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

特許第4199074号
(P4199074)

(45)発行日　平成20年12月17日(2008.12.17)　(24)登録日　平成20年10月10日(2008.10.10)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	660E
H04L	9/08	(2006.01)	H04L	9/00	601E

請求項の数 18　外国語出願　(全 26 頁)

(21)出願番号　特願2003-308871 (P2003-308871)
(22)出願日　平成15年9月1日 (2003.9.1)
(65)公開番号　特開2004-166238 (P2004-166238A)
(43)公開日　平成16年6月10日 (2004.6.10)
審査請求日　平成16年12月14日 (2004.12.14)
(31)優先権主張番号　0220203.4
(32)優先日　平成14年8月30日 (2002.8.30)
(33)優先権主張国　英国 (GB)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】安全なデータ通信リンクのための方法と装置

(57)【特許請求の範囲】
【請求項１】
所望のデータを要求する要求データと、該所望のデータを暗号化する際に用いられる委任鍵とを含むトークンを使用して、第１のデータ処理システムと第２のデータ処理システムとの間の安全な通信リンクを初期設定する方法であって、
前記第１のデータ処理システムは、
前記要求データ及び前記委任鍵のうちの少なくとも１つと、前記第１のデータ処理システムの秘密鍵または前記第１及び第２のデータ処理システムで共有される秘密鍵とを用いて、認証データを生成し、
前記委任鍵と、前記要求データと、前記認証データとを含む第１のメッセージを生成し、
前記第１および第２のデータ処理システムで共有される鍵または前記第２のデータ処理システムの公開鍵を使用して前記第１のメッセージを暗号化して、第１暗号化メッセージを生成し、
安全な通信リンクを初期設定するために前記第１のデータ処理システムから前記第２のデータ処理システムへ、前記第１暗号化メッセージを送信し、
前記第１暗号化メッセージを受信した前記第２のデータ処理システムは、
前記第１暗号化メッセージを復号した結果得られる前記第１のメッセージから、前記委任鍵、前記要求データ、及び前記認証データを取得し、
（ａ）取得された前記委任鍵、前記要求データ、及び前記認証データと、（ｂ）前記

第１のデータ処理システムの公開鍵、または前記第１及び第２のデータ処理システムで共有される前記秘密鍵とを用いて、復号した結果得られた前記第１のメッセージの有効性の有無を確認することを含む方法。

【請求項２】

前記第１暗号化メッセージを受信した前記第２のデータ処理システムは、

前記第１のメッセージが有効であるとき、前記取得された要求データの応答として、前記取得された委任鍵で暗号化された前記所望のデータを前記第１のデータ処理システムへ送信することを含む請求項１記載の方法。

【請求項３】

前記第１暗号化メッセージを受信した前記第２のデータ処理システムは、

前記第１のメッセージが有効であるとき、（ａ）前記所望のデータを要求する新たな要求データと、該所望のデータを暗号化する際に用いる新たな委任鍵とのうちの少なくとも１つと、（ｂ）前記第２のデータ処理システムの秘密鍵、または前記第２のデータ処理システム及び他のデータ処理システムで共有される秘密鍵とを用いて、新たな認証データを生成し、

前記新たな委任鍵、前記新たな要求データ、前記新たな認証データ、前記委任鍵、前記要求データ、及び前記認証データを含む第２のメッセージを生成し、

前記第２のメッセージを暗号化して、第２暗号化メッセージを生成し、

前記他のデータ処理システムへ前記第２暗号化メッセージを送信することをさらに含む請求項１記載の方法。

【請求項４】

第１、第２および第３のデータ処理システム間の安全な通信連鎖を初期設定する方法であって、

前記第１のデータ処理システムは、

所望のデータを要求する第１の要求データと、該所望のデータを暗号化する際に用いられる第１の委任鍵とを含む第１のトークンを生成し、

前記第１のデータ処理システムの秘密鍵または前記第１及び第２のデータ処理システムで共有される秘密鍵を用いて、前記第１のトークンの認証データを生成し、

前記第１の委任鍵と、前記第１の要求データと、前記第１のトークンの認証データとを含む第１のメッセージを生成し、

前記第１および第２のデータ処理システムで共有される鍵または前記第２のデータ処理システムの公開鍵を使用して前記第１のメッセージを暗号化して、第１暗号化メッセージを生成し、

安全な通信リンクを初期設定するために前記第１のデータ処理システムから前記第２のデータ処理システムへ、前記第１暗号化メッセージを送信し、

前記第１暗号化メッセージを受信した前記第２のデータ処理システムは、

前記第１暗号化メッセージを復号した結果得られる前記第１のメッセージから、前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データを取得し、

（ａ）取得された前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データと、（ｂ）前記第１のデータ処理システムの公開鍵、または前記第１及び第２のデータ処理システムで共有される前記秘密鍵とを用いて、前記第１のメッセージの有効性の有無を確認し、

前記第１のメッセージが有効であるとき、前記所望のデータを要求する第２の要求データと、該所望のデータを暗号化する際に用いる前記第２の委任鍵とを含む第２のトークンを生成し、

前記第２のデータ処理システムの秘密鍵または前記第２及び第３のデータ処理システムで共有される秘密鍵を用いて、前記第２のトークンの認証データを生成し、

前記第２の委任鍵、前記第２の要求データ、前記第２のトークンの認証データ、前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データを含む第２のメッセージを生成し、

前記第２及び第３のデータ処理システムで共有される鍵または前記第３のデータ処理システムの公開鍵を使用して前記第２のメッセージを暗号化して、第２暗号化メッセージを生成し、

前記第２のデータ処理システムから前記第３のデータ処理システムへ前記第２暗号化メッセージを送信することを含む方法。

【請求項５】

前記第２暗号化メッセージを受信した前記第３のデータ処理システムは、

前記第２暗号化メッセージを復号した結果得られる前記第２のメッセージから、前記第２の委任鍵、前記第２の要求データ、前記第２のトークンの認証データ、前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データを取得し、

少なくとも（ａ）取得された前記第２の委任鍵、前記第２の要求データ、及び前記第２のトークンの認証データと、（ｂ）前記第２のデータ処理システムの公開鍵、または前記第２及び第３のデータ処理システムで共有される前記秘密鍵とを用いて、前記第２のメッセージの有効性の有無を確認し、

前記第２のメッセージが有効であるとき、前記取得された第１の要求データの応答として、前記取得された第１の委任鍵で暗号化された前記所望のデータを前記第１のデータ処理システムへ送信することを含む請求項４記載の方法。

【請求項６】

前記第２暗号化メッセージを受信した前記第３のデータ処理システムは、

前記第２暗号化メッセージを復号した結果得られる前記第２のメッセージから、前記第２の委任鍵、前記第２の要求データ、前記第２のトークンの認証データ、前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データを取得し、

少なくとも（ａ）取得された前記第２の委任鍵、前記第２の要求データ、及び前記第２のトークンの認証データと、（ｂ）前記第２のデータ処理システムの公開鍵、または前記第２及び第３のデータ処理システムで共有される前記秘密鍵とを用いて、前記第２のメッセージの有効性の有無を確認し、

前記第２のメッセージが有効であるとき、前記取得された第２の要求データの応答として、前記取得された第２の委任鍵で暗号化された前記所望のデータを前記第２のデータ処理システムへ送信することを含む請求項４記載の方法。

【請求項７】

前記第１のトークンの認証データは前記１のデータ処理システムの秘密鍵を用いて生成されている場合、

前記第３のデータ処理システムは、さらに、

（ｃ）取得された前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データと、（ｄ）前記第１のデータ処理システムの公開鍵とを用いて、前記第２のメッセージの有効性の有無を確認することを含む請求項５記載の方法。

【請求項８】

前記第１のトークンの認証データは前記１のデータ処理システムの秘密鍵を用いて生成されている場合、

前記第３のデータ処理システムは、さらに、

（ｃ）取得された前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データと、（ｄ）前記第１のデータ処理システムの公開鍵とを用いて、前記第２のメッセージの有効性の有無を確認することを含む請求項６記載の方法。

【請求項９】

前記トークンは該トークンの有効期間を示す寿命データを含む請求項１記載の方法。

【請求項１０】

前記第１暗号化メッセージは、暗号化されていない前記第２のデータ処理システムの識別子を含む請求項１記載の方法。

【請求項１１】

前記第１のトークンは、前記第１のデータ処理システムで発生されるタイムスタンプ及

びまたは前記第１のデータ処理システムで１回のみ使用される任意の数をさらに含み、前記第１のメッセージは、該タイムスタンプおよびまたは該任意の数をさらに含む請求項４記載の方法。

【請求項１２】

前記第２のトークンは、前記第２のデータ処理システムで発生されるタイムスタンプ及びまたは前記第２のデータ処理システムで１回のみ使用される任意の数をさらに含み、前記第２のメッセージは、該タイムスタンプおよびまたは該任意の数をさらに含む請求項４記載の方法。

【請求項１３】

第１暗号化メッセージを受信する手段と、

前記第１暗号化メッセージを復号した結果得られる第１のメッセージから、所望のデータを要求する第１の要求データと、該所望のデータを暗号化する際に用いる第１の委任鍵と、前記第１の要求データ及び前記第１の委任鍵を含む第１のトークンを認証するための認証データとを取得する手段と、

（ａ）取得された前記第１の要求データ、前記第１の委任鍵、及び前記認証データと、（ｂ）非対称暗号方式の公開鍵または対称暗号方式の秘密鍵とを用いて、前記第１のメッセージの有効性の有無を確認する手段と、

前記第１のメッセージが有効であるとき、前記所望のデータを要求する第２の要求データと、該所望のデータを暗号化する際に用いる前記第２の委任鍵とを含む第２のトークンを生成する手段と、

非対称暗号方式または対称暗号方式の秘密鍵を用いて、前記第２のトークンの認証データを生成する手段と、

前記第２の委任鍵、前記第２の要求データ、前記第２のトークンの認証データ、前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データを含む第２のメッセージを生成する手段と、

前記第２のメッセージを暗号化して、第２暗号化メッセージを生成する手段と、

前記第２暗号化メッセージを送信する手段と、

を含むデータ処理システム。

【請求項１４】

前記確認する手段は、取得された前記第１の要求データと前記第１の委任鍵とから前記第１のトークンを再構成し、再構成された第１のトークンと、取得された前記認証データと、非対称暗号方式の公開鍵または対称暗号方式の秘密鍵とを用いて、前記第１のメッセージの有効性の有無を確認する請求項１３記載のデータ処理システム。

【請求項１５】

他のデータ処理システムとの間で安全な通信リンクを初期設定するデータ処理システムであって、

（ａ）所望のデータを要求する要求データ、（ｂ）該所望のデータを暗号化する際に用いられる委任鍵、（ｃ）前記要求得データと前記委任鍵とのうちの少なくとも１つと、前記他のデータ処理システムの秘密鍵または前記他のデータ処理システムと前記データ処理システムとの間で共有される秘密鍵とを用いて生成された認証データと、を含むメッセージを、前記他のデータ処理システムと前記データ処理システムとの間で共有される鍵または前記データ処理システムの公開鍵を使用して暗号化することにより暗号化メッセージを生成する前記他のデータ処理システムから送信された前記暗号化メッセージを受信する手段と、

前記暗号化メッセージを復号した結果得られるメッセージから、前記要求データと、前記委任鍵と、前記認証データとを取得する手段と、

（ａ）取得された前記要求データ、前記委任鍵、及び前記認証データと、（ｂ）前記データ処理システムの公開鍵、または前記他のデータ処理システム及び前記データ処理システムで共有される前記秘密鍵とを用いて、復号した結果得られた前記メッセージの有効性の有無を確認する手段と、

前記メッセージが有効であるとき、前記取得された要求データの応答として、前記取得された委任鍵で暗号化された前記所望のデータを送信する手段と、
を含むデータ処理システム。
【請求項１６】
前記認証データは、前記要求データと前記委任鍵を含むトークンの認証データであって、
前記確認する手段は、取得された前記要求データと前記委任鍵とから前記トークンを再構成し、再構成されたトークンと、取得された前記認証データと、前記データ処理システムの公開鍵、または前記他のデータ処理システム及び前記データ処理システムで共有される前記秘密鍵とを用いて、前記メッセージの有効性の有無を確認する請求項１５記載のデータ処理システム。
【請求項１７】
コンピュータを、
第１暗号化メッセージを受信する手段、
前記第１暗号化メッセージを復号した結果得られる第１のメッセージから、所望のデータを要求する第１の要求データと、該所望のデータを暗号化する際に用いる第１の委任鍵と、前記第１の要求データ及び前記第１の委任鍵を含む第１のトークンを認証するための認証データとを取得する手段、
（ａ）取得された前記第１の要求データ、前記第１の委任鍵、及び前記認証データと、（ｂ）非対称暗号方式の公開鍵または対称暗号方式の秘密鍵とを用いて、前記第１のメッセージの有効性の有無を確認する手段、
前記第１のメッセージが有効であるとき、前記所望のデータを要求する第２の要求データと、該所望のデータを暗号化する際に用いる前記第２の委任鍵とを含む第２のトークンを生成する手段、
非対称暗号方式または対称暗号方式の秘密鍵を用いて、前記第２のトークンの認証データを生成する手段、
前記第２の委任鍵、前記第２の要求データ、前記第２のトークンの認証データ、前記第１の委任鍵、前記第１の要求データ、及び前記第１のトークンの認証データを含む第２のメッセージを生成する手段、
前記第２のメッセージを暗号化して、第２暗号化メッセージを生成する手段、
前記第２暗号化メッセージを送信する手段、
として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項１８】
コンピュータを、他のデータ処理システムとの間で安全な通信リンクを初期設定するデータ処理システムとして機能させるためのプログラムであって、
該コンピュータを、
（ａ）所望のデータを要求する要求データ、（ｂ）該所望のデータを暗号化する際に用いられる委任鍵、（ｃ）前記要求データと前記委任鍵とのうちの少なくとも１つと、前記他のデータ処理システムの秘密鍵または前記他のデータ処理システムとの間で共有される秘密鍵とを用いて生成された認証データと、を含むメッセージを、前記他のデータ処理システムとの間で共有される鍵または前記データ処理システムの公開鍵を使用して暗号化することにより暗号化メッセージを生成する前記他のデータ処理システムから送信された前記暗号化メッセージを受信する手段、
前記暗号化メッセージを復号した結果得られるメッセージから、前記要求データと、前記委任鍵と、前記認証データを取得する手段、
（ａ）取得された前記要求データ、前記委任鍵、及び前記認証データと、（ｂ）前記データ処理システムの公開鍵、または前記他のデータ処理システム及び前記データ処理システムで共有される前記秘密鍵とを用いて、前記メッセージの有効性の有無を確認する手段、
前記メッセージが有効であるとき、前記取得された要求データの応答として、前記取得

された委任鍵で暗号化された前記所望のデータを送信する手段、
として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は全般的に、特に責任が要求されるところの安全な通信リンクのための方法、装置、およびコンピュータプログラムコードに関する。発明は特に信頼が委任されるシステムにおいて、責任の連鎖を確立するために役に立つ。
【背景技術】
【０００２】
操作の端末のモードを適合させるソフトウェアコンポーネント、システム、またはアプリケーションソフトウェアの購買などのmコマースのために、安全なデータ伝送は重要である。また、移動端末へのソフトウェアの安全なダウンロードとインストールもマルチメディアエンターテインメント、遠隔医療、プログラマブル移動端末のためのアップグレード、異なった無線規格へのアップグレードなどで重要である。再構成可能な移動端末は、例えば異なったタイプの無線システムを支持し、および異なったシステムの統合を許容するため、所望のアプリケーションをダウンロードおよびインストールすることによりエンドユーザが彼らの個人的な必要性のために端末をカスタム設計することができる増加した柔軟性を提供することができる。しかしながら、彼らのソフトウェアを受話器製造者、ネットワークオペレータまたは信頼された第三者ソースからの利用可能なソフトウェアと悪意に取りかえるハッカーに対して移動端末を保護する技術が必要である。
【０００３】
PANは互いにおよびそれらのユーザと共に情報を交換する必要がある多くの移動装置を含むかもしれない。セルラー無線、ブルートゥース(商標)（ブルートゥース特別利益団体(SIG)、http://www.bluetooth.com/）、IrDA(赤外線データ協会(IrDA)、http://www.irda.org/)、およびWLAN（例えば、無線のローカル・領域・ネットワークIEEE規格802.11“1999版のISO/IEC 8802-5-1998、ローカルおよびメトロポリタン領域ネットワークのための規格－無線のLAN媒体アクセス制御(MAC)と物理レイヤ(PHY)の仕様”1999）のような技術が採用され使われるかもしれない。安全なデータ転送がデータの秘密性、保全、認証、および非拒否などの特性に必要とされる。
【０００４】
ポケットPC、移動電話、およびPAN(パーソナルエリアネットワーク)環境におけるラップトップなどの移動端末間には限られた量の信頼がしばしばある。パーソナル領域ネットワーク(PAN)文脈で作動する再構成可能な移動端末のための安全な移動委任のためのプロトコルの必要がある。特に、PAN文脈で再構成可能な移動端末のための安全な委任を支持するために安全な鍵分配技術が必要である。PAN環境において、例えば代替のネットワークに接続するため、および／または異なったネットワークプロバイダーと他の移動端末を通してアプリケーションサービスを受信するため、装置は再構成する必要があるかもしれない。再構成する装置の能力は再構成可能な領域の潜在力を実現するために処理される必要がある多くの安全な問題点を上げる。非常に分散している環境は安全な委任技術のための要件を示す。さらに、脅威はウイルス、トロイの木馬、およびウォームなどの悪意があるソフトウェアから増える。人は、高レベルアプリケーションとシステムソフトウェア(リングトーンを含んでいる)ダウンから下層ベースバンドモジュールへ、再構成可能な端末におけるソフトウェア変更/アップグレードを防護する安全な移動委任を潜在的に採用することができる。
【０００５】
一般的な暗号方式技術を見直すことが有用である。概して現在のところ、例えば、ソフトウェアダウンロードのための安全なデータ伝送を提供するために、２つの基本的な暗号方式、対称および非対称の技術が使われる。対称の暗号は暗号化と解読の両方に伝統的な線に沿って共通の秘密鍵を使用する。データは、例えば、各伝送のためまたは小さいグル

ープのデータ伝送のために異なる鍵を使用して、この秘密鍵へのアクセスを制限することと鍵管理技術によって保護される。対称の暗号の周知の例は米国データ暗号化規格(DES)アルゴリズムである(米国国立標準局のFIPS-46、FIPS-47-1、FIPS-74、FIPS-81)。この変形は3個の鍵が追加の安全を提供するために連続していて使用されるトリプルDES(3DES)である。対称の暗号方式のアルゴリズムに関する他の例は、RSA Data Security、Inc、および国際データ暗号アルゴリズム(IDEA)からのRC4である。

【０００６】

非対称の、即ち、いわゆる公開鍵暗号は一組の鍵、１つは“秘密”および１つは“公開”(公開鍵の分配は実際にはしばしば制限されるが)を使用する。公開鍵で暗号化されるメッセージは秘密鍵でのみ解読することができ、逆もまた同様である。その結果個人は対応する公開鍵の任意の1つにより解読のため秘密鍵を使用してデータを暗号化することができ、同様に、公開鍵をもっているだれでも秘密鍵だけがデータを解読するのに使用することができるという知識で公開鍵金庫にそれを暗号化することによって個人にデータを安全に送ることができる。

【０００７】

一般に、非対称の暗号方式システムは鍵管理機能を提供する公開鍵インフラストラクチャ(PKI)として知られているインフラストラクチャの中で使用される。また、非対称の暗号は、秘密鍵を使用してメッセージまたはメッセージのダイジェストのどちらかを暗号化することにより、デジタル的署名メッセージに使用することができる。受け手がオリジナルのメッセージを提供すると、それらは例えばデジタル証明書(以下を参照)から得られる対応する公開鍵を使用してメッセージのダイジェストを解読することによって、同じダイジェストを計算しかつその結果署名を認証することができる。メッセージのダイジェストがオリジナルのメッセージから得られ、一般にオリジナルのメッセージよりも短いので、ダイジェストからオリジナルのメッセージを計算することを困難にし、いわゆるハッシュ関数(h)がメッセージのダイジェストを生成するために使用されるかもしれない。一方向性の衝突回避性のある（one-way collision-resistant）(推測しにくい) ハッシュ関数がR.Rivest、“The MD4 message-digest algorithm”Internet Request for Comments 1320、April 1992、およびR.Rivest、“The MD5 message-digest algorithm” Internet Request for Comments 1321、April 1992に与えられる。

【０００８】

デジタル署名と同等物は対称の暗号に存在しており、共有された秘密鍵を使用して計算されるいわゆるMAC(メッセージ立証コード)である。MACに関する例は、ISO 8731-1、“Banking-Approved algorithms for message authentication-Part1: DEA”標準化のための国際機構、ジュネーブ、スイス1987で見出すことができる。MACに関する別の例は、例えばコンピュータデータ認証、国立標準局FIPS発行113、1985に説明されるような鍵をかけられたハッシュ関数である。MACは、例えば受信されたソフトウェアモジュールのハッシュ値と関連するインストールチケットに含まれるそれとを比較することによって、受信されたソフトウェアモジュールの保全をチェックすることができる。しかしながら、この技術は秘密鍵が共有されているので、信頼されたプロバイダーと端末ユーザとのどんな論争の場合も、非拒否を保証しない。

【０００９】

パブリックキーインフラストラクチャは通常、デジタルアイデンティティ（同一性）サーティフィケーション（証明書）の提供を含む。個人が他の誰かのふりをするのを防ぐために、個人は個人の公開鍵を含んでいる認可秘密鍵を使用して署名された証明書を発行する認証局に対して彼のアイデンティティを立証することができる。認証局（ＣＡ）の公開鍵は広く知られかつ信頼されており、証明書が認可秘密鍵を使用して暗号化されただけであるので、個人の公開鍵は証明書によって確かめられる。移動電話ネットワークに関する文脈の中では、ユーザまたはネットワークオペレータがそれらの秘密鍵でメッセージを署名することによって、それらのアイデンティティを認証することができる; 同様に公開鍵はアイデンティティを立証するために使用することができる。無線のアプリケーションの

ためのPKIのさらなる詳細は、WPKI、WAP-217-WPKI、www.wapforum.orgで利用できる2001年4月24日のバージョン、およびwww.ietf.orgで見つけることができるX.509仕様(PKIX)に見い出すことができ、これらはすべてこれに引用文献として組み込まれる。

【００１０】

後で説明されるべき発明の実施例では、PKI(パブリックキーインフラストラクチャ)が採用されていると仮定される。そのような環境において、製造者およびオペレータなどの信頼された一団は、スマートまたは他のカード（例えばSIM: Subscriber Identity Module、WIM：Wireless Identity Module、SWIM: SIMとWIMの結合、USIM:Universal Subscriber Identity Module）のような安全な改変耐性のあるモジュールにそれらを格納する移動端末に彼らの証明書を通常発行する。より一般に公開鍵は製造において端末に、またはSIMカードの上に格納されるか、それらはダウンロードされるかもしれない。例えば、移動端末は他の移動端末の公開鍵か証明書をダウンロードするためにネットワークオペレータの読み出し専用ディレクトリにアクセスするかもしれない。

【００１１】

PKIは非拒絶を提供しかつ双方の一団を保護する；対照的に、対称のセッション鍵は低いオーバーヘッドと速いダウンロードを提供する(例えば、公認された公開鍵を使用して別の信頼された一団からそれがいったん輸送されたなら)。そのようなセッション鍵は増加された安全のため短い期間だけ有効であるかもしれない。対称の暗号を使用して通信リンクを確立するため、非対称の暗号方式技術を使用する安全なソフトウェアダウンロードのための技術は、C.YeunおよびT. Farnham “Secure Software Download for Programmable Mobile User Equipment” IEE 3G Mobile Communication Technologies Conference 2002年5月8-10日、および2002年1月17日に共にファイルされた出願人の係属中英国特許出願第0201048.6および0201049.4に記述された。非対称の暗号は最初にDiffieとHellmanにより1976年に開示され（W. Diffie and D.E.Hellman、“New directions in cryptography”、IEEE Transactions on Information Theory、22(1976)、644-654）、多くの非対称の暗号方式技術は現在公共の領域にあり、その最もよく知られたものはRSA(Rivest、Shamir およびAdleman)アルゴリズムである（R.L.Rivest、A. Shamir and L.M.Adleman、“A method for obtaining digital signatures and public-key cryptosystems”Communications of the ACM、21(1978) 120-126）。他のより最近のアルゴリズムは楕円曲線暗号システム（例えば、X9.63、“Public key cryptography for financial services industry:Key agreement and key transport using elliptic curve cryptography”、Draft ANSI X9F1、10月(1999)）を含む。X.509 ITU(国際電気通信連合)規格は公開鍵証明書に一般的に使用される。この中に鍵発行人のための唯一の識別子を含む証明書は、公開鍵(および、通常アルゴリズムと認証局に関する情報)とともにディレクトリを含み、ディレクトリは個人と機構による使用のための証明書の公共の貯蔵所である。

【００１２】

上で概説された対称および非対称の暗号方式技術は各々利点と欠点を持っている。非対称のアプローチは複雑な計算と安全の対応するレベルを達成するために対称のアプローチより比較的長い鍵長を必要とし、リソース効率が劣る。しかしながら、対称のアプローチは端末の中に秘密鍵の格納を必要とし、非拒否(データの発信または受信を立証する)を提供しない。

【００１３】

データ伝送は移動電話ネットワーク内で重要性をますます増加するようになり、特に、例えば、第三世代パートナーシッププロジェクト(3GPP、3GPP2)によって作られた規格で記述されるいわゆる2.5Gと3G(第三世代)ネットワークで重要であり、その技術的な仕様はwww.3gpp.orgで見出すことができ、これにより引用文献として組み入れられる。

【００１４】

図１は第三世代のデジタル移動電話システム10の一般的な構造を示す。図１において、無線塔12は基地局コントローラ16によって制御される基地局14と結合される。移動通信装置18は、無線、即ちエアインタフェース20、知られているGSM(移動通信のためのグローバ

ルシステム)ネットワークおよびGPRS(ジェネラルパケット無線サービス)ネットワークのUmインタフェース、およびCDMA2000およびW-CDMAネットワークのUuインタフェースを横切って基地局14と双方向通信として示される。通常一時に複数の移動装置18が与えられた基地局に付属され、基地局はこれらの装置にサービスするため複数の無線トランシーバーを含む。

【００１５】

基地局コントローラ16は複数の他の基地局コントローラ(示されない)と共に移動交換センター(MSC)22と結合される。そのような複数のMSCはゲートウェイMSC(GMSC)24に結合され、それは順次移動電話ネットワークを公衆電話交換網(PSTN)26に接続する。ホームロケーションレジスタ(HLR)28とビジターロケーションレジスタ(VLR)30が呼ルーティングとローミングを管理し、他のシステム(示されない)が認証、支払いを管理する。運転と維持センター(OMC)29は、基地局などのネットワークインフラストラクチャ要素からの統計を集めて、ネットワークの性能の高いレベルの視点をネットワークオペレータに提供するために切り換る。例えば、ネットワークの利用可能な容量がどれくらいあるか、またはネットワークの一部が一日の異なる時間に使用されるかを決定するために、OMCを使用することができる。

【００１６】

上記ネットワークインフラストラクチャは、本質的に移動通信装置18と他の移動装置および/またはPSTN 26との間の回路交換音声接続を管理する。GPRSなどのいわゆる2.5Gネットワーク、および3Gネットワークは、回路交換音声サービスにパケットデータサービスを付加する。広い用語で、パケット制御装置(PCU)32が基地局コントローラ16に加えられ、スイッチの階層的なシリーズによりインターネット38などのパケットデータ網に接続される。GSMに基づいたネットワークでは、これらはサービスGPRSノード(SGSN)34とゲートウェイGPRSサポートノード(GGSM)36を含む。図１のシステムと後で説明されるシステムにおいて、ネットワーク内の要素の機能性が単一の物理的なノード上、または、システムの別々の物理的なノード上にあるかもしれないことが認識されるであろう。

【００１７】

一般に、移動装置18およびネットワークインフラストラクチャ間の通信はデータと制御信号の両方を含んでいる。データはデジタルに符号化された音声データを含み、またはデータモデムは移動装置へ、または移動装置からのデータをトランスペアレントに通信するように採用されるかもしれない。GSM-タイプネットワークテキストおよび他の低い帯域幅では、データはまたGSM ショートメッセージサービス(SMS)を使用して送られるかもしれない。

【００１８】

2.5Gまたは3Gネットワークでは、移動装置18は単純な音声の接続よりもむしろ別の電話を提供するかもしれない。例えば、移動装置18はビデオおよび/またはマルチメディアデータサービス、ウェブブラウジング、電子メールおよび他のデータサービスにアクセスを付加的または代替的に提供するかもしれない。論理的に移動装置18は、データプロセッサやパーソナルコンピュータのような端末装置に直列接続で移動端末(加入者アイデンティティモジュール(SIM)カードを組み込んでいる)を含むと考えられるかもしれない。一般に、移動装置がいったんネットワークに付属すると、それは“常にオン”であり、例えば、移動端末－端末装置インタフェースで標準のATコマンドによって、装置と外部のデータネットワークとの間でトランスペアレントにユーザデータを移すことができる。通常の移動電話が移動装置18のために使われるところでは、GSMデータカードなどのような端末のアダプタが必要であるかもしれない。

【００１９】

図２は基本的安全移動通信システムのモデル200を図式的に示す。移動装置、即ち端末202は固定された、即ち基地局206を経て移動電話ネットワークまたはWLANのような移動通信ネットワーク208と結合される。移動通信ネットワーク208は順次インターネットなどのコンピュータネットワーク210と結合され、それにサーバ204が付属される。移動装置202

およびサーバ204の１つまたは両方はデジタル証明書を記憶し、デジタル証明書212はサーバ204のために公開鍵を含んでいる移動装置202に格納され、デジタル証明書214は移動装置202のために公開鍵を含んでいるサーバ204に格納される(他の配列において、これらは必要とされるときダウンロードされてもよい)。例えば、サーバはネットワークオペレータ、移動装置製造者または第三者によって操作されるかもしれない。移動装置は通常ユーザによって操作され、単純さのために単一の移動装置だけが示されているが、一般に多くのそのような装置がある。通信メカニズム216は移動装置202とサーバ204との間でデータを輸送するために提供されるが、そのようなデータは多くの仲介者(図２で示されない)を通して送られる。

【００２０】

3Gに関する文脈では、安全なデータ伝送のための移動電話システム規格はまだ決定されていなくて、議論は現在MExEフォーラム(移動局アプリケーション実行環境フォーラム)において、www.mexeforum.org (そこからまたMExE仕様も利用可能である)で行われている。また、言及はISO/IEC 1170-3、“Information Technology-Security Techniques-Key Management-Part3: Mechanism Using Asymmetric Techniques”、DIS 1996でもなされている。

【００２１】

概してMexEは標準化されたアプリケーション環境を定義する。分散されたネットワークのための委任プロトコルが、特に3GPP TS23.057“移動局アプリケーション実行環境(MExE)”に提示され、引用文献としてここに組み込まれる。PKIを使用した、比較的簡単な認証プロトコルが現在計画され、その中で移動端末(MT)は、MTに安全にインストールされるルート鍵（例えば多くのCAのルート鍵は製造中にインストールされるかもしれない）、または証明書に付属するか供給される署名された公開鍵のどちらかの公開鍵を有する。次に、この公開鍵は対応する秘密鍵を有する実行可能な署名をチェックするのに使用される。例えば、ソフトウェアが第三者ソフトウェア開発者から入手されるところでは、開発者は公開-秘密鍵対および証明書（CAによって署名され、開発者の公開鍵を含んでいる）を生成する（またはCAから得る）。これ(または、いくつかの例において鍵連鎖の一組の証明書)は実行可能に追加され、次に、MTはソフトウェアが開発者の(証明された)公開鍵に対応する秘密鍵によって署名されたことを確認することができる。

【００２２】

再構成可能な、ソフトウェアデファインドラジオ(SDR；ソフトウエア無線機)の概念は最近の、活発な研究の対象である(例えば、“Authorization and use of Software Defined Radio:First Report and Order”、米国の連邦政府通信委員会ワシントンDC2001年9月参照)。SDR可能なユーザ装置およびネットワーク装置は改良された性能および/又は追加特徴を提供するためにそれらの特性を再構成するように動的にプログラムされることができ、したがってまた、サービスプロバイダーのための追加収入の流れの機会を提供する。ソフトウェアデファインドラジオは民間で商用および軍事の両セクターでアプリケーションを持っている。

【００２３】

SDRフォーラム（Software Defined Radio(SDR)Forum http://www.sdrforum.org/）は標準化された機能を有する共通のソフトウェアAPI層のオープンアーキテクチャを定義した。この配列の概要を図3に示す。図3では、SDRは一組の7つの独立したサブシステム302a-gを含み、それぞれ1つ以上のアプリケーションに共通なハードウェア、ファームウェア、オペレーティングシステム、およびソフトウェアモジュールを順次含む。制御機能304はモジュールの間で交換されるデータおよび情報を含むそれぞれの機能的なブロック、ユーザトラヒック（‘Ｉ’）の制御(‘Ｃ’)を提供する。移動(無線)端末におけるSDRの実施は、速度のためにいくつかのベースバンドサービス実施と制御機能が、たとえば中間的リアルタイムのカーネルまたはドライバーを通してよりはむしろハードウェア層に直接インターフェイスするが、一般的なPCで動くソフトウェアに類似している。図３のSDRシステムは後の説明される発明による方法の実施例を実施する際に使用に適している。

【００２４】
しかしながら、安全な委任概念を安全な(SDR)ソフトウェアダウンロードに結合する必要が、例えば、PANに関する文脈である。再構成の過程は、ネットワーク検出から情報を照合しまたは実体を監視し、かつ貯蔵所からソフトウェアコンポーネントをダウンロードするアプリケーション、装置、およびユーザからの要求、能力、およびプロフィールを入手するために必要である。これは潜在的に、信頼の委任が重要である非常に分散している環境である。
【００２５】
安全なシステムの目的のいくつかが認証(例えば、パスワードおよび/又はバイオメトリック技術で、データ創始者または受け手の)、アクセス制御、非拒否、例えば、PANノード間の伝送データの保全、および秘密性(例えばPANノード間でメッセージを暗号化することにより)にある。“匿名”のデータダウンロードへの供給があるかもしれず、それは特に受け手を確認しないでデータを供給または放送することである。しかしながら、既存の安全なメカニズムは他の実体に対する責任の支持とタスクの委任を欠く。このような関係においては、概して責任は、望ましくは協会が別の実体または一団に立証される（または、高い確率で少なくとも決定される）ことができるような方法で、実体を有する物、行動または権利の協会について言及する。概して委任は第1により第２の実体の認可(例えば行動を実行する)について言及し、権利(すなわち、安全な方針または他のデータの何らかの部分）を共有することにより、第２の実体が第１に代わって行動することを可能にされる。責任が委任されるところに、権利または他のデータが共有されるよりもむしろ好ましくは転送され、そのため行動が実体に曖昧でなくリンクされることができる。
【００２６】
委任プロトコルを保証することに関する背景従来技術は、M.Gasser and E. McDermott、“An architecture for practical delegation in a distributed system”、Proceedings of the IEEE Symposium on Security and Privacy、pp. 20-30 1990; M.Low and B. Christianson、“Self authenticating proxies”、Computer Journal Vol33、pp.422-428、October 1994; Y.Ding、P.Horster and H.Peterson、“A new approach for delegation using hierarchical delegation token”、Proceedings of the 2nd Conference on Computer and Communication Security、pp128-143、1996；および特にB.Crispo、“Delegation Protocols for Electronic Cmmerce”、Proceedings of the 6th IEEE Symposium on Computer and Communications、Hammamet、Tunisia、3-5-July 2001に見出すことができる。しかしながら、現在の解決策は責任と信頼を欠くか、または比較的効率が悪い。特にCrispo(ibid)で提案されたプロトコルは4つのメッセージパスを必要として、非対称の技術に制限され、実際には委任をカスケードすることを防止する複雑さのあるものである。
【発明の開示】
【発明が解決しようとする課題】
【００２７】
従来技術により教示されるよりも少ないメッセージパスを有するプロトコルを提供し、好ましくは非対称および対称の暗号方式の技術の両方で作動することが可能なことが望ましい。さらに、比較的コンパクトで効率的であるメッセージを維持している間、カスケードな委任のため適当なプロトコルを提供することが望ましい。
【００２８】
概して、知られているプロトコルで責任の問題を処理するため、ここに記述された方法の実施例では、２つの異なった鍵が導入され、１つは単に認証のためであり、別の鍵は委任鍵として機能する。これは、認証と委任の有効期間が独立していることを許容し、そのような分離はまた、役割ベースのモデルの実現を容易にする。例えば、鍵機能が分離されなくて、委任された権利/責任が認証鍵に異なった寿命があるならば、鍵の更新は非常に厄介であるかもしれない。さらに、ここに記述されたプロトコルはカスケードな委任を容易にして、すべてのかかわった実体(例えば、移動行為者)の中で端から端まで責任を維持

する。

【課題を解決するための手段】

【００２９】

したがって、発明の1つの態様によれば、第１の鍵と関連する第１の要求データとを含む第１のトークンを使用して第１のデータ処理システムと第２のデータ処理システムとの間の安全な通信リンクを初期設定する方法が提供され、方法は前記第１のトークンと、前記第１のシステムの秘密鍵を使って前記第１の鍵および前記第１の要求データのうちの少なくとも１つの処理をすることにより生成された認証データとを含む第１のメッセージを第１のシステムで発生させ；暗号化された第１のメッセージを形成するために前記第１および第２のデータ処理システムの両方に既知の鍵を使用して前記第１のメッセージを暗号化し；前記安全な通信リンクを初期設定するため、前記暗号化された第１のメッセージを前記第１のシステムから前記第２のシステムへ送ることを含む。

【００３０】

望ましくは、認証データは第１の鍵と第１要求データとの両方を作動させることにより、即ち、第１のトークンを作動させることによって発生される。事実上、トークンは委任鍵を含む委任トークンであり、特に認証データのトークンを含むメッセージは、例えば、認証データがデジタル署名またはMAC(メッセージ認証コード)を含むので、証明可能である。

【００３１】

第１のシステムの秘密鍵は個人鍵を含んでもよく、その対応する公開鍵は第２のシステムにアクセス可能であり、またはそれは(少なくとも) 第１と第２のシステムの間で共有される秘密（secret）の鍵を含んでもよく、またはそれは第１(すなわち、委任)の鍵を含んでもよい(例えば、ここでは暗号よりむしろ非拒否が最も重要である)。しかしながら、望ましくは、秘密鍵は非対称(公開鍵)暗号方式のシステムの個人鍵である。

【００３２】

第１のメッセージを暗号化するのに使用された第１および第２のデータ処理システムの両方に知られた鍵は、対称または非対称の暗号方式のシステムのための鍵であってもよい。非対称の暗号方式のシステムの場合では、鍵は第２のシステムの公開鍵を含むかもしれない(理論的に、第２のシステムは公開鍵に対する秘密鍵のみ知る必要があるが、実際には第２のシステムは秘密鍵と公開鍵の両方を知るであろう)。暗号化されたメッセージは有線または無線のリンクなどの通常の通信リンク上で送られるかもしれない。

【００３３】

要求データは役割、タスク、サービス、またはソフトウェアのようなデータを要求するデータ、あるいは幾つかの他の要求データを含むかもしれない。第１の、即ち委任鍵は、第１の、即ちスタートポイントシステムと安全な通信の連鎖を確立するために、第２のシステムにより、または、委任の連鎖の終わりのシステムにより使用されるかもしれない。第１の、即ち委任鍵は第１のシステムに送り返されるべきデータを暗号化するのに使用されるかもしれないか、またはアイデンティティを確認するためにデジタル署名などのある他の安全機能のために使用されるかもしれない(デジタル署名は特定のタイプの暗号化されたデータとして見られるかもしれない)。データは直接またはシステムの連鎖に沿った何れかで第１のシステムに返送されるかもしれない。システムのそのような連鎖では、第１の鍵はエンドシステムと第１のシステムとの間で直接通信のため使用されるかもしれないが、データはシステムの連鎖に沿って、すなわち、間接的に返送され、一組のまたは連鎖の委任鍵が連鎖の各リンクのために1つ採用される。

【００３４】

ここに第１のデータ処理システムはデータ処理システムの連鎖において中間のデータ処理システムであり、方法は、前のデータ処理システムから前のトークンと前の認証データを含む前の暗号化されたメッセージを第１のデータ処理システムで受け取り、前のトークンは前の鍵および関連する前の要求データを含み、前の認証データは少なくとも1つの前の鍵と前のシステムの秘密の鍵を有する前の要求データを作動させることにより発生され

たデータを含み、第１および前のデータ処理システムの両方に知られた鍵を使用して前の暗号化されたメッセージを解読し、第１のメッセージに前のトークンと前の認証データを含んでいることをさらに含んでいる。

【００３５】

望ましくは、前の認証データは、例えば、前のシステムの公開鍵で前の認証データを作動させるか、または対称の暗号方式のシステムの共有された鍵で認証データを作動させることによって確かめられる。同様に第１の認証データは第２のデータ処理システムで確かめられるかもしれない。この方法において、安全な通信リンクは連鎖内の各対のデータ処理システムの間で確立されるかもしれず、各データ処理システムは前のシステムから受け取られた委任トークンと関連した認証データを確認する。

【００３６】

データ処理システムの“連鎖”が言及されるが、これは、例えば連鎖が要素の多重接続ネットワークの要素の系列を含むことができるように、連鎖の要素の間で他の通信リンクを排除しない。しかしながら、委任の過程の実施例はそのようなネットワークの中に安全なリンクの系列を含む安全な連鎖を確立することができる。

【００３７】

別の態様では、発明は連鎖を成す各連続したデータ処理マシンのアイデンティティが確認可能である複数のデータ処理マシンの間の安全な通信リンクの連鎖を確立する方法を提供し、方法は第１のマシンの後の連鎖内の各連続したデータ処理マシンにおいて、認証データと委任鍵を含む委任トークンとを含む暗号化されたメッセージを連鎖内の前のデータ処理マシンから受け取り、前記暗号化されたメッセージを解読し、拡張されたメッセージを形成するために前記連続したデータ処理マシンのための委任トークンおよび認証データを解読されたメッセージに追加し、前記拡張したメッセージを暗号化し、前記暗号化された拡張されたメッセージを連鎖内の次のマシンに転送し、連鎖のエンドマシンに到達するまでこれらのステップを実行することにより安全な通信リンクの前記連鎖が確立されるステップを実行することを含む。

【００３８】

また、発明は上述の方法を実施するように構成されまたはプログラムされた１つまたは複数のデータ処理システムを提供する。

したがって、さらなる態様において、発明はデータ処理装置を提供し、そのデータ処理装置は処理されるべきデータを格納するように作動可能なデータメモリと、プロセッサが実行可能な指示を格納する指示メモリと、データメモリおよび指示メモリと結合され、指示に従ってデータを処理するように作動可能なプロセッサとを含み、前記指示は、トークンと認証データを含むメッセージを発生させ、トークンは鍵および関連する要求データを含み、認証データは少なくとも1つの前記鍵およびデータ処理装置の秘密の鍵を有する前記要求データを作動させることにより発生され、暗号化されたメッセージを形成するため第２のデータプロセッサに既知の鍵を使用して前記メッセージを暗号化し、前記データ処理装置と前記第２のデータプロセッサとの間の安全な通信リンクを初期設定するため、前記暗号化されたメッセージを前記第２のデータプロセッサに送るように、プロセッサを制御するための指示を含む。

【００３９】

このデータ処理装置は、例えば必要な暗号方式の機能を実行するために別の処理システムと関連して例えばスマート端末またはダム端末を含んでもよい。

さらなる態様では、発明は連鎖の1つ以上のデータ処理システムで上述された方法を実施するためのコンピュータプログラムコードを提供する。このコードは、望ましくは、ハードまたはフロッピーディスク、CD-またはDVD-ROMなどの担体、または、リードオンリーメモリやフラッシュメモリなどのプログラムされたメモリに格納されるか、またはそれは光学または電気信号担体で提供されてもよい。熟練した人は、発明が純粋なソフトウェア、またはソフトウェア(または、ファームウェア)とハードウェアの組み合わせ、または純粋なハードウェアによる何れかで実施されてもよいことを認識するだろう。同様に方法の

ステップは単一の処理要素の中で必ず実行される必要はなく、例えば、プロセッサのネットワークのような多くの要素間に分配することができる。

【発明の効果】

【００４０】

その結果、発明の実施例はソフトウェア、チケット、クーポン、および他のデータ、例えば音楽とMPEG映画クリップなどの流されたメディアデータの抜粋とmコマースデータのダウンロードを容易にする。

【発明を実施するための最良の形態】

【００４１】

発明は図を参照して例だけの方法でさらに説明される。

人々はますます携帯電話、ラップトップ、PDA、および同様の装置に依存するようになり、ヘッドホンと音楽プレーヤーなどの周辺機器を持ち運ぶかもしれない。パーソナルエリアネットワーク(PAN)の概念は、IrDA、ブルートゥースおよび／またはWLAN技術(例えば、IEEE 802.11)のような技術を使用してこれらの装置間のローカル(すなわち、個人的な)通信を熟考する。いくつかのPANが認可局の取り締まりを提供するためにコンポーネント管理者を含むかもしれない。一般に、PANの端末は2つのクラス、即ち、PANを制御および構成するかもしれないスマート端末(PDA、スマート電話、ラップトップまたは車など)、および一般に、スマート端末に1つの機能および接続のみを提供するダム端末(プリンタ、スキャナ、記憶媒体、およびユーザーインタフェース装置など)に分類される。ダム端末は、例えば委任トークンの要求を評価するためにスマート端末と通信し、スマート端末はそのような評価の結果を返すかもしれない。端末の２つのクラスは統一された構成をサポートし、装置レベルとPANレベルの両方において制御インタフェースにアクセスすることが期待される。ダム端末に関しては、これはそれらの専門化している機能性に加えて鍵管理能力、ソフトウェアアップグレード能力、およびサービス広告を含むことができる。いくつかのダム端末がまたサービス発見を実行することができ、非補助される他の装置からサービスを要求することさえできるかもしれない。

【００４２】

ソフトウェアをダウンロードするとき、２つの安全の問題があり、第一にどんな偶然または故意の不正に対してもソフトウェアの起源と高潔を保護すること、第二に、例えばSDRについて、ダウンロードソフトウェアを受け入れるかどうか、および含みによりSDRを再構成してそれを使用するためのような自動決定をすることを可能にする認可システムを提供することである。一片のコードへのPKIのデジタル署名の付加はその正当性と起源について確かめるためにコードの受け手により使用することができる。上で説明されたように、署名を確認するために必要な公開鍵は、署名されたコードと共に送られたまたはコードの受け手によって貯蔵所から検索された公開鍵証明書から得られるかもしれない。コードがいったん確かめられると、SDRは、証明書局の１つ以上のアイデンティティに基づくコード、コード署名者公開鍵を得るために確かめられた証明書の方針識別子、装置の所有者および/又はユーザにより入力された任意の方針声明とともに製造者により装置に組み込まれた1つ以上の方針声明、およびコードの使用の意図された範囲の詳細などのコードと直接関連する任意の情報を受け入れるかどうか決めることができる。

【００４３】

非対称(すなわち、公開鍵)の暗号方式を採用する発明の実施例において、我々は、PKIが採用され、それが製造者、オペレータ、信頼された第三者および政府の規制者のような信頼された一団が移動端末にそれらの証明書を発行し、それらを例えば改変耐性のあるハードウェアモジュールに格納することができると仮定する。PKIインフラストラクチャは対称(すなわち、共有された秘密の鍵)の暗号方式を採用するいくつかの実施例では必要ではなく、例えば、そこでは保全の保証のみが要求される。

【００４４】

図４はPANと関連するネットワークインフラストラクチャに関する例を示す。PAN400は示された例において、互いに無線(rf)の通信にある移動端末402、PDA404、およびカメラ4

06を含む。移動端末402はまたインターネット414へのゲートウェイ412を有する第１の3G移動電話ネットワーク410の基地局408と通信にある。第２のユーザにより担持される第２の移動端末416がインターネット414への第２のゲートウェイ422で第２の3G移動電話ネットワーク420の第２の基地局418と通信にある。PDA404はまたインターネット414と結合されるIEEE 802.11 WLANなどのようなWLAN 424と通信にある。認識されているように、第１および第２の第三者ソフトウェア開発者サーバ426、428、ホームPC430および１つ以上のｍ-コマースサーバ432で示されるように、多くの他のシステムがインターネットと結合されるかもしれない。移動端末402と416には、破線434によって示されるように、例えば、ブルートゥースリンクを通して互いに通信の直接ラインがあるかもしれない。

【００４５】

例により委任の使用を例証することは役に立つ。簡単な例では、移動端末402のユーザは、端末の製造者から新しいソフトウェアをダウンロードすることによって、それらの端末のソフトウェアをアップグレードさせることが望まれるかもしれない。これを達成するために、移動端末402は電話ネットワーク410のサービスプロバイダーまたはネットワークオペレータに委任トークン(DT)を渡し、それらは順次委任トークンを製造者に渡し、次に、製造者がサービスプロバイダーまたはネットワークオペレータにソフトウェアアップグレードを実行するタスクを委任する。別の例においては、移動端末402のユーザ（以後移動行為者Aと言う）は新しい映画(または、幾つかの他のソフトウェア)のクリップを取得したがっているが、関連するネットワーク410はこのサービスを提供しない。しかしながら、異なったオペレータによって実行されるネットワーク420はこのサービスを提供し、したがって、移動行為者Aは必要なら最初にネットワーク420からそれを得る移動端末416（以後移動行為者Bと言う）のユーザから映画クリップを入手することができる。続いて２つの例、第一に移動行為者Aが直接移動行為者Bから映画クリップを入手することができること、第二に移動行為者Bが他の移動行為者Cから、この場合ネットワークオペレータ420にクリップを要求しなければならない状況であることが考えられる。

【００４６】

図５は移動端末A502で始まる端末の連鎖500を示し、移動端末A502は第2の端末B504と通信しており、最後に例示された例では連鎖はサーバなどの端末Z506で終わる。各端末はメモリに接続されたプロセッサを含み、メモリは対称および／または非対称の暗号化および解読コードのような暗号方式のコード、および公開鍵証明書(すなわち、他の実施例では、共有された対称の鍵)を格納する。また、各プロセッサは、端末または連鎖の何れかの側の端末と無線(または、有線) 通信リンクを実行するために１つ以上の通信リンクと結合される。例示された例の端末A502はSIMカードを有する移動端末を含み、それは例えば、デジタル証明書データを格納するかもしれない。

【００４７】

図６は連鎖の端末の1つとして使用に適した汎用計算機システム600を示す。コンピュータシステム600はアドレスおよびデータバス602を含み、それにキーボード608、表示610、およびオーディオおよび/又は丈夫なスクリーンインタフェースなどのマン・マシン・インタフェース(MMI)606が結合される。幾つかの実施例において、暗号方式の処理システムすなわち、メモリと(ことによると専用)プロセッサはSIMカードなどの除去可能なカードに提供されるかもしれない。図６はMMIが一般に欠けているが、そのようなシステムを示す。また、バス602にネットワークインタフェース(サーバのための)、無線または赤外線のインタフェース(電話かPDAのための)、または接触パッドインタフェース(SIMカードのための)のような通信インタフェース604が結合される。さらにバス602にプロセッサ612、ワーキングメモリ614、不揮発性データメモリ616、および典型的にフラッシュメモリを含む不揮発性メモリである不揮発性プログラムメモリ618が結合される。

【００４８】

不揮発性プログラムメモリ618は暗号方式コード、すなわち、暗号および解読コード、デジタル署名/MAC検証コード、メッセージおよび委任鍵発生コード、通信インタフェースのためのドライバーコードを格納する。プロセッサ612は、発明の実施例による方法を実

施するために対応する処理を提供するこのコードを実行する。不揮発性データメモリ616は、望ましくはデジタル証明書(非対称の暗号方式が採用されるところで)、および/又は対称のセッション鍵証明書(対称の暗号方式が採用しているところで)内に公開鍵を格納する。

【００４９】

ワーキングメモリは委任鍵を含む1つ以上の委任トークン、および別の端末に通すため受信されまたはダウンロードされたソフトウェア(連鎖の端にこのソフトウェアが不揮発性メモリ、例えばSDRに収納されるかもしれない)を格納するために使用することができる。ソフトウェアはコンピュータプログラムコードおよび/又はビデオまたはMP3データのようなデータを含むかもしれない。

【００５０】

以下のテキストにおいて便利のため、記述されたプロトコルが行為者間の通信に特に役立つように基準が移動行為者に作られるであろう。しかしながら、これは、固定行為者または端末で有効に採用されるかもしれないプロトコルの応用を制限する何らかの方法として解釈されるべきでない。その上、“端末”はここでは広い意味で使用され、何らかの通信能力を有するデータ処理システムを示す。

【００５１】

例えば、再構成可能な端末のための、安全な移動委任のためのプロトコルの一実施例では、移動行為者 Aは以下の方程式 1に設定されるように移動行為者 Bへ署名されたメッセージM1を送る。

$$M1：A\rightarrow B：B \| T_A/N_A \| P_B\ (K_{P-T-E} \| \Gamma \| S_A\ (h\ (DT)))\qquad (式1)$$

ここにA→Bは、AがBにM1を送ることを表し、‖はデータの連結を表す。式1において、DTは委任トークンであり、P_B(Y)はBの公開鍵を使用してYの非対称(公開鍵)の暗号(例えば、RSAを使用する)を表し、S_A(Y)はAの秘密(署名)鍵を使用してYの署名動作を表し、hは一方向性の衝突回避性のあるハッシュ関数(上記のMD4またはMD5アルゴリズムのような)を表す。委任トークン(DT)は以下によって与えられる。

【００５２】

$$DT=K_{P-T-E} \| B \| T_A/N_A \| \Gamma \qquad (式2)$$

ここにΓ＝（R,L）、Rは要求または役割かタスクの組み、Lは移動行為者 Aによって発生された委任トークンDTの寿命を示し、K_{P-T-E}は移動行為者 Aと移動行為者 Bとの間のリンクのための“執行力”委任鍵(移動行為者 Aによって発生された対称鍵か公開鍵のどちらかであるかもしれない)と呼ばれる。“執行力”という句は、ここでは実行されるべきコードがK_{P-T-E}により暗号化されているので、例えば端末Aが製造者からネットワークオペレータを通して新しいオペレーティングシステムをダウンロードおよび実行することである。移動行為者 Aによって発生された対応する秘密の鍵が秘密を保たれる。K_{P-T-E}が公開鍵であるならば、移動行為者 Aは公開暗号化鍵として使用可能な公開鍵および署名のために使用される秘密鍵を有する。それぞれ大きい素数を含むこの対の鍵は、例えば、Blum Blum Shub-タイプジェネレータを使用して、通常発生されるかもしれない。

【００５３】

擬似乱数発生の技術がL.Blum、M.Blum、M.Shub、“A simple unpredictable random number generator”、SIAM Jounal of Computing、 Vol. 15pp 364-383、1986およびW.Alexi、B.Chor、O.Goldreich、and C.P.Schnorr“RSA and Rabin Functions: Certain part are as hard as the whole”、SIAM Jounal of Computing、Vol 17、pp 194-209、1988に開示され、参照されるかもしれない。

【００５４】

値T_AはAで発生される任意のタイムスタンプであり、N_AはAによって発生される任意のノンス（Nonce;一回だけ使用される数）である。ノンスは決定論的疑似-乱数発生器(例えば擬似乱数の同期された級数)のシードとして発生されまたは使用されるかもしれない。タイムスタンプまたはノンスの何れかを使用する選択は移動行為者の技術的な能力および

環境次第であり、例えばタイムスタンプを利用することが再生攻撃を妨げるが、端末が適切な同期されたクロックを欠くところでは、ノンスが好まれるかもしれない。

【００５５】

M1における識別子Bの包含と委任トークンDTは意図された確認者より他のだれかによって受け入れられることからトークンを防ぐために望ましい。

このプロトコルの変形において、非対称の暗号よりも対称な暗号が使用されるかもしれない。この変形において、移動行為者 Aと移動行為者 Bは共有された秘密の鍵k_1の形で予め確立された関係を有し、鍵をされたハッシュ、またはISO 8731-1(前記された)で定義されたMACアルゴリズムの1つのようなメッセージ立証コード(MAC)はデジタル署名として使用することができる。１つ以上の共有された秘密の鍵が、例えば、YeunとFarnham（ibid）およびUK特許出願0201048.6と0201049.4で説明された技術を使用して確立されるかもしれない。１人の移動行為者が頻繁に同じ移動行為者(または、移動行為者の組)と通信するシナリオでは、より少ない処理パワーが要求されるように、これはより効率的な解決策であるかもしれない。メッセージM1がAからBへ以下のように送られる:

$$M1：A\rightarrow B：B \| T_A/N_A \| E_{k1}(K_{P-T-E} \| \Gamma \| MAC_{k1}(DT)) \quad (式3)$$

ここに、$E_{k1}(Y)$はAとBの間で共有される鍵K_1を使用してYの対称の暗号を示す。移動行為者が信頼されたホスト上で実行しており、移動行為者の秘密(すなわち、例えば、安全なハードウェアモジュールにおいて存在している暗号方式の鍵)が信頼を落さなかったなら、式３のプロトコルはデータ起源の保証を提供するに十分である。ここにK_{P-T-E}は、例えば、選択的に端末の能力に依存している時間のデータとハッシュドされおよび／または結合された擬似乱数を使用して、通常発生されるかもしれない対称の暗号方式の鍵である。鍵K_{P-T-E}は、それが（セッションの後または期間あるいは寿命の後に）再使用できないセッション鍵の形を成し、その結果攻撃の受けやすさが減少される。

【００５６】

再び、委任トークン複製と委任トークン削除に対する防御のために、委任トークンDTは、望ましくは、意図された受け手とタイムスタンプなどのリフレッシュ値、および／または乱数(一度以上使用することができる、例えば疑似ランダム数列からの数)、および／またはノンスを含むように組み立てられる。以前に言及されたように、時計ベースのタイムスタンプは同期された時計を必要とし、それはいくつかのプラットホームには実用的でないかもしれない。

【００５７】

上記プロトコルそれ自身カスケード委任に導かれ、即ち初期の移動行為者 Aから連鎖内の第２の行為者Bへ、それから第3の行為者Cへ、そしてデータが返されるか、または最終的なメッセージがオリジナルの移動行為者 Aに送られる前に、そのように連鎖内の最終的なの行為者、即ちZへカスケードされる委任に多重移動行為者がある。このような連鎖は図５を参照してより詳細にすでに説明された。

【００５８】

以下に説明されるカスケードされたプロトコルにおいて、オリジナルの移動行為者Aは他の移動行為者によって十分に信頼されていると仮定され、AからZへのそれぞれの移動行為者は委任トークンに署名するため移動行為者の暗号方式の鍵を使用することによって容易に有効な署名を生成することができる。説明されたプロトコルは、委任のカスケードが連鎖の下方へ続くとき、複雑さとメッセージサイズの比較的小さい増加の利点がある。

【００５９】

非対称および対称の両方の暗号方式の実施例のために、委任の初期の段階（即ち、AからBへ）が以前に説明されたように同じである。したがって、非対称の暗号について：

$$M1：A\rightarrow B：B \| T_A/N_A \| P_B(K_{P-T-E} \| \Gamma \| S_A(h(DT))) \quad (式4)$$

そしてBからCへの委任の第２段階のメッセージは:

$$M2；B\rightarrow C：$$

$$C \| T_B/N_B \| B \| T_A/N_A \| P_C(K_{P-T-E}, \| \Gamma' \| S_B(h(DT')) \| \Gamma \| K_{P-T-E}$$

$\| S_A$（h（DT））　　(式5)

ここに、

$DT' = K_{P-T-E'} \| C \| T_B / N_B \| \Gamma'$

$K_{P-T-E'}$ は移動行為者 Bと移動行為者 Cとの間の委任鍵を実行する能力であり、$\Gamma' = (R', L')$ ここに、R'＝ 要求または役割かタスクの組、L'＝ 移動行為者 Bによって発生された委任トークンDT'の寿命である。S_A（h（DT））は、それがメッセージM1に(暗号化された)Bによって受け取られたとき、M2に包含のためBに利用可能であることが認識されるだろう。

【００６０】

したがって、移動行為者Aによって提供されたDTが移動行為者 Bのメッセージの中に組み込まれまたはカスケードされる。M2およびDT'内の識別子Cの包含は意図された確認者より他の誰かにより受け入れられるトークンを防ぐために望ましく、前と同様に、タイムスタンプT_BまたはノンスN_Bのようなリフレッシュ値がまた付加されるかもしれない。さらに、委任は必要に応じて同じ手順の拡大によりさらに署名されたDTをもたらす。

【００６１】

対称の暗号の場合において、我々は、共有された秘密鍵k_i，i＝１，２，…，ｎおよび鍵をかけられたハッシュまたはMAC署名の形に予め確立した関係を仮定する。ここに、移動行為者はMAC関連委任トークンにその暗号方式の鍵を使用して有効なMACを生成することができる。しかし、望ましくはそれぞれの対称の鍵が連鎖における各対の移動行為者の間でのみ共有されるので(対立するものとして、例えば、各行為者は連鎖内の各他の行為者の共有された秘密鍵を知っている)、論争があるなら、連鎖内の各行為者は、例えばそれが受けたMACを確認する各行為者のように委任連鎖を見直し、確認し、または検証することに巻き込まれる。

【００６２】

対称な暗号のカスケードな委任のためのプロトコルが続く。委任の初期の段階（即ち、AからBへの段階）は前に対称の暗号のために説明されたのと同じである:

$M1：A \rightarrow B：B \| T_A / N_A \| E_{K1}$（$K_{P-T-E} \| \Gamma \| MAC_{K1}$（h（DT））　　(式6)

そしてBからCへの委任の第２段階のメッセージは：

Ｍ２；Ｂ→Ｃ：

$C \| T_B / N_A \| B \| T_A / N_A \| E_{K2}$（$K_{P-T-E'} \| \Gamma' \| MAC_{K2}$（DT'）$\| \Gamma \| K_{P-T-E} \| MAC_{K1}$（DT））　　(式7)

ここにE_{K_i}(Y)はｉとｉ＋１の間で共有された鍵K_i，i＝１，２，…，ｎを使用してYの対称の暗号を表し、Bで発生される委任トークンDT'は、

$DT' = K_{P-T-E'} \| C \| T_B / N_B \| \Gamma'$

ここに$K_{P-T-E'}$ は移動行為者 Bと移動行為者 Cとの間の委任鍵を実行する能力であり、$\Gamma' = (R', L')$ ここに、R'＝ 要求または役割かタスクの組、L'＝ 移動行為者 Bによって発生された委任トークンDT'の寿命である。

【００６３】

再び、移動行為者A により提供されるDTは移動行為者 Bのメッセージの中で組み込まれまたはカスケードされる。M2およびDT'内の識別子Cの包含は意図された確認者より他の誰かにより受け入れられるトークンを防ぐために望ましく、前と同様に、タイムスタンプT_BまたはノンスN_Bのような新鮮な値がまた付加されるかもしれない。さらに、委任は必要に応じて同じ手順の拡大によりさらに署名されたDTをもたらす。

【００６４】

委任の連鎖のエンドポイントにおける手順の例は、今記述される。移動行為者 Aのような創始者が仲介者へ、そして結局移動行為者 Yという最後の委任者に権利を渡すとき、最後の委任者は、例えば適切なサービスプロバイダー(連鎖のエンドポイント)のサーバZに連絡して、サービスが移動行為者 Aに許諾されることを要求するために、それが有効な(すなわち、適切に署名された) DTを保持することを証明する。

【００６５】
サーバが要求について確かめるため、すべての(署名された)DTが添付され、その結果、責任の追跡が必要であるなら、DTの拡散が追跡されることができる。これは、特定のDTを次の一団に渡すとき特定のDTを署名している各一団により、かつまたカスケードな委任で作成されたすべての署名されたDTを添付することにより達成される。エンドポイントはすべての添付署名を確認することができるが(例えば、適切な公開鍵証明書がPKIで利用可能であるので)、移動行為者の連鎖における最後の一団により供給される委任されたK_{P-T-E}を単に使用することだけが法的であるかもしれない。これは、この鍵(非対称または対称の鍵のどちらであれ)を使用して暗号化されたデータが移動行為者の連鎖における最後の一団によって解読可能または理解されるだけであるかもしれないからである。代わりに、例えば、アプリケーションと利用可能な通信リンクに依存して、サーバZはAのK_{P-T-E}を使用して直接Aに返答するかもしれない。
【００６６】
この配列はまた、トークンが使用されているところの追跡を許容する。DTは能力を提供し、すなわち、それは安全な通信またはある他の安全機能を可能にするが(例えば、K_{P-T-E}は署名に使用されるかもしれない)、DTはその能力を実行する許可を提供するというわけではない。例えば、図４を参照すると、ネットワーク420は異なるネットワーク、ネットワーク410によって役立たされる端末402にソフトウェア(コードまたはデータ)を提供するために移動端末416を禁じるかもしれない。サービス要求に続いて、DTがエンドポイント(例えばサーバZ)に提示されて、首尾よくアクセス制御方針に対してチェックされるときだけ、能力を使用する許可が許諾されるかもしれない。そのようなチェックは移動行為者 Aとの追加通信を必要とするかもしれず、そうだとすれば、この通信は、例えば、移動行為者 Aとエンドポイントとの間に、互いの認証、秘密性、および保全を提供するPKIサポートを有するSSL(安全なソケット層)のような安全なチャンネル上に作られているかもしれない。ソフトウェアをダウンロードして実行するために、例えば、開発者からの許可が一般的に必要であるが、例えば、クーポンの他のデータ実体は許可なしで移転可能であるかもしれない。
【００６７】
図４を参照して議論された上述の例に戻ると、移動行為者 Aが移動行為者 Bから映画クリップを要求する場合、方法またはプロトコルの一実施例において出来事のシーケンスは以下の通りである:
１．移動端末402(A)は委任鍵Kと所望の映画クリップのための要求Γを含む委任トークンを作成する（例えば、上述されたように鍵Kが慣例上発生されている）。要求Γは望ましくは、要求データRと同様に、例えば、映画クリップのための1時間または1日のような委任トークンDTの有効期間を指定する寿命データLを含んでいる。例えば一連の15分の映画クリップを要求することにより完全な映画が要求されるかもしれず、またはゲームのようなソフトウェアの項目が後に加えられた付加的な特徴を有して基本的で、初期のバージョンで要求されるかもしれないというように、要求は一連のサブ要求へ分析されるかもしれない。
【００６８】
２．端末Aは委任トークンDTをハッシュし、次にデジタル署名を作成するためにAの秘密鍵でハッシュされた値を暗号化する(代わりにMAC機能がDTに適用されるかもしれない)。ハッシュすることは必須ではないが、伝送されるべきデータの量を減少させるので好ましい；しかしながら、他の実施例においてはDTがハッシュすることなしに（選択的に、メッセージ回復を許すアルゴリズムとともに）署名されるかもしれない。
【００６９】
３．端末Aは、例えばネットワークオペレータ410またはネットワークオペレータ420のどちらかによって保持された（読み出し専用）倉庫からダウンロードされた、端末Bのための証明書から公開鍵P_Bを検索する。次に、端末Aは公開鍵P_B（または、AとBの共有された秘密の鍵）を使用して委任鍵K、要求Γおよびデジタル署名(またはMAC)を暗号化する。

【００７０】
4．端末Aは、上述されたように、端末Bのための識別子B（1人以上の可能な受け手がいて、ものまね攻撃を妨げることが好ましい任意の場合に必要）および望ましくはタイムスタンプまたはノンスを含んでいるメッセージM1を作成する。これはメッセージM1が時間間隔の後に満了することを許容し、例えば時間の窓内に回答がないなら、比較的短い期間が攻撃が可能である間に定義されることを許容する。連鎖内の端末が同期された時計(1秒より良いという)を有するならタイムスタンプが好ましく、そうでなければ、知られているシードから開始する擬似乱数発生器により発生されたノンスが使われるかもしれない。望ましくは、委任トークンDTはまたBのための識別子とタイムスタンプおよび／またはノンスを含む。この方法において、攻撃者がタイムスタンプまたはノンスを変えることを試みるなら、これは委任トークンDTに暴露するであろう。

【００７１】
5．次に、端末Aは任意の通常の通信手段を使用してメッセージM1を端末Bに送る。
6．端末Bは端末Aからのメッセージ M1を受ける。
7．端末Bは端末Bの公開鍵で(または、対称なシステムにおいて、AとBによって共有された秘密の鍵で) 暗号化されたメッセージM1の部分を解読する(PKIインフラストラクチャにおいて、端末BはAのデジタル証明書を所有しているか、または得ることができる)。次に、端末Bは委任鍵K、要求Γおよび端末Aのデジタル署名またはMACを抽出する。

【００７２】
8．端末Bは委任鍵K、要求Γおよび採用されるなら端末Bの識別子およびタイムスタンプ/ノンスを使用して委任トークンDTを再構成する。端末Bは次に、h(DT)を決定するために端末Aと同じハッシュ関数を委任トークンDTに適用し、端末Aの公開鍵(例えば、倉庫からダウンロードされる)を使用して端末Aの秘密鍵で署名されたメッセージh(DT)を解読し、2つのハッシュ値を比較する(代わりに、対称のシステムでは、２つのMACが比較されるかもしれない)。2つの値が同じであるならば、メッセージは確認されまたは認証され、したがって有効であると考えられる。（他の実施例において、端末Bが署名をチェックするこの鍵を知っているか、または入手することができるので、端末Aはh(DT)のデジタル署名を作成する委任鍵Kを採用するかもしれない。しかしながら、これはより弱い安全を提供する）。

【００７３】
この点において、端末Bは端末Aから送られた委任トークンを再構成し、確認した。したがって、端末Bは端末A(すなわち、責任がある)から発せられた知られている有効で認証された要求と委任鍵Kを所有している。したがって、端末Bは委任鍵Kで映画クリップ(または、他のデータ)を暗号化し、次に端末Aに暗号化されたデータを送り返す要求に応答することができる。端末Bは、例えば互いの認証、秘密性、および保全を提供するPKIサポートでSSL(安全なソケット層) などの別々の安全なチャンネルを使用して、例えばアクセスまたは防御方針に対して要求をチェックして、要求に応じる前に付加的の段階を実行するかもしれない。したがって、例えば映画クリップの場合では、端末Bは、端末Aがクリップを受けることを許可されているネットワークオペレータと共にチェックするかもしれない。その結果、要求に応答して端末Aに暗号化されたデータを送る端末Bの能力は、端末Bが要求に返答し、必要な操作を実行する許可(能力と対照的に)を有するか否かの質問から別々に取扱われるかもしれない。

【００７４】
9．この例において、端末Bが許可を有すると仮定すると、端末Bは委任鍵を使用して映画クリップを暗号化し、端末Aに暗号化されたデータを送り返す。(連鎖がAとBとの間に存在するところでは、暗号化されたデータは連鎖を下って、または直接BからAへ返送されるかもしれない)。

【００７５】
10．端末Aは端末Bから暗号化された映画クリップデータを受け取って、このデータを解読することができる。委任鍵Kが共有された秘密の鍵であるところでは、端末Aは対称の暗

号方式のアルゴリズムを使用してデータを解読する。委任鍵Kが非対称の暗号方式のシステムの公開鍵である場合は、端末Aは対応する秘密鍵を保有して、したがって、再び暗号化されたデータを解読することができる。

【００７６】

非対称の暗号方式が採用されるところでは、例えばAからの委任トークンがAの公開鍵を使用して確認されるかもしれないようにPKIが使用されることが見ることができる。実用的なシステムにおいて、端末AがSIMカードを組み込む移動端末であるところでは、SIMは連鎖における各端末のデジタル証明書を格納して、例えば、鍵発生のためプロセッサを組み込むかもしれない。代わりに、ネットワークオペレータの全ての端末は中央に、互いにアクセス可能な倉庫に格納されたデジタル証明書を提供され、どんな必要な証明書もメッセージの端末に送られるかもしれない。

【００７７】

上で説明されたプロトコルが委任鍵Kと要求Γのものまねを妨げる。概して端末AはKおよびΓを含む委任トークンを作成し、これに署名し、端末Bに組み合わせを送る前にB’の公開鍵でトークンと署名を暗号化する。端末Bは鍵と要求を抽出するためにトークンと署名を解読し、次に、署名が正しいと確かめられるならば、要求を満たすために鍵を使用することができる。

【００７８】

このプロトコルは上で記述されたように、連鎖の第３の実体Cがある場合に拡張されてもよい。上の例において、行為者Cが端末B416のためにネットワークオペレータのサーバを含むかもしれないので、端末Aが要求した映画クリップを端末Bが所有していないならば、端末BはAにクリップを渡す前に、その関連するネットワークオペレータからクリップを検索することができる。この場合に、端末BがメッセージM1を受信し、委任トークンDTの値を決定し、デジタル署名またはMACが端末Aのものであることを確かめた点で、上の手順は段階８に続いて変更される。次に、手順は以下の通り続く:

９．端末Bが、端末Aによるトークン DTの創造と同じ方法で、新しい委任鍵K’及び新しい要求Γ’を含む新しい委任トークンDT’を作成する。ΓとΓ’は所望の映画クリップのための要求データRを含むが、ΓとΓ’は一般に異なった有効期間、したがって異なった寿命LとL’を有するであろう。鍵KとK’は異なるので、連鎖の各リンクは異なった鍵で暗号化される。これはまた以下に見られるような責任を提供する。

【００７９】

１０．端末Bは、所望の映画クリップを要求しているのが端末Bであるかのように端末C(サーバ)に送られる新しいメッセージM2を構成する。したがって、端末Bは事実上端末Aの行為者になる。メッセージM2は、例えば、DT’の署名されたハッシュまたはDT’のMACを含む端末Bの委任トークンDT'および署名のためのメッセージM1データの解読されたコンテンツを追加し、次に、端末Cの公開鍵(または、共有された秘密の鍵)で全体を暗号化することによって構成される。選択的に、Cのための識別子とBのためのタイムスタンプ/ノンスが明確に添付されてもよい。メッセージM2は端末Cに送られる。

【００８０】

１１．端末Cは、その秘密鍵(または、共有された秘密の鍵)、DTおよびDT’を含む解読されたデータおよび端末Aと端末Bのための署名を使用してメッセージM2の暗号化された部分を解読する。(端末の連鎖では、最後の端末は連鎖のすべての端末のための委任トークンと署名を有する)。DTの署名されたハッシュが端末A(Bの公開鍵で暗号化された)からのメッセージM1に端末Bによって受け取られたので、端末Aにより署名されたDTのハッシュを含む端末Cのためのメッセージを発生させるために、端末Bが端末Aの秘密鍵を所有する必要がないことが認識されるであろう。この例において、端末Cは(端末の連鎖において、連鎖内の端末のそれぞれの進行のために)端末Bと端末Aの両方について委任トークンとトークンのための署名にアクセスを有する。すでに言及したように、PKIは連鎖における各端末(AとB)の各署名が確認されることを許容し、したがって各委任トークンが認証されることを許容する。また、連鎖の各実体(この場合、AとB)がそれら自身の署名された要求と鍵を

取着したので、プロトコルは責任を提供する。

【００８１】

12．端末Cは連鎖における各実体(この場合、AとB) の署名を確認し、必要であるところでは、要求または幾つかの要求のための許可をチェックする。次に端末Cは、Aの暗号化された委任トークンDTの鍵Kを使用して端末Aに直接返答するか、端末Cは、特に、端末Aの要求Γに応答するため鍵Kを使用して、順番にデータを転送する端末Bに送られるデータを暗号化するために委任鍵K'を使用して要求Γ’に対して端末Bに返答してもよい。ここにKは、端末Aによって解読されるだけであるかもしれないAの鍵Kにより暗号化された非対称の暗号方式のシステムデータの公開鍵であることが認識されるであろう。

【００８２】

この方法において、委任の安全で責任のある連鎖が委任トークンと対応する署名をカスケードすることにより確立することができることを見ることができる。これは連鎖のエンドポイントが連鎖における各実体によって実行される責任を追跡することを許容する。これは責任を提供し、その結果、例えば、通信が失敗し何のメッセージも端末Aから受け取られなかったことを端末Bが主張するなら、端末Bの委任トークンおよび署名が端末Cにより受け取られかつ解読されたメッセージM2にあるので、端末Cは端末Bが不正確であると立証することができる。PKIインフラストラクチャは連鎖におけるすべての端末の公開鍵を端末Cに提供し、端末Cはすべての中間的委任鍵にアクセスすることができる。しかしながら、データが連鎖上で返送されているところでは、連鎖のすぐ前の端末だけが対応する秘密鍵(または共有された秘密の鍵)を有するので、一般に隣接している(前の)端末からの鍵委任だけが連鎖上を返送されるべきデータを暗号化するために使われるかもしれない。

【００８３】

暗号よりむしろ非拒否だけが望まれているところでは、移動端末は、インフラストラクチャを簡素化するが安全のレベルを減少させる削除鍵（それはまたメッセージに署名するために作成し、それは送る）を使用するかもしれない。対称の暗号はより少ない処理パワーを必要とするけれども、対称の暗号は保全のチェックを提供するが、非拒否を提供しないことが認識されるであろう。

【００８４】

この点において、コア要素に焦点を合わせて、委任手順の概観を提供することがプロトコルを理解するのに役立つ。(プロトコルの非対称のバージョンの) 初期のメッセージM1のために、コア要素は以下を含む:

$$M1：A\rightarrow B：P_B(K_{P-T-E}\|\Gamma\|S_A(h(DT)))\qquad(式8)$$

ここに、

$$DT=K_{P-T-E}\|\Gamma$$

プロトコルの対称のバージョンでは、P_BはE_{K1}になり、$S_A(h(DT))$は$MAC_{K1}(DT)$になる。

【００８５】

(プロトコルの非対称のバージョンの) 第２のメッセージM2において、コア要素は以下を含む：

$$M2；B\rightarrow C：P_C(K_{P-T-E'}\|\Gamma'\|S_B(h(DT'))\|\Gamma\|K_{P-T-E}\|S_A(h(DT)))\qquad(式9)$$

ここに、

$$DT'=K_{P-T-E'}\|\Gamma'$$

再び、プロトコルの対称のバージョンでは、P_CはE_{K1}になり、$S_B(h(DT'))$は$MAC_{K2}(DT)$になる。

【００８６】

熟練した人は、M3:C→Dおよび、より一般にMi:i→jにこのプロトコルの拡大を容易に認識するであろう。

プロトコルの選択的ではあるが望ましい安全関連の態様が次に議論される。

タイムスタンプがフレッシュかつユニークな保証を提供し、メッセージ再生を検出するために使用されてもよく、知られた鍵攻撃に対する防御が要求され、他方技術が一方的な鍵認証プロトコルのための攻撃を再演するために潜在的に傷つきやすいときに有利である。タイムスタンプベースの技術の安全は共通の時間基準の使用に依存する。これは、ホスト時計が利用可能であるべきであり、同期が時計ドリフトを打ち返すために必要でありかつ使用される受け入れ可能な時間窓を収容するために適切でなくてはならないことを意味する。サービスの否定攻撃の危険は、寿命が短ければ短いほどリスクがより低いので、Γについて寿命を指定することにより減少することができる。

【００８７】

非対称および対称の暗号方式のアプローチの両方において、各実体は秘密に保つべきである鍵を維持するが、非対称のアプローチの公開鍵は開示される。この鍵が信用を落すならば、安全な委任プロトコルは保証することができないので、望ましくはそれぞれの移動行為者がそれ自身の鍵をしっかりと管理するように委ねられる。公開鍵システムを使用する1つの利点は信頼された秘密のサーバが必要ないことであるが、共通の対称の鍵を使用することによって、より大きい性能が達成されるかもしれない。しかしながら、DTがいつもデジタル的に署名されるので、両方の代替手段は委任の責任を提供する。非対称の鍵ベースのプロトコルにおいて、エンドポイントはK_{P-T-E}の起源を確認することができるが、例えば、データベースに格納されるかもしれない公開鍵がしっかりと保護されないならば、移動行為者のふりをする攻撃者からの潜在的リスクがまだある。対称鍵ベースのプロトコルでは、サーバはいつも信じられ、したがって危険にさらされるべきでない。プロトコルは監査しているメカニズムを提供するが、実際にはこれらは攻撃を防ぐためよりも可能な紛争を解決する証拠を提供することにより多く役に立つかもしれない。

【００８８】

上述されたプロトコルは、すべてのかかわった移動行為者の間で端から端への責任を提供することが可能であり、その結果、責任と信頼を増加させることを助ける。それらは特に、例えば、端末の操作のモードを適合させるためにソフトウェアコンポーネントまたはシステムまたはアプリケーションソフトウェアを購入するためのM-コマースアプリケーションの役に立ち、そこでは限られた量の信頼がPAN環境においてポケットPC、移動電話、およびラップトップのような移動端末間に存在するかもしれない。技術はまた将来のプログラマブル移動ユーザ装置のMExE規格に適している。プロトコルはそれぞれの端末/クライアント要求のソフトウェア、チケット、クーポン、およびm-商業関連のデータの安全なダウンロードを可能にし、それらが従来より少ないメッセージパスを有するので、(対称および非対称のバージョンの両方について)比較的効率的である。カスケードな委任プロトコルはコンパクト、効率的でありおよび再構成可能な端末によく適合する。

【００８９】

発明の実施例はサーバおよび移動通信システムの移動端末の文脈で説明されたが、発明の態様は例えば、ネットワークコンピュータシステムおよび無線システムと同様に有線システムにも他のアプリケーションを有する。上記プロトコルにおいて、一般に任意の端末またはサーバが最初のメッセージ創始者を含んでもよく、任意の端末またはサーバが連鎖のエンドポイントを形成してもよいことがまた認識されるであろう。

【００９０】

多くの効果的な代替手段が熟練した人に疑いなく思い浮かぶであろうし、発明が記述された実施例に制限されないことが理解されるが、請求の精神および範囲内で技術に熟練した者に明らかな変更を含む。

【図面の簡単な説明】

【００９１】

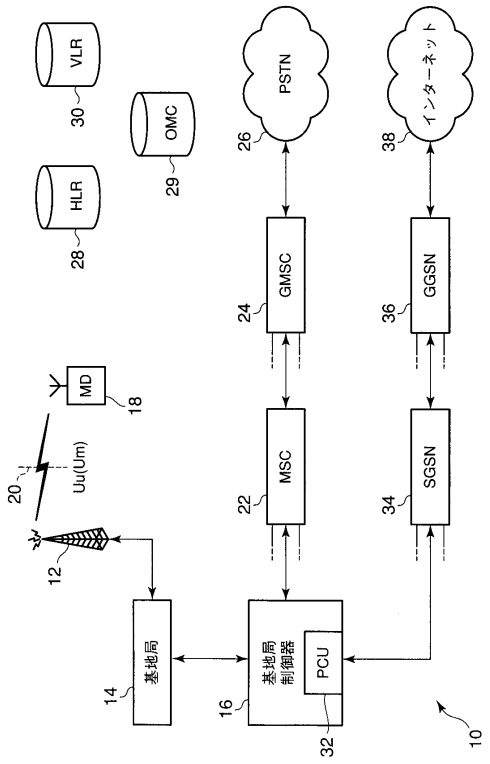
【図１】3G移動電話システムのための一般的な構造を示す。

【図２】通信ネットワークの移動端末とサーバとの安全な通信リンクの概要を示す。

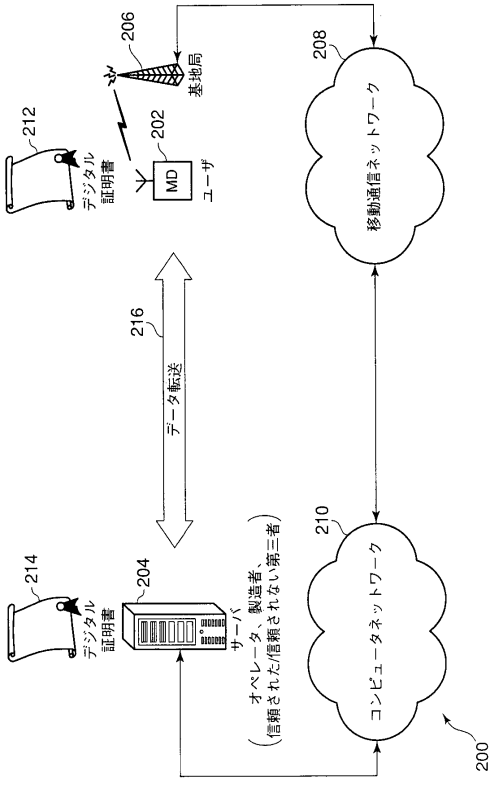
【図３】ソフトウェアデファインドラジオ(SDR；ソフトウエア無線機)ハードウェアとソフトウェア構造の例を示す。

【図４】パーソナルエリアネットワークと関連するインフラストラクチャに関する例を示す。
【図５】安全な委任プロトコルを実施するために構成されたサーバとの通信の移動実体の連鎖を示す。
【図６】本発明の実施例による方法を実施するために、図５の端末またはサーバとして使用に適したコンピュータシステムを示す。
【符号の説明】
【００９２】
４００…PAN　１０…第３世代デジタル移動電話システム　２００…基本的に安全な移動通信システム　５００…端末の連鎖　６００…コンピュータシステム

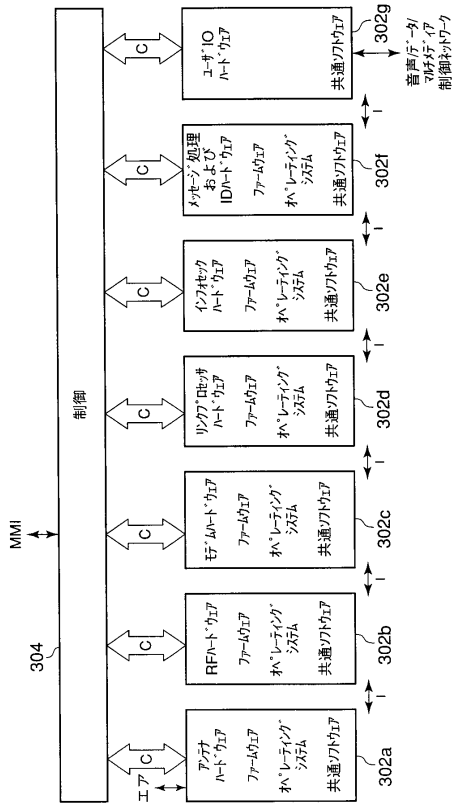
【図１】



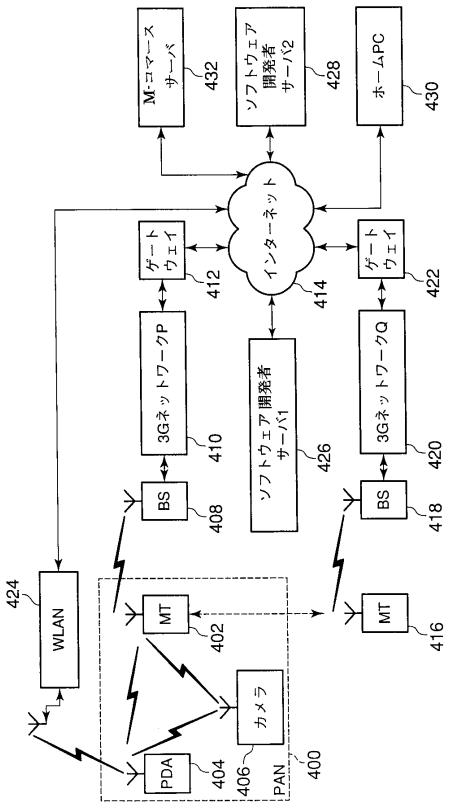
【図２】



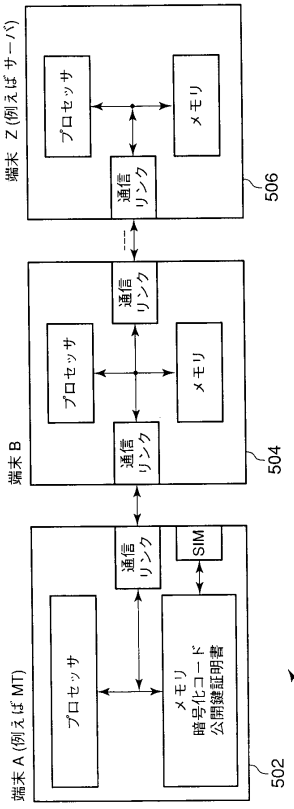
【図３】


MMI
304
制御
エア
C
アンテナ ハードウェア
ファームウェア
オペレーティング システム
共通ソフトウェア
302a
RFハードウェア
302b
モデムハードウェア
302c
リンクコロッサ ハードウェア
302d
インフォセック ハードウェア
302e
メッセージ処理 および IDハードウェア
302f
ユーザI/O ハードウェア
302g
音声データ/ マルチメディア 制御ネットワーク

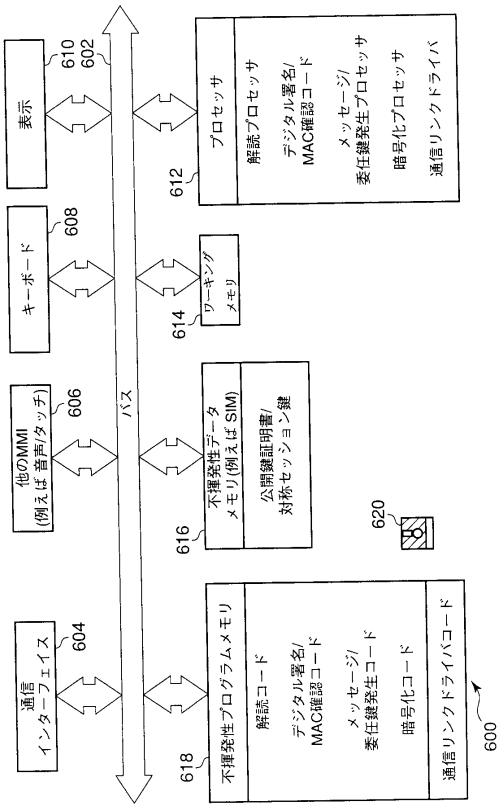
【図４】


M-コマース サーバ
432
ソフトウェア 開発者 サーバ2
428
ホームPC
430
インターネット
414
ゲートウェイ
412
ゲートウェイ
422
3Gネットワーク P
410
3Gネットワーク Q
420
BS
408
BS
418
ソフトウェア 開発者 サーバ1
426
WLAN
424
MT
402
MT
416
PDA
404
カメラ
406
PAN
400

【図５】


端末 A (例えば MT)
プロセッサ
通信 リンク
SIM
メモリ
暗号化コード
公開鍵証明書
502
500
端末 B
プロセッサ
通信 リンク
メモリ
504
端末 Z (例えば サーバ)
506

【図６】


表示
610
602
キーボード
608
他のMMI (例えば 音声/タッチ)
606
通信 インターフェイス
604
バス
プロセッサ
612
解読プロセッサ
デジタル署名/ MAC確認コード
メッセージ/ 委任鍵発生プロセッサ
暗号化プロセッサ
通信リンクドライバ
ワーキング メモリ
614
不揮発性データ メモリ(例えば SIM)
公開鍵証明書/ 対称セッション鍵
616
620
不揮発性プログラムメモリ
618
解読コード
デジタル署名/ MAC確認コード
メッセージ/ 委任鍵発生コード
暗号化コード
通信リンクドライバコード
600

フロントページの続き

(72)発明者 チャン・イエオ・イェン
イギリス国、 ビーエス１・４エヌディー、 ブリストル、 クイーンズ・スクエア ３２、 トーシバ・リサーチ・ヨーロッパ・リミテッド内
(72)発明者 ジョルジオス・カログリディス
イギリス国、 ビーエス１・４エヌディー、 ブリストル、 クイーンズ・スクエア ３２、 トーシバ・リサーチ・ヨーロッパ・リミテッド内
(72)発明者 ゲイリー・クレモ
イギリス国、 ビーエス１・４エヌディー、 ブリストル、 クイーンズ・スクエア ３２、 トーシバ・リサーチ・ヨーロッパ・リミテッド内

審査官 速水 雄太

(56)参考文献 特開平０９－３０７５４２（ＪＰ，Ａ）
特開２００１－２１１１６８（ＪＰ，Ａ）
Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, １９９６年, p. 509

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／０８