークサービスによって認証される場合（判定３０８）、ネットワークサービスは、提供された認証に基づいてユーザを認証し（動作３１０）、動作は図３Ｂのラベル Ａに続く。いくつかの実施形態では、ユーザ認証情報は、ＯＡｕｔｈなどのプロトコルを介して第三者のＩＤプロバイダを使用して、例えば、ユーザに帰属するＧｏｏｇｌｅ又はＦａｃｅｂｏｏｋアカウントを使用して、取得又は検証することができる。

【００５５】

図３Ｂは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャート３２０を提示する。ユーザは、モバイルコンピューティングデバイスのユーザインターフェースディスプレイを介して、短命なユーザ識別子の要求を生成する（動作３２２）。要求は、ネットワークサービスによる認証が成功したとき、例えば、ユーザが、特定のスタンドアロンコンピューティングデバイスにアクセスするための特定のアプリケーション又はウェブサイトに入り、正しいアカウントクレデンシャルの入力に成功したとき、自動的に行われてもよい。要求はまた、スタンドアロンコンピューティングデバイスへの、又はスタンドアロンコンピューティングデバイスの能力（例えば、多機能プリンタ上で文書を印刷すること、又はＩｏＴデバイス上のセンサ若しくは測定値にアクセスすること）へのアクセスを要求する別のコマンド若しくはメッセージの一部であってもよい。

【００５６】

ユーザは、モバイルコンピューティングデバイスのユーザインターフェースディスプレイを介してネットワークサービスに、短命なユーザ識別子の要求を送信する（動作３２４）。ネットワークサービスは、ユーザから、短命なユーザ識別子の要求を受信する（動作３２６）。ネットワークサービスは、短命な鍵及びユーザ固有のメタデータを含む、短命なユーザ識別子を生成する（動作３２８）。ユーザ固有のメタデータは、ネットワークサービスによって記憶されてもよい。ネットワークサービスは、ネットワークサービスの秘密鍵に基づいて、短命なユーザ識別子にデジタル署名する（動作３３０）。ネットワークサービスは、モバイルコンピューティングデバイスに、デジタル署名された短命なユーザ識別子を送信する（動作３３２）。モバイルコンピューティングデバイスは、ネットワークサービスから、デジタル署名された短命なユーザ識別子を受信し（動作３３４）、動作は図３Ｃのラベル Ｂに続く。

【００５７】

図３Ｃは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャート３４０を提示する。モバイルコンピューティングデバイスは、ネットワークサービスの公開鍵を使用して、デジタル署名された短命なユーザ識別子がネットワークサービスによって署名されていることを検証する（動作３４２）。ネットワークサービスの公開鍵は、その取得を所望する任意のエンティティで利用可能であり、動作３０２の登録プロセス中にユーザに提供されてもよ

いことに留意されたい。検証が成功しなかった場合（判定３４４）、動作は戻る。
【００５８】
検証が成功した場合（判定３４４）、モバイルコンピューティングデバイスは、無線アクセスポイント又は無線ルータを伴わない第１の無線プロトコル（例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）、Ｗｉ－Ｆｉ　ｄｉｒｅｃｔ、又はＮＦＣ）に基づいて無線でスタンドアロンコンピューティングデバイスとペアリングする（動作３４６）。モバイルコンピューティングデバイスは、スタンドアロンコンピューティングデバイスの能力にアクセスする第１のコマンドを生成し、第１のコマンドは、デジタル署名された短命なユーザ識別子を含む（動作３４８）。モバイルコンピューティングデバイスは、スタンドアロンコンピューティングデバイスに、第１の無線プロトコルに基づいて第１のコマンドを送信し（動作３５０）、動作は図３Ｄのラベル Ｄに続く。
【００５９】
図３Ｄは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャート３６０を提示する。動作中、スタンドアロンコンピューティングデバイスは、モバイルコンピューティングデバイスから、第１の無線プロトコルに基づいて第１のコマンドを受信する（動作３６２）。スタンドアロンコンピューティングデバイスは、ネットワークサービスの公開鍵を使用して、デジタル署名された短命なユーザ識別子がネットワークサービスによって生成されたことを検証する（動作３６４）。ネットワークサービスの公開鍵は、スタンドアロンコンピューティングデバイスに、製造、ファームウェアアップグレード、又は他のプロセスの間にそのファームウェアの一部として提供されてもよい。
【００６０】
いくつかの実施形態では、検証工程（動作３６４）は、図１Ｃに関連して上述したように、異なる方式で実行されてもよい。具体的には、短命なユーザ識別子をモバイルコンピューティングデバイスから完全に隠すことが望ましい場合がある。短命なユーザ識別子を隠すことの動機は、短命なユーザ識別子の構築に使用されているユーザ固有のメタデータを隠すことである。これを達成するために、短命なユーザ識別子は、モバイルコンピューティングデバイスではなく、スタンドアロンコンピューティングデバイスのみが、識別子を復号し、それが実際にネットワークサービスによって又は同等にクラウドベースのサーバによって生成されたことを検証することができるように暗号化され得る。これは、クラウドベースのサーバとスタンドアロンコンピューティングデバイスとの間のＴＬＳ型のハンドシェイクによって、モバイルコンピューティングデバイスを信頼されていないリレーとして使用して実現される。
【００６１】
この実施形態が機能するための一要件は、スタンドアロンコンピューティングデバイスが、自らの公開暗号鍵及び秘密復号鍵を有し、スタンドアロンコンピューティングデバイスが、復号鍵をセキュアに記憶するために、トラステッドプラットフォームモジュールなどのハードウェアリソースを有することである。この要件が満たされると、スタンドアロンコンピューティングデバイスは、いわゆる「セッション鍵」を生成し、独自の秘密復号鍵でセッション鍵を署名し、クラウドサーバの公開暗号鍵を使用してセッション鍵と署名の組み合わせを暗号化して、セッション暗号文を生成することができる。スタンドアロンコンピューティングデバイスは、セッション暗号文をモバイルコンピューティングデバイスに送信することができ、続いて、モバイルコンピューティングデバイスは、セッション暗号文をクラウドベースのサーバに転送することができる。
【００６２】
そのような実施形態では、モバイルコンピューティングデバイスは、セッション暗号文を復号することも、スタンドアロンコンピューティングデバイスの署名を検証することもできない。一方、クラウドベースのサーバは、セッション暗号文を、その復号鍵を使用して復号して、セッション鍵及び署名を得ることができる。次いで、クラウドベースのサーバは、スタンドアロンコンピューティングデバイスの公開暗号鍵に基づいて署名を検証し

て、セッション鍵が実際にスタンドアロンコンピューティングデバイスによって生成されたことの保証を得ることができる。次に、クラウドベースのサーバは、セッション鍵を使用して短命なユーザ識別子及びメッセージ認証コード（ＭＡＣ）の暗号化を生成し、この組み合わせをモバイルコンピューティングデバイスに送信することができ、モバイルコンピューティングデバイスは、この組み合わせをスタンドアロンコンピューティングデバイスに転送することができる。モバイルコンピューティングデバイスはセッション鍵を知らず、したがって、この組み合わせを復号することができないことに留意されたい。しかしながら、スタンドアロンコンピューティングデバイスは、セッション鍵を使用して、受信した組み合わせを復号することができ、短命なユーザ識別子を明らかにし、ＭＡＣを使用して、メッセージが送信中に改ざんされていないことを検証することができる。

【００６３】

検証が成功しなかった場合（判定３６８）、動作は戻る。検証が成功した場合（判定３６８）、スタンドアロンコンピューティングデバイスは、スタンドアロンコンピューティングデバイスの能力にアクセスすることによってユーザ固有のメタデータに基づいて第１のコマンドを実行する（動作３７０）。第１のコマンドは、スタンドアロンコンピューティングデバイス上で文書を印刷する（多機能プリンタの場合のように）、スタンドアロンコンピューティングデバイスのセンサから測定値を取得する（ＩｏＴ対応デバイスの場合のように）、又は特定の物理的タスクを実行する（ロボットの場合のように）ためのコマンドを含むことができる。スタンドアロンコンピューティングデバイスは、実行された第１のコマンドに関連付けられたトランザクション情報を示す通知メッセージを生成する（動作３７２）。トランザクション情報は、例えば、印刷されたページの数、消費されたデータの量、監視測定値の要求に対する応答などを含むことができる。スタンドアロンコンピューティングデバイスは、モバイルコンピューティングデバイスに通知メッセージを送信し（動作３７４）、動作は図３Ｅのラベル Ｄに続く。

【００６４】

図３Ｅは、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするための方法を示すフローチャート３８０を提示する。動作中、モバイルコンピューティングデバイスは、スタンドアロンコンピューティングデバイスから通知メッセージを受信する（動作３８２）。モバイルコンピューティングデバイスは、ネットワークサービスに通知メッセージを送信する（動作３８４）。ネットワークサービスは、モバイルコンピューティングデバイスから通知メッセージを受信する（動作３８６）。ネットワークサービスは、通知メッセージに示されたトランザクション情報に基づいて、データ構造内のエントリを更新し、エントリはユーザ固有のメタデータに対応する（動作３８８）。いくつかの実施形態では、スタンドアロンコンピューティングデバイスによって生成された通知メッセージは、平文であり、モバイルコンピューティングデバイスに可視である。他の実施形態では、例えば、通知メッセージが、スタンドアロンコンピューティングデバイスによって提供されたサービスのコストに関する情報を含む場合、通知メッセージを暗号化することは、そのコンテンツをモバイルコンピューティングデバイスから隠すために、及びモバイルコンピューティングデバイスがコンテンツを変更することを防止するために有益である。これは、クラウドベースのサーバ又はネットワークサービスの公開鍵を使用して通知メッセージを暗号化することによって簡単に達成される。更に別の実施形態では、通知メッセージは、スタンドアロンコンピューティングデバイスとクラウドベースのサーバ（又はネットワークサービス）との間に確立されたセッション鍵から導き出された鍵を使用して暗号化されてもよい。具体的には、セッション鍵は頻繁な間隔でセキュアに更新されることができるため（「循環される」又は変更されるとも呼ばれる）、この最後の実施形態は、敵対者に、将来の攻撃で得られる危殆化したセッション鍵を使用して過去の暗号化されたメッセージを復号することが可能になると期待して暗号化されたメッセージを保存することをやめさせる、当該技術分野において既知の概念である、「前方秘匿性」を提供する要件が存在する場合に好ましい。

【００６５】

図４は、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にするためのスタンドアロンコンピューティングデバイスによる方法を示すフローチャート４００を提示する。動作中、システムは、スタンドアロンコンピューティングデバイスによって、ユーザに関連付けられたモバイルコンピューティングデバイスから、スタンドアロンコンピューティングデバイスの能力にアクセスする第１のコマンドを受信し、第１のコマンドは、短命な鍵とユーザ固有のメタデータとを含む短命なユーザ識別子を含んでおり、短命なユーザ識別子は、第１のコマンドに固有であり、短命な鍵は、ネットワークサービスによって生成されており、短命なユーザ識別子は、ネットワークサービスの秘密鍵でデジタル署名されており、スタンドアロンコンピューティングデバイスは、ネットワークサービスによって直接アクセス可能ではない（動作４０２）。システムは、スタンドアロンコンピューティングデバイスによって、ネットワークサービスの公開鍵を使用して、短命なユーザ識別子がネットワークサービスによってデジタル署名されていることを検証する（動作４０４）。検証が成功しなかった場合（判定４０６）、動作は戻る。検証が成功した場合（判定４０６）、システムは、スタンドアロンコンピューティングデバイスによって、スタンドアロンコンピューティングデバイスの能力にアクセスすることによってユーザ固有のメタデータに基づいて第１のコマンドを実行する（動作４０８）。

【００６６】

図５は、本発明の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にする例示的な分散コンピュータ及び通信システム５００を示す。コンピュータシステム５０２は、プロセッサ５０４、メモリ５０６、及び記憶デバイス５０８を含む。メモリ５０６は、管理メモリとして機能する揮発性メモリ（例えば、ＲＡＭ）を含むことができ、１つ以上のメモリプールを記憶するために使用することができる。更に、コンピュータシステム５０２は、ディスプレイデバイス５１０、キーボード５１２、及びポインティングデバイス５１４に連結することができる。記憶デバイス５０８は、オペレーティングシステム５１６、コンテンツ処理システム５１８、及びデータ５３０を記憶することができる。

【００６７】

コンテンツ処理システム５１８は、コンピュータシステム５０２によって実行されると、コンピュータシステム５０２に本開示に記載されている方法及び／又は処理を実行させることができる命令を含むことができる。具体的には、コンテンツ処理システム５１８は、コンピュータネットワークを介して他のネットワークノードに／から、又は無線アクセスポイント若しくはルータを伴わない無線プロトコルを介して、データパケットを送信及び／又は受信するための命令を含み得る（通信モジュール５２０）。データパケットは、データ、登録要求、短命なユーザ識別子、コマンド、及び通知を含むことができる。

【００６８】

コンテンツ処理システム５１８は、スタンドアロンコンピューティングデバイスによって、ユーザに関連付けられたモバイルコンピューティングデバイスから、スタンドアロンコンピューティングデバイスの能力にアクセスする第１のコマンドを受信するための命令を更に含むことができ、第１のコマンドは、短命な鍵とユーザ固有のメタデータとを含む短命なユーザ識別子を含んでおり、短命なユーザ識別子は、第１のコマンドに固有であり、短命な鍵は、ネットワークサービスによって生成されており、短命なユーザ識別子は、ネットワークサービスの秘密鍵でデジタル署名されており、スタンドアロンコンピューティングデバイスは、ネットワークサービスによって直接アクセス可能ではない（通信モジュール５２０）。コンテンツ処理システム５１８はまた、スタンドアロンコンピューティングデバイスによって、ネットワークサービスの公開鍵を使用して、短命なユーザ識別子がネットワークサービスによってデジタル署名されていることを検証するための命令を含むこともできる（検証モジュール５２２）。コンテンツ処理システム５１８は、スタンドアロンコンピューティングデバイスによって、スタンドアロンコンピューティングデバイスの能力にアクセスすることによってユーザ固有のメタデータに基づいて第１のコマンド

を実行するための命令を含むことができる（コマンド実行モジュール５２４）。
【００６９】
コンテンツ処理システム５１８は、スタンドアロンコンピューティングデバイスによって、モバイルコンピューティングデバイスに、第１のコマンドの成功した実行を示す通知を送信するための命令を追加的に含むことができる（通知管理モジュール５２６）。コンテンツ処理システム５１８は、スタンドアロンコンピューティングデバイスによって、ＷｉＦｉ－Ｄｉｒｅｃｔと、Ｂｌｕｅｔｏｏｔｈ（登録商標）と、ＮＦＣと、無線プロトコルと、無線アクセスポイント又は無線ルータを伴わない無線プロトコルと、のうちの１つ以上に基づいて無線でモバイルコンピューティングデバイスとペアリングするための命令を含むことができる（接続確立モジュール５２８）。
【００７０】
コンテンツ処理システム５１８はまた、モバイルコンピューティングデバイスとネットワークサービスとの間にトランスポート層セキュリティプロトコルに基づいて第１のセキュア接続を確立するための命令を含むこともできる（接続確立モジュール５２８）。コンテンツ処理システム５１８はまた、モバイルコンピューティングデバイスとスタンドアロンコンピューティングデバイスとの間にトランスポート層セキュリティプロトコルに基づいて第２のセキュア接続を確立するための命令を含むこともできる（接続確立モジュール５２８）。
【００７１】
データ５３０は、入力として必要とされるか、又は本開示に記載される方法及び／若しくは処理によって出力として生成される、任意のデータを含むことができる。具体的には、データ５３０は、少なくとも、コマンド、短命なユーザ識別子、短命な鍵、ユーザ固有のメタデータ、デジタル署名された短命なユーザ識別子、ネットワークサービスのインジケータ又は識別子、モバイルコンピューティングデバイスに関連付けられたユーザのインジケータ又は識別子、モバイルコンピューティングデバイスのインジケータ又は識別子、スタンドアロンコンピューティングエンティティのインジケータ又は識別子、公開鍵、秘密鍵、通知、通知メッセージ、メッセージ、実行されたコマンドに関連付けられたトランザクション情報、無線アクセスポイント又は無線ルータを伴わない無線プロトコルを介しての成功したペアリングのインジケータ、２つのエンティティの間に確立された成功した接続のインジケータ、トランスポート層セキュリティプロトコルを介して接続をサポートするための情報、並びに多機能プリンタ、ＩｏＴ対応デバイス、及びロボットのインジケータ又は識別子を記憶することができる。
【００７２】
図６は、本出願の一実施形態による、スタンドアロンコンピューティングデバイスへのユーザアクセスを容易にする例示的な装置６００を示す。装置６００は、有線、無線、量子光、又は電気通信チャネルを介して互いに通信し得る複数のユニット又は装置を備えることができる。装置６００は、１つ以上の集積回路を使用して実現されてもよく、図６に示されているものよりも少ない又は多いユニット又は装置を含んでもよい。更に、装置６００は、コンピュータシステムに統合されてもよく、又は他のコンピュータシステム及び／若しくはデバイスと通信することができる別個のデバイスとして実現されてもよい。具体的には、装置６００は、図５のコンピュータシステム５０２のモジュール５２０～５２８と同様の機能又は動作を実行するユニット６０２～６１０を備えることができ、これには、通信ユニット６０２、検証ユニット６０４、コマンド実行ユニット６０６、通知管理ユニット６０８、及び接続確立ユニット６１０が含まれる。
【００７３】
発明を実施するための形態において記載されるデータ構造及びコードは、典型的には、コンピュータ可読記憶媒体上に記憶され、コンピュータシステムによって使用されるコード及び／又はデータを記憶することができる任意のデバイス又は媒体であってもよい。コンピュータ可読記憶媒体としては、揮発性メモリ、不揮発性メモリ、ディスクドライブなどの磁気及び光学記憶デバイス、磁気テープ、ＣＤ（コンパクトディスク）、ＤＶＤ（デ

ジタル多用途ディスク若しくはデジタルビデオディスク）、又は既知の、若しくは今後開発されるコンピュータ可読媒体を記憶することができる他の媒体が挙げられるが、これらに限定されない。

【００７４】

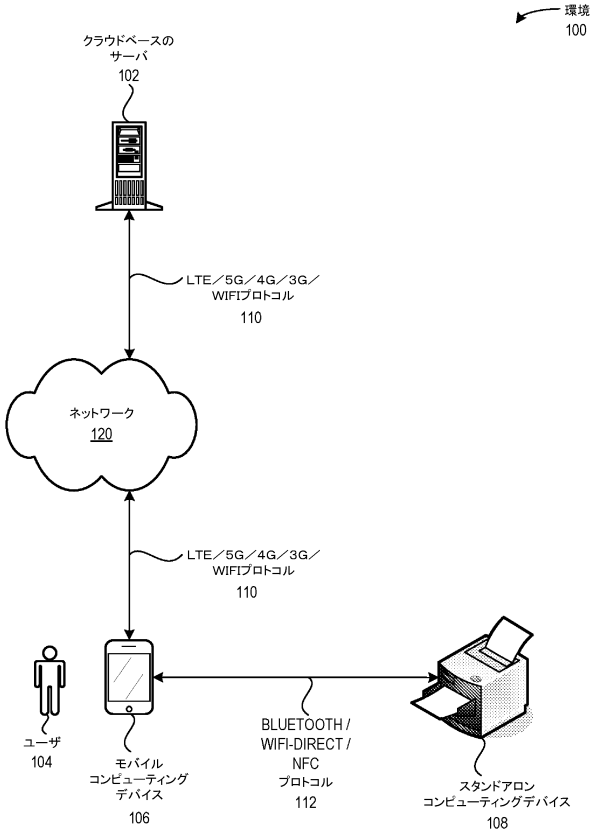
発明を実施するための形態セクションに記載される方法及び処理は、上記のようにコンピュータ可読記憶媒体に記憶され得るコード及び／又はデータとして具体化することができる。コンピュータシステムが、コンピュータ可読記憶媒体上に記憶されたコード及び／又はデータを読み取って実行すると、コンピュータシステムは、データ構造及びコードとして具体化され、コンピュータ可読記憶媒体内に記憶された方法及び処理を実行する。

【００７５】

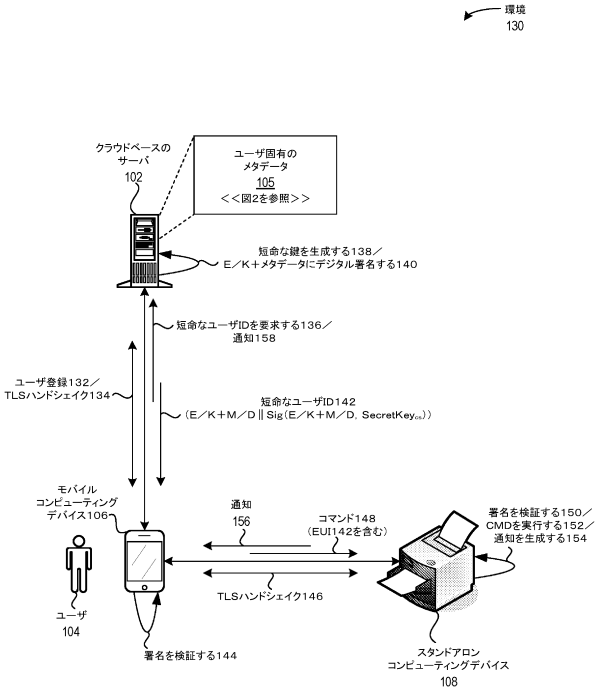
更に、上述の方法及び処理は、ハードウェアモジュール又は装置に含まれてもよい。ハードウェアモジュール又は装置としては、特定用途向け集積回路（ａｐｐｌｉｃａｔｉｏｎ－ｓｐｅｃｉｆｉｃ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ、ＡＳＩＣ）チップ、フィールドプログラム可能ゲートアレイ（ｆｉｅｌｄ－ｐｒｏｇｒａｍｍａｂｌｅ ｇａｔｅ ａｒｒａｙ、ＦＰＧＡ）、特定の時刻に特定のソフトウェアモジュール又はコードを実行する専用又は共有プロセッサ、及び、既知の又は後に開発される他のプログラム可能論理デバイスを含むことができるが、これらに限定されない。ハードウェアモジュール又は装置が起動されると、それらの内部に含まれる方法及び処理が実行される。

【図面】

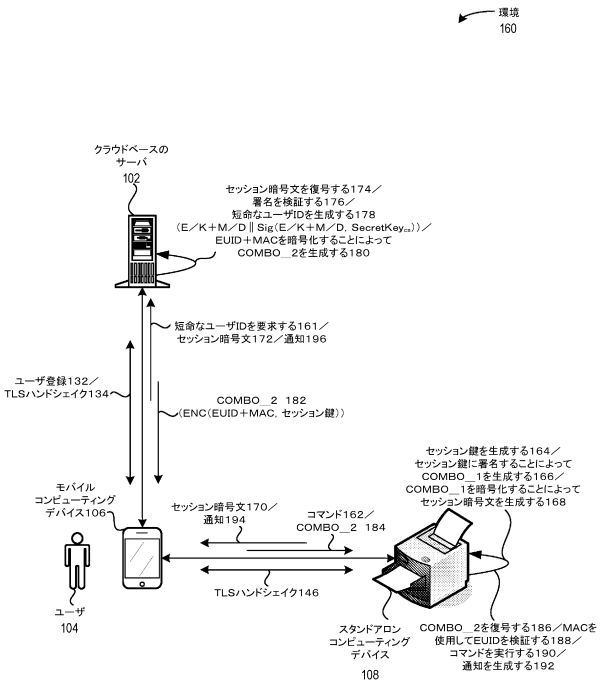
【図１Ａ】



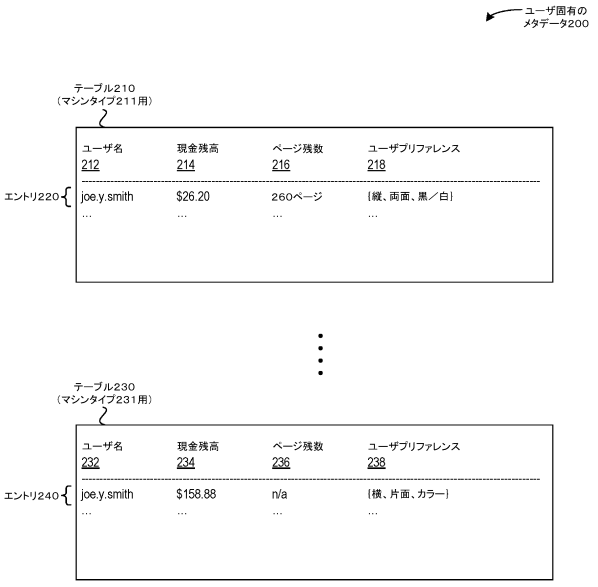
【図１Ｂ】



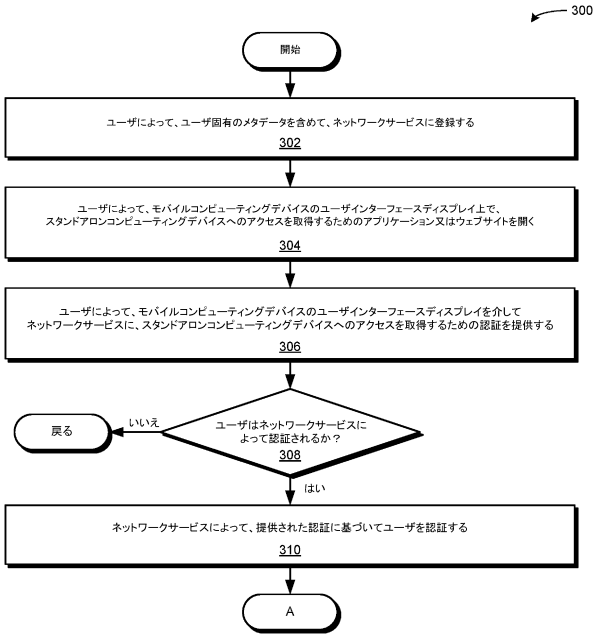
【図１Ｃ】



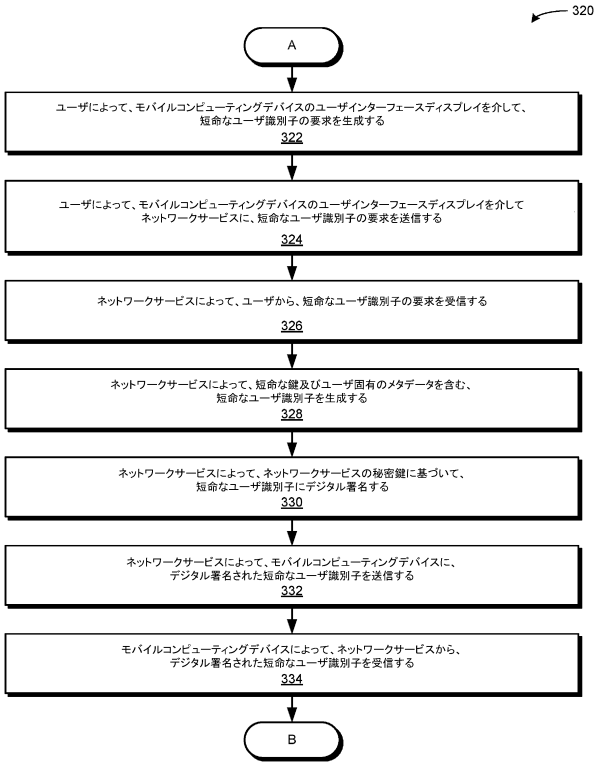
【図２】



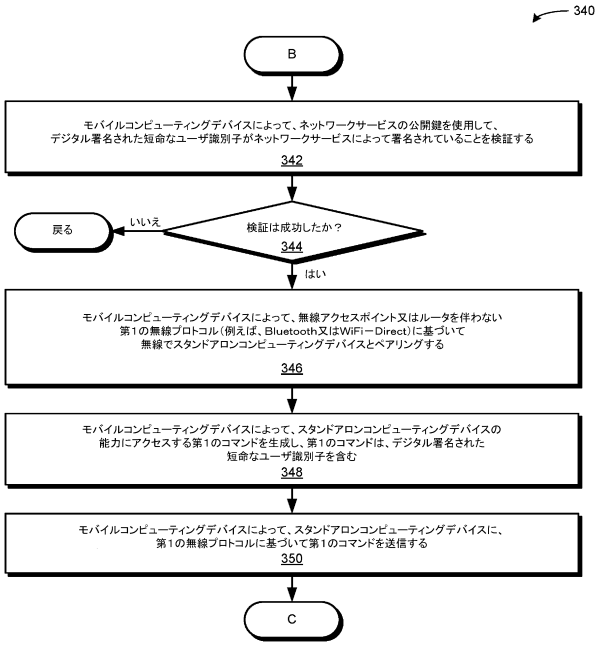
【図３Ａ】



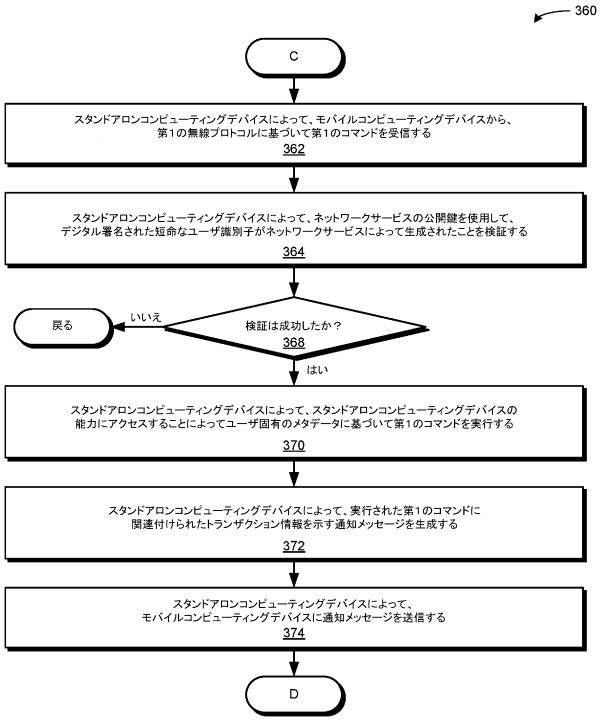
【図３Ｂ】



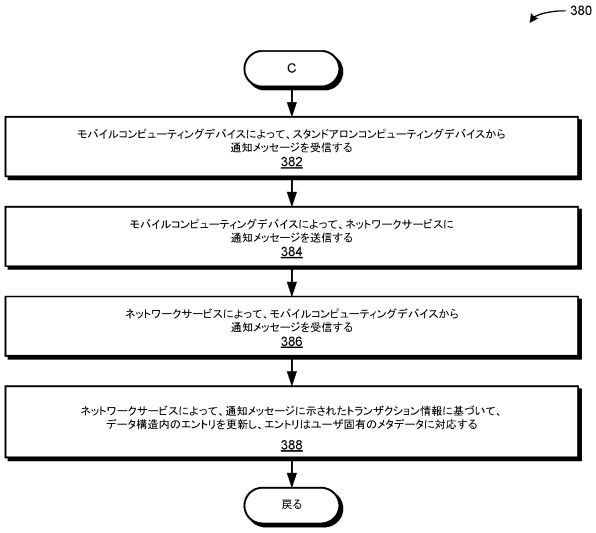
【図３Ｃ】



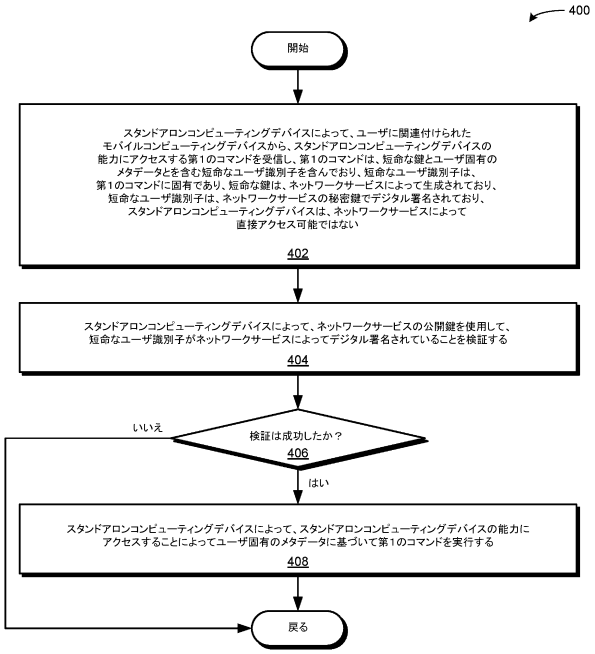
【図３Ｄ】



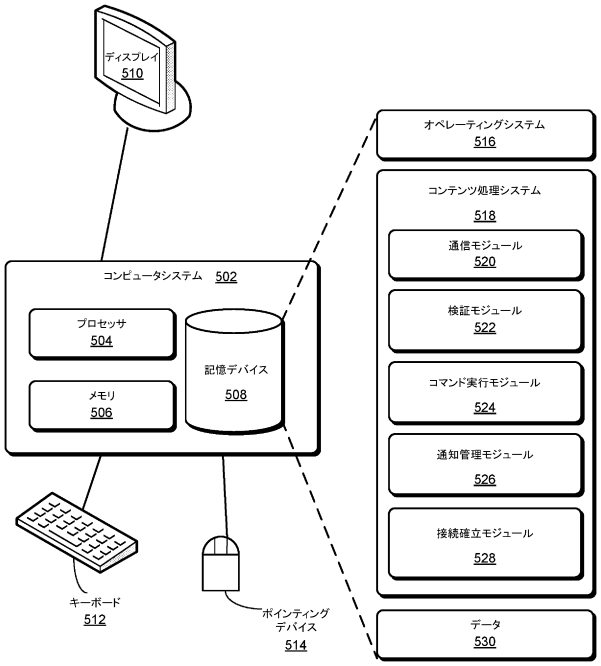
【図３Ｅ】


380
C
モバイルコンピューティングデバイスによって、スタンドアロンコンピューティングデバイスから
通知メッセージを受信する
382
モバイルコンピューティングデバイスによって、ネットワークサービスに
通知メッセージを送信する
384
ネットワークサービスによって、モバイルコンピューティングデバイスから
通知メッセージを受信する
386
ネットワークサービスによって、通知メッセージに示されたトランザクション情報に基づいて、
データ構造内のエントリを更新し、エントリはユーザ固有のメタデータに対応する
388
戻る

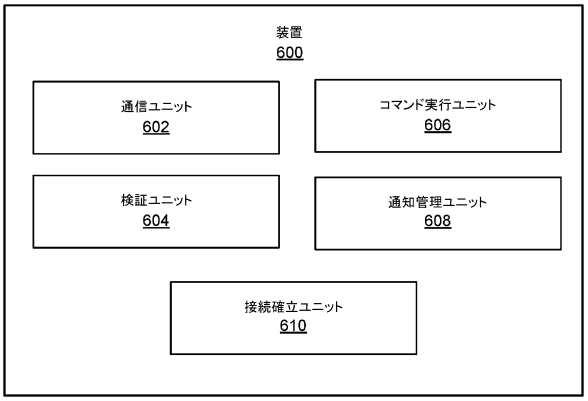
【図４】


400
開始
スタンドアロンコンピューティングデバイスによって、ユーザに関連付けられた
モバイルコンピューティングデバイスから、スタンドアロンコンピューティングデバイスの
能力にアクセスする第１のコマンドを受信し、第１のコマンドは、短命な鍵とユーザ固有の
メタデータとを含む短命なユーザ識別子を含んでおり、短命なユーザ識別子は、
第１のコマンドに固有であり、短命な鍵は、ネットワークサービスによって生成されており、
短命なユーザ識別子は、ネットワークサービスの秘密鍵でデジタル署名されており、
スタンドアロンコンピューティングデバイスは、ネットワークサービスによって
直接アクセス可能ではない
402
スタンドアロンコンピューティングデバイスによって、ネットワークサービスの公開鍵を使用して、
短命なユーザ識別子がネットワークサービスによってデジタル署名されていることを検証する
404
いいえ
検証は成功したか？
406
はい
スタンドアロンコンピューティングデバイスによって、スタンドアロンコンピューティングデバイスの能力に
アクセスすることによってユーザ固有のメタデータに基づいて第１のコマンドを実行する
408
戻る

【図５】


ディスプレイ
510
コンピュータシステム 502
プロセッサ
504
メモリ
506
記憶デバイス
508
キーボード
512
ポインティング
デバイス
514
オペレーティングシステム
516
コンテンツ処理システム
518
通信モジュール
520
検証モジュール
522
コマンド実行モジュール
524
通知管理モジュール
526
接続確立モジュール
528
データ
530

【図６】


装置
600
通信ユニット
602
コマンド実行ユニット
606
検証ユニット
604
通知管理ユニット
608
接続確立ユニット
610

フロントページの続き

弁理士　上杉 浩
(74)代理人　100120525
弁理士　近藤 直樹
(74)代理人　100139712
弁理士　那須 威夫
(74)代理人　100158551
弁理士　山崎 貴明
(72)発明者　シャンタヌ・レイン
アメリカ合衆国 カリフォルニア州 ９４０２５ メンロー・パーク シャロン・パーク・ドライブ ６７５ アパートメント ２０１
(72)発明者　アレハンドロ・イー・ブリト
アメリカ合衆国 カリフォルニア州 ９４０４０ マウンテン・ビュー オルテガ・アベニュー １６３

審査官　平井 誠
(56)参考文献　国際公開第２０１８／１６０８６３（WO，Ａ１）
特表２０１５－５１４２６９（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／００－４０
Ｇ０６Ｆ　２１／００－８８