(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-180280
(P2004-180280A)
(43)公開日　平成16年6月24日(2004.6.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	H04L 9/00	675B	5J104
G06F 17/60	G06F 17/60	140	
G09C 1/00	G06F 17/60	512	
	G09C 1/00	640E	

審査請求 未請求　請求項の数 42　OL　（全 32 頁）

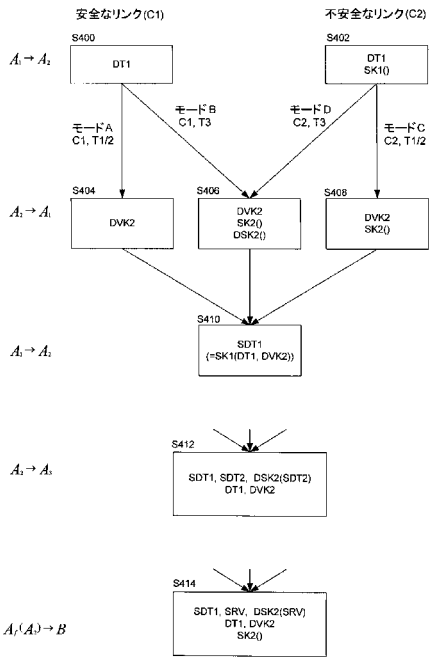
(21)出願番号　特願2003-352384(P2003-352384)
(22)出願日　平成15年10月10日(2003.10.10)
(31)優先権主張番号　0223853.3
(32)優先日　平成14年10月14日(2002.10.14)
(33)優先権主張国　英国(GB)

(71)出願人　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】適応性のある委任のための方法とシステム

(57)【要約】　（修正有）
【課題】特に信頼が委任されるところで責任の連鎖がシステムで必要であるところで、安全な委任のための方法、システムを提供する。
【解決手段】第１のデータ処理実体から第２のデータ処理実体へ委任するための委任の方法が記述され、前記第１および第２の実体は互いに双方向の通信リンクを持っている。方法は第１の実体から第２の実体へ委任トークンを送り、前記委任トークンは委任要求に関連する情報を含み；前記第１の実体で前記第２の実体からの回答を受け取り、前記回答は前記第２の実体により前記委任トークンによって示めされた委任の承認を決定する情報を含み；前記第１の実体から前記第２の実体へ前記回答に対する署名を送り、前記署名は少なくとも前記委任トークンの署名を含むことを含んでいる。
【選択図】　図５



【特許請求の範囲】
【請求項１】
第１および第２のデータ処理実体が互いに双方向の通信リンクを有し、前記第１のデータ処理実体から前記第２のデータ処理実体への委任の方法であって、
前記第１の実体から前記第２の実体へ委任トークンを送り、前記委任トークンは委任要求に関連する情報を含み、
前記第１の実体で前記第２の実体からの回答を受け取り、前記回答は前記第２の実体により前記委任トークンによって表された委任の承認を決定する情報を含み、
前記回答に応答して前記第１の実体から前記第２の実体へ署名を送り、前記署名は少なくとも前記委任トークンの署名を含むことを含む方法。
【請求項２】
前記回答が委任確認鍵を含み、前記署名が前記委任トークンと前記委任確認鍵の署名を含む請求項１で請求された方法。
【請求項３】
前記回答が前記第２の実体の署名を含み、方法はさらに前記回答に応じる前に前記第２の実体の署名を検証することを含む請求項１または２に請求された方法。
【請求項４】
前記第２の実体の署名が少なくとも前記委任トークンの署名を含む請求項３に請求された方法。
【請求項５】
前記委任確認鍵が一対の鍵の１つの鍵を含み、もう片方の鍵が委任署名鍵を含み、前記回答が前記委任署名鍵で発生された前記委任確認鍵の署名を含む、請求項２に従属するときに請求項４に請求された方法。
【請求項６】
前記第１の実体から前記第２の実体へ前記委任トークンを送ることが、さらに少なくとも前記委任トークンの第１の実体の署名を送ることを含む請求項１乃至５の何れか１項に請求された方法。
【請求項７】
前記委任トークンを送ることと前記委任トークン署名を送ることの１つまたは両方が、前記第２の実体によって確認されたタイムスタンプおよび/又はその場限りのデータを送ることを含む請求項１乃至６の何れか１項に請求された方法。
【請求項８】
前記受け取ることが前記第２の実体からタイムスタンプおよび/又はその場限りのデータを受け取ることを含み、方法はさらに前記タイムスタンプおよび/又はその場限りのデータを確認することを含み、前記委任トークン署名を送ることが前記確認への応答である、請求項１乃至７の何れか１項に請求された方法。
【請求項９】
請求項１の方法を実行し、
安全の所望のレベルを決定し、
前記決定に応答して前記送ることと受け取ることに含まれるべき任意の追加情報を選択することを含む適応性のある委任の方法。
【請求項１０】
前記追加情報が請求項１乃至８の何れか1項により要求された情報から選択される請求項９に請求された方法。
【請求項１１】
前記任意の追加情報の前記選択が、
前記第１の実体のPKI署名を含む前記委任トークンを送るための任意の追加情報;および/又は１つ以上を含む前記回答を受け取るための任意の追加情報:前記第２の実体により保持された一対の鍵の１つを含む委任確認鍵、前記第２の実体のPKI署名、および前記一対の鍵の他方により署名されるデータ、

を選択することを含む請求項９に請求された適応性のある委任の方法。
【請求項１２】
前記第１の実体から前記第２の実体へ委任する請求項１乃至８の何れか１つの方法を実行し、さらに前記第２の実体から第３のデータ処理実体へ委任することを含み、
前記第２の実体から前記第３の実体へ第２の委任トークンを送り、
前記第２の実体で前記第３の実体からの回答を受け取り、前記回答は前記第３の実体による前記委任トークンにより表された委任の承認を決定する情報を含み、
前記第３の実体からの前記回答に応答して、前記第２の実体による前記第２の委任トークンの署名、前記第１の実体からの前記委任トークン、および前記第１の実体からの前記委任トークンの署名を含む第２の実体の委任トークンの署名を前記第２の実体から前記第３の実体へ送ることによる、
安全なカスケード委任の方法。
【請求項１３】
前記第３の実体からの前記回答に応答して、前記第２の実体の委任確認鍵を前記第２の実体から前記第３の実体へ送ることをさらに含む、請求項２に従属するとき請求項１２に請求された方法。
【請求項１４】
前記第３の実体からの前記回答に応答して、前記第２の実体の委任確認鍵を使用して検証可能な前記第２の実体の委任トークン署名のための署名を、前記第２の実体から前記第３の実体へ送ることをさらに含む請求項１３に請求された方法。
【請求項１５】
第４またはさらなるデータ処理実体に委任するために拡張された請求項１２乃至１４の何れか１項に請求された方法。
【請求項１６】
各々前記第１の実体と双方向の通信にある複数の前記第２の実体に前記第１の実体から委任するため、請求項１乃至１５の何れかの請求項で請求された方法を実行することを含み、送ることと受け取ることが前記第１の実体とそれぞれの前記第２の実体の間で行われる安全な同報通信委任の方法。
【請求項１７】
第１のデータ処理実体と第２のデータ処理実体とが互いに双方向の通信リンクを有し、前記第１の実体から前記第２実体へ委任の受諾を確認する方法であって、
前記第１の実体から委任トークンを受け取り、前記委任トークンは委任要求に関連する情報を含み、
前記第１の実体のための回答を発生させ、前記回答は少なくとも一対の鍵の１つの鍵を含む委任確認鍵、委任署名鍵を含むそのもう片方の鍵を含み、前記委任署名鍵は前記第２の実体からメッセージのための署名を発生させるのに使用可能な鍵であり、前記委任確認鍵は前記署名を確認するため使用可能であり、
前記委任の受諾を確認するため前記回答を前記第１の実体に送ることを含む方法。
【請求項１８】
前記回答が前記委任署名鍵で発生された前記委任確認鍵の署名を含む請求項１７に請求された方法。
【請求項１９】
前記回答が前記第２の実体による前記委任トークンの署名を含む請求項１７または１８に請求された方法。
【請求項２０】
最終点データ処理実体から少なくとも１つの長さの委任データ処理実体の連鎖で委任データ処理実体によるサービスを要求する方法であって、方法は前記委任実体から前記最終点実体へ要求を送ることを含み、前記要求は、
前記連鎖における各委任実体から１つ、各前記委任トークンが委任要求に関連する情報を含んでいる一組の委任トークン；

前記連鎖における各委任実体から１つ、各々がそれぞれの前記委任トークンのそれぞれの委任実体署名を含んでいる一組の委任トークン署名；
サービス要求データを含む方法。
【請求項２１】
前記要求はさらに少なくとも前記サービス要求データの公開鍵インフラストラクチャ（PKI）署名を含み、方法はさらに前記最終点実体に前記要求データを送っている前記委任実体のPKI鍵対の秘密鍵で前記サービス要求データを署名することを含む、請求項２０に請求された方法。
【請求項２２】
各前記委任トークン署名が前記委任トークンおよび関連する委任トークン検証鍵の両方の署名を含み、前記要求はさらに前記連鎖における各委任実体から１つ、一組の前記委任確認鍵を含む請求項２０または２１に請求された方法。
【請求項２３】
前記委任確認鍵が一対の鍵の１つの鍵、委任署名鍵を含む他方の鍵を含み、前記要求が前記最終点に前記要求データを送っている前記委任実体と関連した委任署名鍵を使用して発生された少なくとも前記サービス要求データの署名をさらに含む、請求項２２に請求された方法。
【請求項２４】
委任プロトコルを使用して第１のデータ処理実体から第２のデータ処理実体へ委任する方法であって、前記委任プロトコルは前記第１の実体から前記第２の実体へ署名された委任トークンを送ることを含み、前記署名された委任トークンは前記第１の実体により前記第２の実体から受け取った委任トークンと鍵の署名を含む方法。
【請求項２５】
第１のデータ処理実体から第２の委任プロトコル実体へ委任する方法であって、
前記第１の実体から前記第２の実体へメッセージを送り、メッセージは少なくとも、
委任トークン；
前記委任トークンと秘密鍵との組み合わせの署名；
前記秘密鍵の暗号化されたバージョンを含む方法。
【請求項２６】
前記署名は署名されたメッセージの回復を許容し、前記委任トークンと前記暗号化された秘密鍵とは前記署名の中に提供される請求項２５に請求された方法。
【請求項２７】
前記秘密鍵が非対称の暗号方式のアルゴリズムのための秘密鍵を含む請求項２５または２６に請求された方法。
【請求項２８】
前記メッセージが非対称の暗号方式のアルゴリズムのための鍵対を含み、前記鍵対が前記秘密鍵を含んでいる請求項２７に請求された方法。
【請求項２９】
前記秘密鍵が対称の暗号方式のアルゴリズムのための共有された秘密鍵を含む請求項２５または２６に請求された方法。
【請求項３０】
さらに前記送ることの前に前記秘密鍵を発生させることを含む請求項２９に請求された方法。
【請求項３１】
前記秘密鍵が対称の暗号方式のアルゴリズムのための共有された秘密鍵を含み、前記秘密鍵の前記暗号化されたバージョンが前記第２の実体の公開鍵を使用して暗号化される請求項２５に請求された方法。
【請求項３２】
前記委任することの少なくとも１つの安全なパラメタを決定し、
前記決定の結果に応答して前記送ることの安全を増加させることをさらに含む請求項２

４乃至３１の何れか１項に請求された方法。
【請求項３３】
前記少なくとも1つの安全なパラメタが前記メッセージを送ることのために採用された通信媒体の安全のレベルを示すパラメタを含む請求項３２に請求された方法。
【請求項３４】
前記少なくとも1つの安全なパラメタが前記第２の実体の信頼できることのレベルを示すパラメタを含む請求項３２または３３に請求された方法。
【請求項３５】
前記決定することが自動的に実行される請求項３２乃至３４の何れか１項に請求された方法。
【請求項３６】
実行するとき、請求項１乃至３５の何れか１項による方法を実施するためのプロセッサ制御コード。
【請求項３７】
請求項３６のコードを担持する担体。
【請求項３８】
請求項１乃至１１および１７乃至３５の何れか１項に請求された方法を実施するために構成されたデータ処理実体。
【請求項３９】
請求項１２乃至１６の何れか１項の方法を実施するために構成されたデータ処理システム。
【請求項４０】
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；
プロセッサ実行可能な指示を格納する指示メモリ；
データメモリおよび指示メモリに結合され、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を含み、指示は、
委任トークンを前記第２のプロセッサに送り、前記委任トークンは委任要求に関連する情報を含み、
前記第２のプロセッサから回答を受け取り、前記回答は前記第２のプロセッサによる前記委任トークンにより表された委任の受諾を決定する情報を含み、
前記回答に応答して前記第２のプロセッサに署名を送り、前記署名は少なくとも前記委任トークンの署名を含む、プロセッサを制御するための指示を含む、
第２のデータプロセッサに委任するために構成されたデータ処理装置。
【請求項４１】
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；
プロセッサ実行可能な指示を格納する指示メモリ；
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するプロセッサとを含み、指示は、
前記委任しているプロセッサから委任トークンを受け取り、前記委任トークンは委任要求に関連する情報を含み、
前記委任しているプロセッサのための回答を発生させ、前記回答は一対の鍵の１つの鍵を含む少なくとも委任確認鍵、委任署名鍵を含むそのもう片方の鍵を含み、前記委任署名鍵はデータ処理装置からメッセージのための署名を発生させるために使用可能な鍵であり、前記委任確認鍵は前記署名を検証するために使用可能であり、
前記委任の受諾を確認するために前記回答を委任しているプロセッサへ送るようにプロセッサを制御するための指示を含み、
委任しているデータプロセッサから委任を受け入れるために構成されたデータ処理装置。
【請求項４２】
連鎖が少なくとも１つの長さを有し、委任データプロセッサの連鎖にあるとき、最終点データプロセッサからサービスを要求するように構成されたデータプロセッサであって、

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；
プロセッサ実行可能な指示を格納する指示メモリ；
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を含み、指示が前記最終点プロセッサへ要求を送るためにプロセッサを制御するための指示を含み、前記要求は、
各前記委任トークンが委任要求に関連する情報を含んでいる、前記連鎖における各委任プロセッサから１つの一組の委任トークン；
各々がそれぞれの前記委任トークンのそれぞれの委任実体署名を含んでいる、前記連鎖における各委任プロセッサから１つの一組の委任トークン署名；および
サービス要求データを含むデータプロセッサ。

【発明の詳細な説明】
【技術分野】
【０００１】
この発明は一般に適応性のある、しかし安全な委任のための方法、システムおよびコンピュータプログラムコードに関連する。発明は信頼が委任されるシステムで責任の連鎖が必要であるところで有用である。
【背景技術】
【０００２】
発明に関する背景と文脈を理解する際に、簡潔に委任のいくつかの例について議論するのは役に立つ。概して委任は、第２のシステムまたはオブジェクトが第１を代理してタスクを実行することができるように、１つのデータ処理システムまたはオブジェクトから第２への権威の委任について言及する。一般に、委任された権威は、例えばある他のプログラムが動作を実行することを許容するようにデータまたはメッセージを含むかもしれない委任トークン、またはさらに或は代わりに、分散システムまたは別のマシンの他の部分で実行するように意図されたプログラム(すなわち、いわゆる移動行為（mobile agent）MA)をそれ自体含む委任トークンの形で通過される。このようにして、事実上、委任トークンは一般にトークンのユーザによって定義された一組のデータおよび/又は指示を含む。
【０００３】
M-商業の例を取ると、委任トークンは、例えばベンダーのリストのように、ソフトウェアが配送の期限および/又は価格束縛から購入されるかもしれない幾つかの束縛、およびモデルまたはバージョンの範囲が入手でき、データ指定受入れ可能なモデルまたはバージョンである状態で、特定のコンピュータゲームが付加的または代わりに購入されることを可能にするプログラムを含むかもしれない。通常、委任トークンはまた、ゲームを購入する認可が切れるときを決定するために満期を含むだろう。1つのシナリオにおいて、このような委任トークンの形における権威は、移動電話受話器などのユーザの移動端末(MT)からプログラムへ委任されるかもしれず、この場合、ユーザのホームＰＣ端末で“静的な”行為の居住者として知られている。このシナリオでは、委任トークンはトークンが購買プログラムそれ自体を含む必要がない購買のときに束縛を特定しているホームにメッセージを含む。
【０００４】
別のシナリオにおいて、委任トークンは移動行為として作動するソフトウェア購買プログラムを含み、このプログラム(トークン)はそれがコンピュータゲームを購入するために遠隔で実行するホームＰＣに通される。移動端末の場合では、移動端末はこのプログラムを作成し、例えば、受話器製造者かネットワークオペレータという信頼されるサーバからそれをダウンロードするかもしれない。プログラムが信頼されることができることを示す適切な情報がプログラムを実行させるなら、提供されるときプログラムは静的なプラットホームを必要とせず、さまざまなマシンでホストされることができる。したがって、委任トークンは遠隔マシン上で実行のためのプログラムを含んでもよい。議論するシナリオでは、サービス(購入されたコンピュータゲームソフトウェア)は端末またはホームＰＣ(委任トークンが配送情報を含むかもしれない)の何れかに提供されるかもしれない。また、

このシナリオでは、ユーザは、ホームＰＣがユーザの自己の移動端末から委任トークン(移動行為)をいつも信頼すべきであると決めるかもしれないが、他のシナリオでは、移動行為を実行させる前に高度の信頼が必要であるかもしれないと認識されるだろう。

【０００５】

一般に委任ベースの技術は、ソフトウェアチケット、クーポン、および例えば音楽およびMPEG映画クリップのような流されたメディアデータのような他のデータへのアクセスを容易にする。

別の例において、移動端末はドキュメントを蓄えるために追加メモリ格納スペースのための要求を持つかもしれない。分配されたファイル格納はローカルなサーバを通して有効であるかもしれず、したがって、移動端末は、例えばサーバベースの格納に使用されていないファイルを一時動かすことにより、分散環境におけるリソースを平均するために委任トークンを作成することによって、要求を処理するかもしれない。委任トークンはファイルのための費用束縛、安全要求およびアクセス方針と共に、サーバベースの格納にファイルを保存するという要求を含むかもしれない。代わりに、委任トークンは、いくつかの型のデータまたはファイルを格納する権威が委任される移動行為を含むかもしれない。どちらの場合でも委任トークンはそれを受け入れるかどうかを選ぶことができるサーバに通される。しかしながら、サーバが受け入れるならば、委任トークン責任は格納されるためにデータを管理するサーバに渡されるべきであり、望ましくは、サーバが委任トークンを受け入れたと立証するいくつかの手段があるべきである。サーバは時々要求自体を満たすことができないが、別のサーバにその要求(または、別の要求)を伝えるかもしれず、その結果、委任の連鎖を創設する。

【０００６】

第３の例を取るために、移動端末のオペレーティングシステムソフトウェアなどのアップグレードソフトウェアへの必要性または要望があるかもしれない。この場合、委任トークンは必要なソフトウェア、移動端末の任意の必要な細部を含んでいてかつ端末への新しいコードの配送を要求している委任トークンを提供するためにサーバに要求を含むかもしれない。しかしながら、このシナリオは以前に議論したそれらと比べて比較的簡単であり、例えば、委任の連鎖がより通常の安全なダウンロード技術を必要としない限り、委任ベースの技術に望ましいかもしれない。

【０００７】

委任ベースの技術は潜在的に非常に強力であるが、この安全と責任のために重要であることが認識されるだろう。例えば、悪意のハッカーが委任トークンの移動行為に代わってそこにそれら自身のソフトウェアを代入することができることが、財政的かつデータ安全の重要な含みであることができる。

【０００８】

以下の記述において、主として移動装置と無線のネットワークが参照されるが、熟練した人は説明されるべき技術がそのようなシステムに制限されないで、例えば有線のコンピュータネットワーク、より一般的には分配された、またはオブジェクト指向のコンピューティングシステムで採用されることを認識するだろう。

【０００９】

無線のネットワークに関するいくつかの例の運転は現在、いくつかの暗号方式技術と共に見直されるだろう。

パーソナル領域のネットワーク（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。セルラーラジオ、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)と物理的な層(PHY)の仕様”1999）のような技術が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、および非拒絶などの特性に必要とされる。

【００１０】
ポケットPC、移動電話、およびPAN(パーソナル領域ネットワーク)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り、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。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、および虫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/アップグレードを安全にする安全な移動委任を潜在的に採用することができる。
【００１１】
パーソナル領域ネットワーク(PAN)の概念は、IrDA、ブルートゥースおよび/又はWLAN技術(例えば、IEEE 802.11)などの技術を使用している装置間のローカル(すなわち、個人的な)通信を熟考する。いくつかのPANが認可権威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支持し、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。
【００１２】
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、証明書権威の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。
【００１３】
図１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。PAN100は示された例において、互いとの無線(rf)の通信にある移動端末102、PDA104、およびカメラ106を含む。移動端末102はまたインターネット114へのゲートウェイ112を有する第１の3G移動電話ネットワーク110の基地局108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116がインターネット114への第２のゲートウェイ122で第２の3G移動電話ネットワーク120の第２の基地局118と通信にある。PDA104はまたインターネット114と結合されるIEEE 802.11 WLANなどのようなWLAN 124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126、128、ホームPC130および１つ以上のM-商業サーバ132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102と116には、破線134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。

【００１４】

移動端末102のユーザの文脈における委任の使用の簡単な例では、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102は電話ネットワーク110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102のユーザは新しい映画(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110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120はこのサービスを提供し、したがって、ユーザは必要なら最初にネットワーク120からそれを得る移動端末116のユーザから映画クリップを入手することができる。

【００１５】

次に、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。

【００１６】

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。

【００１７】

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。一方向性で衝突回避性のある（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 Requ

est for Comments 1321、April 1992に与えられる。

【００１８】

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することで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、非拒絶を保証しない。

【００１９】

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。サーティフィケーションオーソリテイ（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。

【００２０】

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。

【００２１】

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 signat

ures 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証明権威に関する情報)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。

【００２２】

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、非拒絶(データの発信または受信を立証する)を提供しない。

【００２３】

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2.5Gと3G(第三世代)ネットワークなどの移動電話ネットワーク内ではデータ伝送も重要であり、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。

【００２４】

図２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２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Un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。

【００２５】

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。

【００２６】

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との間の回路切り換え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、回路切り換え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。

【００２７】

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。

【００２８】

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。

【００２９】

図３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３で示されない)を通して送られる。

【００３０】

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、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。

【００３１】

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 t23.057“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かめることができる。

【００３２】

再構成可能な、ソフトウェアデファインドラジオ(SDR)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。

【００３３】

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４に示す。図４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４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。

【００３４】

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。

【００３５】

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/又は生物測定技術で、データ創始者または受け手の)、アクセス制御、非拒絶、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)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移送され、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。

【００３６】

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B.Crispo、“Delegatio

n 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。

【００３７】

他の背景情報はM.Abadi、C. Kaufman、and B.Lampson、“Authentication and delegation with smart-cards”、Science of Computer Programming 、21:91-113、October 1993; M.Abadi、 M. Burrows、B.Lampson and G.Plotkin、“A calculus for Access Control in Distributed Systems”、ACM Transactions on Programming Languages and Systems、Vol. 15、No４、Pages 706-734、September 1993; M.Gasser、A.Goldstein、C. Kaufman、and B.Lampson、“The digital distributed system security architecture”、Proceedings of the National Computer Security Conference、1989; K.R.Sollins、“Cascaded authentication”In Proceedings of the 1988 IEEE Symposium on Security and Privacy、pages156-163、April 1988;およびV.Varadharajan、P.Allen.and S.Black、“An analysis of the proxy problem in distributed systems”、In IEEE Symposium on Security and Privacy、pages255-277 1991に見出すことができる。

【発明の開示】

【発明が解決しようとする課題】

【００３８】

これらの文献に記述された委任プロトコルは以下の1つ以上を含むさまざまな欠点に悩まされる: 高いコンピュータの費用および/又はネットワーク帯域幅とリソースのための高い要求；専門化された委任センターのような特別なインフラストラクチャを求める要求；委任の責任の不足; さまざまのネットワークにおける使用のための不適当; 適応性; 同報通信委任の支持の不足。例えば、委任パスポートを提案するSollinsは、すべての実体が認証トークンを管理するために登録されなければならないことを信頼された静的なサーバに要求し、ところがCrispoは、特に移動装置即ち端末における実施が熟考されるところでコンピュータ資源に望ましくない高い要求を置く。

【００３９】

発明者の以前の英国特許出願番号0220203.4(“Methods and apparatus for secure data communication links” 2002年8月30日出願)、およびSDRフォーラム2002年11月に明らかにした関連した論文、C.Y.Yeun、G.Kalogridis、and G.Clemo、“Secure Methods Delegation for Future Reconfigurable Terminals and Applications”はこれらの短所のいくつかを処理するが、それにもかかわらず委任トークンを同報通信するその性能において制限される。例えば、同報通信は、すべてが要求を受け入れるとは限らないが、それが多くの異なった実体に実質的に同じ要求を送ることを必要とするときに役に立つ。次を試みる前に応答を待っている各実体に要求が順次されるならば、委任の処理はかなり遅くされるかもしれない。その上、再構成可能な端末とPANアプリケーションに適しているが、他の委任シナリオでは、利点の異なったプロフィールが好まれるかもしれない。

【００４０】

例えば、装置のハードウェアを再構成するために、PANアプリケーションおよび敏感な個人的なファイルの同期などの他のアプリケーション、移動商業、遠隔コンピューティング、およびラジオレベルソフトウェアモジュールのオンラインアップグレードを含んでいる委任のための潜在的アプリケーションの過剰がある。また、インターネットベースのネットワーク(インターネット、イントラネット、およびエクストラネットなど)、セルラー通信ネットワーク、他のホームおよびオフィスの有線および無線のネットワーク(IEEE 802.15とHiperlan/2など)を含む多くの種類のネットワークがある。これらにはさまざまなサービスと安全な要求を有し、順次他のパラメタに影響を与える。例えば権限消費とバッテリー生命はCPUデータ処理要求に関連され、その結果、暗号方式の負荷に関連する。しかしながら、概して、現在の安全な委任の技術は特定のシステムおよび/又はネットワーク、あるいは丈夫さ不足および/又はコンピュータの効率の何れかに制限される。例えば、軽量であるならばそれらは責任と認証の明快を欠くか、またはそれらが発行と維持のた

めの中央の委任権威あるいは委任トークンおよび/又は委任鍵のような特定のインフラストラクチャに依存するかの何れかである。特定のインフラストラクチャに依存しないものは重いコンピュータの処理負荷を課し、および/又は長くて複雑なメッセージ交換を必要とする。強健な安全な特徴と妥当な性能を持っているいくつかのプロトコルがあるが、これらはまだ適応性を欠いていて、一般に、多くのアプリケーションでサブ最適である。

【００４１】

したがって、サービスの範囲と動作環境に適した効率的で、強健で適応性のある委任プロトコルの必要がある。

【課題を解決するための手段】

【００４２】

したがって、発明の第１の態様によると、第１のデータ処理実体から第２のデータ処理実体への委任の方法が提供され、前記第１および第２の実体は互いに双方向の通信リンクを有し、方法は第１の実体から第２の実体へ委任トークンを送り、前記委任トークンは委任要求に関連する情報を含み；前記第１の実体で前記第２の実体からの回答を受け取り、前記回答は前記第２の実体により前記委任トークンによって示めされた委任の承認を決定する情報を含み；前記第１の実体から前記第２の実体へ前記回答に対する署名を送り、前記署名は少なくとも前記委任トークンの署名を含むことを含んでいる。

【００４３】

３つのメッセージ交換プロトコルと署名された委任トークンの使用は、同報通信委任を容易にし、実施例で安全と権限消費およびネットワークトラヒック要求のような他の要求にしたがって、それが動的に適合させることができるように適応性がある。プロトコルの実施例はまた、責任と認証を提供する。プロトコルの適合は、後で説明されように、例えば、動作の特定のモードの検出または要求に応答して自動的に成されることができる。

【００４４】

プロトコルの実施例は、移動商業およびインターネットサービス関連アプリケーション、およびパーソナル領域ネットワークを含んでいる（しかし、限定されない）アプリケーションの範囲とネットワーク環境とに両立性がある。したがって、前記第1または第2の実体は移動端末またはサーバのようなデータプロセッサ、またはある他の分散コンピューティング環境においてはコンピュータプログラムコードオブジェクトを含むかもしれない。同様に通信リンクはネットワークの一部のような有線または無線のリンクを含み、または例えば、コンピュータプログラムコードオブジェクトのようなある他のリンクを含むかもしれない。委任トークンは要求データ、またはプログラムコード、あるいは両方のようなデータを含むかもしれない。望ましくは、第１の実体からの署名は、これがなんらかのこれ以上のインフラストラクチャの必要性を避けるように対応する公開鍵で証明可能なPKI署名である。

【００４５】

第２の実体からの回答は単純な受信通知、または“私は委任を受け入れる”のようなメッセージを含むかもしれず、その場合メッセージは第２の実体によって署名され、再び、望ましくはPKI署名を使用する。署名されるならば、第１の実体が委任トークンを第２の実体に送る前に署名は確認されることができる。付加的にまたは代わりに、回答は委任確認鍵を含むかもしれず、署名はこの鍵と委任トークンの署名を含むかもしれない。概してどんな型の署名も前述のRSA署名のように採用されるかもしれない。

【００４６】

望ましくは、委任確認鍵は第２の(委任)実体によって作成された(または、少なくとも検索された)および管理された一対の１つであり、委任署名鍵と呼ばれるかもしれない一対の他の鍵は望ましくは、第２の実体によって秘密に保たれる。したがって鍵のこの対は望ましくは、仲間対仲間ベースで管理される。これは委任権威サービスの必要性なしに強健な責任を容易にする。鍵の対は対称の暗号のために鍵を含むかもしれないが、望ましくは、向上した安全のために鍵は非対称の暗号方式の処理のためのものである。

【００４７】

方法の実施例では、初期の委任要求(トークンが送られるとき)と回答のコンテンツは、通信リンク(または、ネットワーク)の安全と第２の実体の信頼できることに依存して変更されるかもしれない。例えば、ネットワークが比較的安全であり、第２の実体が信頼されているところでは、回答は第２の実体によって署名される必要はない。リンクがより安全でないところでは、第１の実体が署名、例えば、委任トークンの署名で委任トークンを送ることが望ましく、第２の実体の回答が第２の実体の署名を含んでいることがさらに望ましい。望ましくは、これらの署名の両方がPKI署名である。

【００４８】

第２の実体が信頼できない即ち非信頼なら、回答はまた、(秘密)の委任署名鍵を使用して発生された第２の実体からの署名を含むかもしれない。例えば、この鍵は、委任確認鍵に署名するために使用されるかもしれない。

委任確認鍵が採用されているすべての場合では、この鍵が第１の実体の署名におけるトークンと共に、例えば、署名された委任トークンで束縛されることは望ましい。このように、第１の実体が委任要求のための責任を保つことができ、委任確認鍵が委任署名鍵にリンクされるので、第２の実体はまたこの責任の中に含まれる(同じ公開鍵から2つの異なった秘密鍵を作成することは困難であるので)。

【００４９】

送られかつ受け取られるメッセージの幾つかまたはすべてが、回答の攻撃を妨げるためにタイムスタンプおよび/又はノンス(その場限りの)データを含むことがさらに望ましい。一般に、時計ベースのタイムスタンプは少なくとも実質的に同期された時計を実体に必要とし、ノンスはこれが利用可能でないときに好ましいかもしれない。そのようなノンスは、例えば、ファイルから読まれるか、決定論的疑似乱数発生器に(例えば擬似乱数の同期したシリーズを発生するため)より発生され、または決定論的疑似乱数発生器のためのシードとして使用されるかもしれない。付加的な安全/信頼のため、メッセージ送り手のアイデンティティはメッセージに、および任意にメッセージ署名に含まれるかもしれないが、これはより重要ではない。

【００５０】

認識されることができるように、プロトコルは適応性であり、安全の決定されたレベルにしたがって適合させられるかもしれない。例えば、移動端末はユーザのホームＰＣを認識するため、それが信じられると考えるようにプログラムされるかもしれない。ＰＣへの短距離のまたは、暗号化された無線のリンク(ブルートゥース（商標）のような)があるなら、リンクは安全であると考えられるかもしれない。同様に、端末は製造者によって制御された信頼された特定のサーバに製造者によって予めプログラムされたかもしれない。また他のシナリオでは、端末はリンクおよび/又は委任を信頼するかどうかをユーザに尋ねるかもしれない。この方法において、安全の費用は、攻撃のある型がありそうもないときに、例えば、処理パワー/バッテリーの寿命に関して自動的に削減されるかもしれない。これは順次に改良された効率と、多くの場合減少されたリンクまたはネットワークトラヒックを導く。

【００５１】

プロトコルに含まれるかもしれない任意の特徴のいくつかは以下の通りである：第１の実体から送られた委任トークンと共に第１の実体の(PKI)署名がある；および回答とともに、第２の実体の委任確認鍵および/又は(PKI)署名および/又は委任署名鍵を使用して発生された署名がある。端末または他のデータ処理システムで実施される方法の実施例において、端末(またはシステム)はこれらのすべての任意の特徴からよりもむしろサブセットから選択するかもしれない。

【００５２】

上述の委任方法は第２から第３の実体へ、この第３から第４の実体へというように委任することを容易に広げられるかもしれない。この方法において、委任はカスケードにされるかもしれない。プロトコルの異なったバージョンは異なった委任で採用されるかもしれず、その結果例えば、プロトコルのより容易なバージョンは移動端末からの委任のために

採用され、その後の委任のためのより強健で安全なバージョンは、安全のコンピュータの費用がオーバーヘッド以下を表すかもしれない、たとえばサーバからの委任のために採用される。同報通信委任は多くの第２の前記実体へ委任トークンを送るために第１の実体のために配列により実施されるかもしれない。また、必要ならこの同報通信委任はカスケードされるかもしれない。

【００５３】

また、発明は第２の実体が委任要求を受け入れる方法を提供した。

したがって、別の態様において、発明は第１のデータ処理実体から第２のデータ処理実体へ委任の受入れを確認する方法を提供し、前記第１および第２の実体は互いに双方向の通信リンクを持っており、方法は前記第１の実体から委任トークンを受け、前記委任トークンは委任要求に関連する情報を含み、前記第１の実体のための回答を発生し、前記回答は一対の鍵の１つの鍵、委任署名鍵を含む他の鍵を含む少なくとも委任確認鍵を含み、前記委任署名鍵は前記第２の実体からのメッセージのための署名を発生するために使用可能な鍵であり、前記委任確認鍵は前記署名を確認するために使用可能であり、前記回答を前記委任の受入れを確かめるために前記第１の実体に送ることを含む。

【００５４】

以前に言及したように、委任確認および委任署名鍵は、望ましくは、例えば、第２の実体にアクセス可能な以前に作成されたファイルから鍵を読むか、鍵を発生させることによって第２の実体によって生成される。大きい素数をそれぞれ含む一対の鍵が、例えばL.Blum、M.Blum、およびM.Shub、“A simple unpredictacle random number generator”SIAM Jounal on Computing、Vol.15 pp 364-383、1986およびW.Alexi、B.Chor、O.Goldreich、およびC.P.Schnorr、“RSA and Rabin Functions:Certain parts are as hard as the whol”、SIAM Jounal on Computing、Vol.17 pp 194-209、1988に記述されたBlum Blum Shub-型ジェネレータを使用して発生されるかもしれず、それへの言及がなされるかもしれない。

【００５５】

回答に対応して、第１の実体は署名された委任トークンを第２の実体に送るかもしれず、署名された委任トークンは委任トークンと、選択的に第２の実体から第１の実体に送られた委任確認鍵を含むデータの署名である。第２の実体から第３の実体へカスケード委任のとき、第２の３方向メッセージ交換処理が第２の委任トークンおよび関連づけられた第２の委任トークン署名(第２の署名された委任トークン)をもたらし、それは責任の連鎖を創設するために第１の実体からの委任トークンおよび署名(署名された委任トークン)と共に第３の実体に渡されるかもしれない。

【００５６】

第２の実体の委任確認鍵が第２の実体によって署名されたデータに含まれていたなら、この鍵はまた署名の検証を許容するため第３の実体に渡される。委任がカスケードされるところでは、前の各実体の連鎖における委任検証鍵は同様の理由で次の実体に通過されるデータに含まれるべきである。(しかしながら、第１の実体が委任確認鍵を作成する必要がないことが注意されるだろう)。

【００５７】

連鎖の端で、最後の委任はサービスを要求するために委任最終点に連絡する(そのような連鎖が1つの実体の長さに持っているかもしれないカスケードされた委任でなくても)。

したがって、発明の更なる態様によると、最終点データ処理実体から少なくとも1つの長さの実体を処理する委任データの連鎖における委任データ処理実体により、サービスを要求する方法が提供され、方法は前記委任実体から前記最終点実体へ要求を送ることを含み、前記要求は前記連鎖におけるそれぞれの委任実体からの１つの一組の委任トークンを含み、各前記委任トークンは委任要求に関連する情報、それぞれの前記委任トークンのそれぞれの委任実体署名を各々が含む前記連鎖におけるそれぞれの委任実体からの１つの一組の委任トークン署名、およびサービス要求データを含む。

【００５８】

サービス要求データは連鎖の開始点またはある他の実体へサービスを提供することを要求するかもしれない。概して最終点実体は、実施される対応する組みの委任確認鍵と選択的に連鎖における実体の一組の識別子とともに、連鎖における実体のための一組の委任トークンと対応する署名(署名された委任トークン)を受ける。任意に、サービス要求データは最後の委任実体の委任署名鍵を使用して、および/又は最後の委任のPKI鍵を使用して署名されるかもしれない。

【００５９】

他の態様では、発明は委任プロトコルを使用して第１のデータ処理実体から第２のデータ処理実体へ委任する方法を提供し、前記委任プロトコルは前記第１から前記第２の実体へ署名された委任トークンを送ることを含み、前記署名された委任トークンは委任トークンの署名および前記第１の実体によって前記第２の実体から受けた鍵の署名を含む。

【００６０】

上で説明されたプロトコルは、概して署名された委任トークンが委任実体から委任者に送られることを含む第３のメッセージだけのように簡素化されるかもしれない。

したがって、更なる態様では、発明は第１のデータ処理実体から第２の委任プロトコル実体への委任の方法を提供し、方法は前記第１から前記第２の実体へメッセージを送ることを含み、メッセージは少なくとも委任トークン、前記委任トークンと秘密鍵の組み合わせの署名、および前記秘密鍵の暗号化されたバージョンを含む。

【００６１】

プロトコルのこの変形では、秘密鍵は潜在的に悪意がある第三者などのような鍵を知ることが許されない他の実体から秘密に保たれる。秘密鍵が対称の暗号方式のアルゴリズムの鍵を含むかもしれず、その場合、鍵は第１と第２の実体の両方に共通であり、第１の実体によって第２の実体と共有される。代わりに、秘密（secret）鍵は秘密(private)鍵、または望ましくは非対称の暗号方式の公開－秘密鍵対を含むかもしれない。

【００６２】

委任トークンおよび暗号化された秘密鍵はメッセージ回復を可能にする署名アルゴリズムを採用することにより署名の中で提供されるかもしれす、または署名はメッセージ回復を可能にしないで発生されるかもしれず、その場合秘密鍵は、例えば、公開実体の公開鍵を使用して別々に暗号化される。いったん第２の実体が秘密鍵を持つと、これは生成物の活性化のように、委任トークンに関連する暗号またはある他の機能に使用されるかもしれない。このような生成物は、例えばソフトウェアが負荷される、および/又は退避される、および/又は通信される、および/又は実行されることを可能にする活性化鍵を必要とするソフトウェアを含むかもしれない。

【００６３】

上で説明されたプロトコルと方法は適応性であり、実施例で変えられるかもしれなくて、それは知覚された安全な要求に従って、動作の多くのモードの選択された１つで作動される。従って、例えば、委任している実体および委任実体間の通信リンクの安全の知覚されたレベルを分類するパラメタ、および/又は第２の実体の信頼できることのレベルを分類するパラメタのような、１つ以上の決定された安全なパラメタにしたがって、方法またはプロトコルは変えられるかもしれない。そのような安全なパラメタはユーザとの相互作用で決定されるかもしれないが、望ましくは、例えば、ユーザ入力構成データ、不履行設定、予めプログラムされたデータ(製造者かシステム/ネットワーク管理者によって予めプログラムされたデータなど)、および/又はPKI証明書データのような他のデータに基づいて、分類が自動的に作られる。安全の決定されたレベルに応答して、プロトコルは変えられるかもしれず、例えば、上で説明されたプロトコルにおいて、委任トークン、署名、および暗号化された鍵は付加的なメッセージを送るか交換することにより、および/又は付加的な署名か鍵データを含むことにより送ることの安全を増加させることによって送られる。

【００６４】

発明はまた、上で説明された方法/プロトコルを実行するため、構成されまたはプログ

ラムされたデータ処理実体/システムを提供する。
したがって、さらなる態様において、発明は委任のために第２のデータプロセッサに構成されたデータ処理装置を提供し、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、指示にしたがってデータを処理することができるプロセッサとを含み、指示は委任トークンを前記第２のプロセッサに送るためにプロセッサを制御する指示を含み、前記委任トークンは委任要求に関連する情報を含み、前記プロセッサは前記第２のプロセッサからの回答を受け取り、前記回答は前記第２のプロセッサによって前記委任トークンにより表された委任の承認を決定する情報を含み、前記プロセッサは前記回答に応答して署名を送り、前記署名は少なくとも前記委任トークンの署名を含む。

【００６５】
発明はさらに委任データプロセッサから委任を受け入れるために構成されたデータ処理装置を提供し、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、指示にしたがってデータを処理することができるプロセッサとを含み、指示は委任トークンを前記委任プロセッサから受けるためにプロセッサを制御する指示を含み、前記委任トークンは委任要求に関連する情報を含み、前記プロセッサは前記委任プロセッサのための回答を発生し、前記回答は一対の鍵の１つの鍵を含む少なくとも委任確認鍵、委任署名鍵を含む他の鍵を含み、前記委任署名鍵はデータ処理装置からメッセージのための署名を発生するために使用可能な鍵であり、前記委任確認鍵は前記署名を確認するため使用可能であり、前記プロセッサは前記委任の受入れを承認するため前記委任プロセッサに前記回答を送る。

【００６６】
発明はさらに委任データプロセッサの連鎖のとき最終点データプロセッサからサービスを要求するために構成されるデータプロセッサを提供し、連鎖は少なくとも1つの長さを有し、データプロセッサ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、プロセッサが実行可能な指示を格納する指示メモリを含み、プロセッサはデータメモリおよび指示メモリに結合されて指示にしたがってデータを処理するように作動可能であり、指示は要求を前記最終点プロセッサに送るためプロセッサを制御する指示を含み、前記要求は前記連鎖の各委任プロセッサから１つの一組の委任トークンを含み、各前記委任トークンは委任要求に関する情報、それぞれ前記委任トークンのそれぞれの委任実体署名を各々が含んでいる前記連鎖の各委任プロセッサから１つの一組の委任トークン署名、およびサービス要求データを含む。

【００６７】
記述された方法の実施例は移動端末または装置、サーバまたは他のコンピューティング装置で実行されるかもしれない。いくつかの実施では、ハードウェアとソフトウェアの組み合わせが採用され、例えば暗号方式の機能が特殊化されたハードウェアアクセラレータによって提供されるかもしれない。いくつかの実施はゲートアレイおよび/又はASICなどのハードウェアに完全に依存するかもしれない。

【００６８】
さらなる態様において、発明は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。このコードはハード即ちフロッピーディスク、CD-またはDVD-ROM、あるいは読み出し専用メモリまたはフラッシュメモリなどのプログラムされたメモリのような担体に格納されるかもしれない。コードはまた、光学的または電気的信号担体に設けられるかもしれない。以前に言及されるように、発明は純粋にソフトウェア、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で実施されてもよい。記述された方法の部分は単一の処理要素で実行される必要はなく、例えば、ネットワークで繋がれたプロセッサのような多くの要素の中に分配することができる。

【発明を実施するための最良の形態】

【００６９】
発明は添付図面を参照して例示のみの方法でさらに説明される。
初めに、プロトコルの好ましい実施例を説明する際に使われる記法を確立することが役に立つ。
無線ネットワークのような配分システムを考慮する。このネットワークの中の実体は大文字で指示される：委任はA_iによって指示され、ここにiは委任の連鎖における実体を表し、最初の主(委任)はA_1で指示され、最終的な処理を実行する主は文字Bで指示される。A_1とBの間に、A_1から委任を受ける少なくとも1つの実体、A_2がいつもある。委任者A_2は適切であるならば、A_3などにさらにいくつかの委任権利を譲渡するかもしれない。この連鎖、即ちカスケードの終わりで、最終的な委任実体A_fがBに連絡して委任権利を行使する。主が別の主に委任するとき、それは委任トークンを形成し、A_iがA_{i+1}に与える委任トークンはDT_iとして表される。
【００７０】
公開鍵インフラストラクチャ(PKI)は製造者、オペレータ、第三者および政府の規制者のような一団が証明書で提供される中で想定される。特に我々は、全ての実体が同じPKIの部分であり、結果としてそれぞれの実体の公開鍵が知られているか、または対応する秘密鍵が認証、検証、および責任のために使用することができるように各々他の実体にアクセス可能であると仮定する。例えば、移動端末の証明書、および任意に他の証明書は例えば、端末の中の改変耐性のあるハードウェアモジュールにダウンロードおよび/又は格納されるかもしれない。委任者A_iは、公開鍵インフラストラクチャ(PKI)の一部であるそれぞれ署名鍵、および検証鍵と呼ばれるSK_iおよびVK_iで表された鍵対を有する。
【００７１】
次に、我々は委任署名鍵と委任確認鍵としてそれぞれDSK_iとDVK_iを指示する。これはA_iが委任目的に使用するもうひとつの非対称の鍵対である。この鍵対はA_iによって作成されて、維持されるが、A_{i-1}は受け取られたDT_{i-1}によってそれのために定義される役割を働かせるようにA_iに権限を与えるためにそれを認可しなければならない。この鍵対はPKIの一部ではなく、公開鍵だけがA_{i-1}とA_iの間で共有される。したがって、A_iだけがDSK_i秘密を保つために責任がある。何かが続く場合、SK_i、VK_i、DSK_i、およびDVK_iがスタンドアロンで使用されるとき、それらは実際の鍵を示すが、それらが括弧(data)により続けられるとき、それらは括弧付けられたデータを署名または確認する実際の暗号方式の機能を表す。署名機能はメッセージ回復を提供する必要性がない（しかし、提供するかもしれない）。
【００７２】
熟練した人が理解するように、どんな署名機能についても、機能が（括弧を付けられた）データのハッシュ値に適用されるが、明快のため、後で説明されるプロトコルを特定する方程式でこれが明示的に指示されないことが好ましい。これは例えば、DSK_i(data)、およびSK_i(data)、望ましくは、DSK_i(h(data))およびSK_i(h(data))を表し、ここにh()がハッシュ関数を指示する。
【００７３】
最後に、以下の方程式(1)と(2)において、我々は望ましくは新鮮な無作為の系列値かタイムスタンプでA_iがA_{i+1}に譲渡する署名された委任トークン(SDT_i)を定義する。
【００７４】
$$SDT_i = r_i \| SK_i (A_i \| A_{i+1} \| DT_i \| r_i \| DVK_{i+1}) \quad (1)$$
ここに、
【００７５】
$$r_i = T_i \| N_i、または r_i = T_i、または r_i = N_i \quad (2)$$
記号‖は連鎖を表す。新鮮な無作為の系列r_iはたぶんタイムスタンプT_iであるユニークな一片の情報、またはその場限りのN_iあるいはこれらの両方の組み合わせを表す。系列数または無作為のデータはいずれもその場限りとして使用されるかもしれない。値r_iはそれが作成して、SDT_iを送るすぐ前にA_iによって生成され、したがってそれはSDT_i

に縛られる。他の場合にr_i'はタイムスタンプまたはその場限りを示すように使用される。

【００７６】

また、連鎖関数C()は以下の方程式(3)で定義されるように使われるだろう：

【００７７】

$$C_i(a_{i-k}) = a_1 \| a_2 \| \cdots \| a_{i-k} \quad (3)$$

次に、認証、保全、および責任の供給が考慮される。

責任は特定の行為が特定の動作を実行したという証拠を示す。委任の責任は厳密に委任された権利に従わない詐欺の委任の行為の検出を可能にするべきである。さらに、それはその委任された権限を誤用する主張からそれ自体を保護するためにその場限りでない委任を可能にするべきである。

【００７８】

強健な責任のために、委任トークン(DT_i)を使用するプロトコルの実施例において、以下を受けることが望ましい:

・1つの特定の実体から別の特定の実体へ委任されるべき一組のタスクの明確な定義。そのような定義のための形式はM.Abadi、M. Burrows、B. LampsonおよびG.Plotkin、“A calculus for Access Control in Distributed Systems”、ACM Transactions on Programming Languages and Systems、Vol. 15、No. 4、Pages706-734、September1993、に開示され、その形式は参照としてここに明確に取り入れられる。

・委任された権利の用法に関連する方針と制限。これらは保全の理由のため、前述された一組のタスクにしっかりと縛られるべきであり、望ましくは委任権利が自動的に取り除かれる絶対満期期日および/又は時を含むべきである。

・合法な委任信任状として使用することができる、ここでは上で定義されたような署名された委任トークン(SDT_i)のような明確な声明。この要求は係わったすべての行為者(実体)に知られているべきであり、どんな代替人も受入れられるべきでない。

・委任が特定の一組の動作について責任がある程度(通常100%)の明確な理解。

【００７９】

簡単で効率的であるが、強健な解決法を提供するために委任は２つの非対称の鍵対を採用し、その一対（の１つの鍵）は認証要求にこたえるPKI権威で登録される。その上、委任確認鍵(したがって、暗に委任署名鍵)は、委任を認可に結合するため(認可)署名鍵SKに結合される。

【００８０】

ここに説明されるプロトコルの重要な特徴はその適応性であり、その適応性は、それが安全な環境の範囲に適合させられることを許容する。特に、プロトコルは安全の調整可能なレベル、即ち委任の認証と責任のレベルを提供するように適合することができ、その結果、安全のレベル、ここでは環境が許すときコンピュータのおよび/又は通信トラフィック負担を軽減することができる。さらに特に、プロトコルは、委任に対するおよび／又は委任装置における委任する装置の信頼上で通信リンクの安全において委任装置の信頼に依存して適応可能である。

【００８１】

まず最初に、我々は通信リンクまたは媒体を考慮し、2つの異なったクラス、C1、およびC2を定義する。

クラスC1は安全であるべきと思われる通信リンクまたは環境に関連する。クラスC1接続に関する1つの例は、移動端末とコンピュータとの直接の有線の接続、または個人的な信頼されたLAN(ローカルエリアネットワーク)を通る接続である。別のものはホームの環境かオフィスで信頼されたPANか無線のLANに接続された移動端末であり、そこでは、例えば、ブルートゥース、IEEE802.11または同様のもののように基本的なネットワーク技術によって安全は提供される。

【００８２】

クラスC2は悪意がある実体により通信妨害の可能性がある通信リンクに関係づけられ、

このクラスは委任が潜在的に敵意の環境で行われるときに採用される。クラスC2環境に関する1つの例は、どんな安全も提供しないか、または安全にリスクがあるその場しのぎか公衆通信回線に接続された端末である。別の例は端末が(無線または固定された)インターネットアクセスポイントを使用するか、または信頼できないまたは未知のネットワークかネットワークを通して委任するところである。

【００８３】

次に、我々は委任を考慮して信頼の4つのカテゴリを定義する:

ａ）T1: このカテゴリでは、移動装置は委任を盲目的に信頼する。そのような委任の例はホームＰＣや個人的なワークステーションなどのプラットホームで作動する行為サービスであるかもしれない。

ｂ）T2: 端末は委任のための高いレベルの信頼がある。例えば、委任者は知られているサービスかサイトであるか、または委任する装置かユーザにある方法で保証される。例は法人のLANで実行しているサービス、または端末の製造者のデジタル署名を支持するどこでも実行しているサービスであるかもしれない。

ｃ）T3: 端末は委任のための信頼を受入れ可能なレベルを有する。そのような委任者の例は受入れ可能な証明書がある認証された実体であるかもしれない。

ｄ）T4: この場合、端末は委任者を信じない。

【００８４】

以前に言及されるように、すべての実体はPKI権威で登録されることが想定されるか、または期待される。また、委任プロトコルは、(i) 委任者が特定の役割(DT_i で記述された)のため責任も引き受ける端末の要求を受け入れた後に、委任権限が特別に署名されたトークン(SDT_i)として送信され、(ii)任意の実体が新しい鍵対を動的に作成することの可能性があり、また、そのような鍵対の署名（秘密）鍵を安全に保つために責任があると仮定する。

【００８５】

前の分類を使用して、端末により委任の動作の５つのモードの分類は以下の表に設定するように定義される。

【００８６】

【表１】

モード	リンク安全／委任信頼
A	C1/T1またはC1/T2
B	C1/T3
C	C2/T1またはC2/T2
D	C2/T3
E	C1/T4またはC2/T4

動作のこれらの異なったモードで交換されるメッセージは以下に提示され、記法$A_i \rightarrow A_j$ はA_i からA_j へ送られるメッセージを表す。

1．第１のメッセージ〈$A_1 \rightarrow A_2$〉：

｛ａ｝または｛ｂ｝：$A_1 \parallel DT_1$

｛ｃ｝または｛ｄ｝：$A_1 \parallel DT_1 \parallel r_1' \parallel SK_{A1}(A_2 \parallel DT_1 \parallel r_1')$

2．第２のメッセージ〈$A_2 \rightarrow A_1$〉：

｛ａ｝：DVK_2

｛ｂ｝または｛ｄ｝：$r_2' \parallel DVK_2 \parallel DSK_2(DVK_2) \parallel SK_{A2}(A_1 \parallel DT_1 \parallel r_2' \parallel DSK_2(DVK_2))$

｛ｃ｝：$r_2' \parallel DVK_2 \parallel SK_{A2}(A_1 \parallel DT_1 \parallel r_2' \parallel DSK_2)$

3．最終的なメッセージ〈$A_1 \rightarrow A_2$〉：

｛ａ｝または｛ｂ｝または｛ｃ｝または｛ｄ｝：SDT_1

モードeでは、委任者は信じられない第三者である－委任者は署名鍵と検証鍵対をもっていることがあるかもしれないが、それらは信じられない。A_2 が例えば、A_2 の証明書のためローカルストアまたは証明書貯蔵所をチェックすることにより、第１のメッセージを送る前に知られていないことを端末A_1 が決定する。この場合、付加的認可ステップはプロトコル実施に先行する。例えば警告メッセージは、委任者への委任が認可されて、行われるかもしれないというユーザ確認を求める要求と共に表示されるかもしれない。このような初期の認可ステップが、応用に依存して多くの形を取るかもしれないことが認識されるだろう。認可が確認されるならば、プロトコルは環境に依存してモード｛ａ｝乃至｛ｄ｝の何れかにしたがって進められるが、モードcやモードdなどの一般により安全なモードが好まれるかもしれない。

【００８７】

すべての場合において、委任プロトコルは３つのメッセージ交換を含む。まず最初に、端末は委任要求をする。そして、委任者は要求を受け入れるか、または拒絶する。要求が拒絶されるならば(または、無視される)、プロトコルは終わる。要求が受け入れられるならば、委任者は新しい委任鍵対を作成し、委任権威を委任鍵対に与えるための要求と同様に承認の確認を返送する。最終的に端末は委任者の要求を承諾して、署名された委任トークンSDT_1 を形成するためそれらを署名することにより委任鍵と共に委任トークンを義務付ける。プロトコルの簡易化されたバージョンでは、委任者からの回答と署名された委任トークンは委任(検証)鍵を省略するかもしれない。

【００８８】

動作のモードはモードdから始めて、より詳細に記述されるであろう。

モードdにおいて、要求(DT_1)は署名とタイムスタンプによって伴われ、したがってA_1 をA_2 に認証しかつ回答攻撃を妨げる。委任者A_2 がDVK_2 とSDK_2 を作成して、認可するためA_1 のためにDVK_2 を返送するがSDK_2 を秘密に保つ。DSK_2 の存在を立証するため、この鍵はDVK_2 に署名するために使用され、その結果A_1 はDSK_2 の値を言わないが、それにもかかわらず、それはDSK_2 が存在してかつ唯一であることを信じる良い理由を持っている。しかしながら、後述のようにカスケード委任のとき、この委任メカニズムが他の委任の過程によって従われるときにだけこの知識は安全をかなり改良するだろう。特定の委任の承認の前に、委任鍵の強度はチェックされるかもしれない。モードdにおいて、委任者A_2 はメッセージの署名を連鎖することによって付加的にA_1 にそれ自体を認証する。同じ署名がまた、A_2 が委任要求(DT_1)を受け入れたA_1 による証拠として使用することができる。

【００８９】

すべてのモードで同じであるプロトコルの最終的なメッセージにおいて、A_1 は署名された委任トークンをA_2 に送り、それはこの委任を実行する権限をA_2 に与える。SDT_1 は傍受することができ、任意の他の実体により読まれることができるが、証明可能である署名された委任トークン(SDT_1)署名がA_2 のための識別子（の署名）を含んでいるので、A_2 によってのみ使用可能である。

【００９０】

モードc(不確かなリンクであるが、比較的信頼された委任者)は委任者の応答(第２のメッセージ)を除いて、モードdと同様である。モードcのこのメッセージでは、委任者は委任確認鍵を返送し、それ自体を認証し、かつその場限りおよび/又はタイムスタンプでメッセージの新しさを保護するが、DVK_2 の特徴の支持として情報を提供する。しかしながら、このモードでA_2 がT_1 かT_2 領域に属すと仮定されるので、これは必要でない。

【００９１】

モードbは、モードdと同様に、A_2 (カテゴリT_3 の)が比較的信頼されないので、委任がに受け入れられる署名された宣言を返送することをA_2 に要求する。しかし、通信リンクが比較的安全であると考えられるので(および中央の人の攻撃(man-in-the-middle attack)がありそうもないと考えられるので)、プロトコルの効率を増加させるため、A_1 は第１のメッセージに署名のないDT_1 を送る必要があるだけである。A_1 がこのステップでA_2 に

それ自体を認証しないので、委任者A_2は悪意がある一団から発するかもしれない委任の承認に正式に署名する。しかしながら、A_1はそれ自体を認証することの義務を負わされ、最終的なメッセージに委任を承認する。

【００９２】

モードaはプロトコルの最も軽量のバージョンであり、端末のための暗号方式の責任は最後のメッセージで単に署名の作成のみである。この場合、単に片道認証を持つのみであるが、A_2の信頼された特徴のため、一方的な認証は必要と見なされない。再び通信媒体は安全であると考えられ、その結果、中央の人の攻撃の可能性は無視される。

【００９３】

プロトコル実体の簡易化された変形において、A_iが委任トークンDT_1と秘密鍵Mを作成して、署名された委任トークンSDT_1を発生するためDT_1の組み合わせに署名し、次に以下のメッセージを送る:

$\langle A_1 \rightarrow A_2 \rangle : A_1 \parallel A_2 \parallel DT_1 \parallel SDT_1 \parallel enc(M)$

ここに、enc（M）はMの暗号化されたバージョンを示す。鍵Mは対称のアルゴリズムのためにA_1とA_2の間の共通の秘密鍵を含むかもしれず、またはそれは非対称の暗号方式のアルゴリズムに適した鍵対を含むかもしれない(この後者の場合では、熟練した人は対の1つのみが暗号化される必要であると認めるだろう)。暗号enc()がA_2の公開鍵で実行されるか、例えば、先の鍵交換プロトコルからA_1とA_2間で共有された別の共通の秘密鍵を使うかもしれないか、メッセージ回復を可能にする署名アルゴリズムが使用されるかもしれないか、その場合、別々にDT_1およびMを含む必要がない、の何れかがあるかもしれない。そのようなアルゴリズムの例はメッセージ回復アルゴリズムを有するRSA署名（ISO/IEC 9796、“Information technology-Security techniques-Digital signature scheme giving message recovery”、International Organization for Standardization、Geneva、Switzerland、1991）である。プロトコルのこの簡易化されたバージョンは、例えば上で説明されたさらなるメッセージおよび/又は署名および/又は鍵を加えることにより送られたメッセージの安全を増加させることにより、柔軟に実行されるかもしれない。したがって、例えば、上で説明された線に沿った最初の第１および第２のメッセージは、署名された委任トークン(そして委任トークンと鍵)を送るために追加の安全を提供するように加えられるかもしれない。

【００９４】

提示された端末の委任プロトコルはカスケード委任にまっすぐ広げることができる。

さらなる実体A_3に委任をカスケードするとき、最初のステップはA_2に委任のために上で説明されたのと同じようである。望ましくは、カスケード委任は第１の委任トークンによって受入れられるべきである(すなわち、この委任トークンは望ましくは、カスケード委任が受入れられることを示すデータを含むべきである)。次に、第１の２つのメッセージがA_1とA_2の間の第１の２つのメッセージに対応するA_2とA_3の間の交換が続く。これに続いて、委任を進めることを願う委任者(この場合A_3)は、前の委任トークンから形成された新しい委任トークンで受け取られた新しい委任確認鍵を義務付ける(新しい署名された委任トークンに)。責任のため、新しい署名された委任トークンは前の署名された委任トークンによって伴われる。その結果この第３のメッセージは以下(A_2からA_3への委任のために)で示される形を取り、対応する第３のメッセージはそれぞれのその後の委任のために送られる。

【００９５】

$\langle A_2 \rightarrow A_3 \rangle : A_1 \parallel DT_1 \parallel DVK_2 \parallel SDT_1 \parallel SDT_2 \parallel DSK_2 (SDT_2)$

委任のカスケード、即ち連鎖が任意の長さを持つことができ、一般的な場合には、A_{i-1}からA_iへの委任において、交換に関する第３のメッセージは：

$\langle A_{i-1} \rightarrow A_i \rangle : C_i (A_{i-2}) \parallel C_i (DT_{i-2}) \parallel C_i (DVK_{i-1}) \parallel C_i (SDT_{i-1}) \parallel DSK_{i-1} (SDT_{i-1})$

A_1がDVK_1を作成せず、したがって、上の方程式で暗示されるものがヌルデータであると考えられることが認識されるであろう。委任の連鎖、即ちカスケードでは、委任者はそ

れが直ぐ前の前任者から受ける署名された委任トークンについてのみ確認する必要があり、全体の連鎖の署名された委任トークンについて確かめる必要はない。

【００９６】

最終的な委任者(A_f)はサービスを提供することである最終点(B)に連絡する。委任者A_fは有効なSDT_{f-1}が保持されることをBに立証し、A_1または連鎖の内または外の幾つかの他の実体に許諾されるべきサービス(SRV)を要求する。サーバ(B)は、サービス要求(SRV)が最後の委任トークンに従うことを確認し、また、取り付けられるべきであるすべての委任トークンがそれらの前のトークンに従うことを確かめる。委任トークンの全体の連鎖が消尽され、サーバが最終的にDT_1に到達し、確認し、分析するまで、検証は反復的に実行される。保全と責任理由に加えて、最終的な委任者は署名された委任トークンをサーバに提供すべきであり、望ましくはサービス要求SVRでA_fを義務付ける署名を作成しかつ送るため委任署名鍵を使用すべきである。したがって一実施例では、連鎖における最終的なメッセージは以下の構造を持っている:

$〈A_f \rightarrow B〉 : C_f(A_f) \| C_f(DT_{f-1}) \| C_f(DVK_f) \| C_f(SDT_{f-1}) \| r_f \| SRV \| SK_f(A_f \| B \| SRV \| r_f) DSK_f(r_f \| SRV)$

責任に関しては、最終的な委任者はそれが作成するDSK_fについてと同様に前の実体から受信されるSDT_{f-1}の適切な使用法に責任がある。さらに、SRVIはA_fで制限されているが、これはA_fがSDT_{f-1}のために責任があることを必ずしも意味するわけではない。これらのトークンの創造への責任は後方に伝えられ、この方法において容認された規則を誤用する実体が検出されるかもしれない。すべての委任が首尾よく合法な動作を示すならば、サービスの供給への責任の連鎖は、結局最初の委任トークンを作成したA_1に終わる。

【００９７】

見ることができるように、最終的な委任者は新しい署名された委任トークンを作成しないが、代わりにサービス要求SVRを作成する。プロトコルの実施例では、SVRは署名された委任トークンSDTに同様の形式と機能性を持っているが、BがSVRのために責任をほかのところへ委任することを許容しない。実体Bは、(委任トークンDT形式にそれを閉じ込めた後に)SRVをさらに委任する候補B'を配置することを試みるかもしれない。しかしながら、そのようなさらなる委任は、既存の委任およびしたがってBで終わる既存の連鎖の延長というよりもむしろ新しい委任として実行される。プロトコルへのより一般的な変更において、最終的な委任者A_fが連鎖の最終点へサービス要求SRVよりむしろ委任トークンDT_fを送るかもしれないが、多くの場合サービス要求を送ることが望ましい。

【００９８】

委任の連鎖が成功しているところでは、Bは適切な実体に役立って、望ましくはしっかりとどんな必要なデータもそれに送る。このデータは委任の連鎖に沿って返送される必要はない。多くの場合、サービスはA_1に提供されるが、サービスはDT_1の仕様と$C_f(DT_{f-1})$の全体の連鎖に従ってSRVで指定される任意の実体に提供されるかもしれない。

【００９９】

最終点への委任は、委任鍵を交換する必要がないときはちょうど1つのメッセージで達成されたかもしれないが、３つのメッセージ交換プロトコルを使用することができた。概して３つのメッセージプロトコルは３つの主な利点を提供する:最初のメッセージへの応答(カスケード委任/グループ同報通信に役立つ)、委任の承認の正式な証拠、委任確認鍵の作成および返送のための委任の提供、およびこれらの特徴の最初の２つがまた最終点に委任するとき有用である。

【０１００】

図５は動作状態のもとで上述されたプロトコルに送られたメッセージの概要を示す。最初のメッセージは通信リンクが安全であるかどうかに依存してステップS400かS402に従って送られる。安全なリンクのための回答は信頼された端末についてステップS404とS408で概説され、それほど信頼されない端末のために回答がステップS406で概説される。ステップS410で概説される最終的なメッセージは動作のすべてのモードに共通である。さらなる委任の最終的なメッセージはステップS412で概説され(DT_2がA_2とA_3の間で交換された

３つのメッセージの第１にA_3によって受け取られることが認識されるだろう)、最終点に送られたメッセージはステップS414で概説される。

【０１０１】

上の説明されたプロトコルとその変形はどんな特別な構造も要求せず、単に従来のPKIインフラストラクチャに影響力を与える。どんな特別な集中化された制御も必要とせず、プロトコルは数量化可能である。委任(および安全の等級の選択的な決定)のモードの選択は端末で行われ、それはプロトコルの実施例を採用しているデータ処理実体がさまざまな動作環境と両立性であることを許容する。

【０１０２】

初めに活性化されたとき、端末は一般に、どの場合でも、多くのシナリオのために望ましいモードであるモードdまたはモードcのようなより安全なモードの１つを履行しないであろう。以前に指定されていないならば、例えば、ホームＰＣのアイデンティティと証明書を指定することによって、ユーザが現在または不履行作業環境のために移動装置を構成するように促されるかもしれない。いくつかの例において、その設定に依存して、端末は自動的に初期化され、いくつかの場合、初期構成データは、例えば信頼されるとき１以上の製造者(または、オペレータ)のサーバを定義するために、製造者かネットワークオペレータによってインストールされたかもしれない。安全で信頼されたPANを入れると、端末はモードbかcなどの委任の別のモードを選び、この検出とモード変化は自動的に実行されるかもしれない。

【０１０３】

ユーザはまた、例えば、個人的なホームマシンで作動する個人的な移動行為(MA)のような移動行為と共に端末を初期化する必要性があるかもしれない。かかるMAは以前にインストールされたかもしれず、例えば、製造者によってインストールされるか、または例えば、動的にダウンロードされるかもしれない。熟練した人は、そのようなMAが提供されるかもしれない多くの方法があることを認識するであろう。例えば、タクシーサービスを配置するMAは、空港に関連づけられて、ユーザ認可と共にダウンロードされるサーバから提供されて、タクシーを見つけるタスクを委任するために実行するかもしれない。そのような場合では、端末はユーザが安全な環境(例えばホーム)あるいは潜在的に敵意の環境にいるかどうかを決定し、モードaおよびc間で選択する必要があるかもしれない。環境が安全であることを決定することができないかぎり、一般に端末は潜在的に敵意の環境に適切なモードを不履行とするかもしれない。

【０１０４】

図６はそのようなプロトコルメッセージ選択手順に関する概要フローチャートを示す。スイッチオンにしたがってステップS450で端末はモードdのような不履行動作モードを初期化し、およびステップS452(またはユーザコマンドに対応して)で移動行為を初期化するかもしれない。そして、製造者および/又はユーザ入力データから得られる構成データファイル(S456)と、他のユーザ入力データ(S454)からの情報を使用して、端末はそれが可能である限りにおいて通信安全を決定する(ステップS458、S460)。端末は次に、同様のデータを使用して、潜在的委任(S462、S470)の信頼性を決定することを試みて、一般に、不安定な通信媒体と信じられない委任者の仮定を不履行とする(ユーザの選択によるけれども)結果に基づいて決定(S464、S472)をする。通信媒体が安全であるか不安定であるかよって、および委任者が信じられるかどうかによって、それぞれ動作モードの何れか｛ａ｝、｛ｂ｝、｛ｃ｝、｛ｄ｝(または｛e｝、図６に示されない)が選択される。動作のプロトコルモードが自動的に選ばれることが望ましい。製造者または他の様々な権威から予めインストールされた根源証明書を移動端末に提供することにより、またホームＰＣ、個人的な徘徊する移動行為者および/又はオフィスまたは工場のコンピュータシステムのような他の様々な実体と第1の時間に同期するために安全で強健なメカニズムを有する移動端末を提供することによって、これは容易にされることができる。非対称の暗号を使用する委任プロトコルの実施例は説明されたが、また非対称の鍵対の代わりに対称の委任鍵(K_i)を使用して対称の暗号が採用されるかもしれない。対称の暗号を使用するとき、プロトコル

は以下の通り修正される:
ａ）K_i は安全な方法で交換される(通常の技術を使用して);
ｂ）K_i は委任する実体か委任者のどちらかによって作成されるかもしれない;
ｃ）署名された委任トークンは以下の方程式(4)で定義される:
【０１０５】
$$STD_i = r_i \| SK_i (A_i \| A_{i+1} \| DT_i \| r_i \| K_i) \quad (4)$$
また、説明された委任プロトコルの実施例は、それらが（ｉ）(1)または(4)で定義されたようにSDT_i を送ることにより委任を引渡し、（ｉｉ）同じであるか両立性の委任トークンDT_i 使用するならば、それらは他の委任アルゴリズムと両立性がある利点を有する。これは、彼が委任目的に対称鍵対(すなわち委任署名鍵で署名された委任確認鍵の署名を提供することによって)の代わりに非対称の鍵対を使用する委任者立証を有することにより、モードdにおける安全を高める1つの理由である。
【０１０６】
プロトコルの実施例は、プロトコルの応用がこれらのプラットホームに制限されないが、MExE仕様と同様に無線インターネットサービスを提供するセルラネットワークおよび同様のネットワークと両立性である。例えばMExEについて言及すると、これは付随のデジタル署名の特性に応じて、4つの異なった領域にダウンロードされた物体を分類する。あらゆる領域において特定の許容は与えられており、アプリケーションはそれ自体を特定の機能性に制限するように強制する。これは、Javaサンドボックスを形成することにより主として達成される。上述された委任プロトコルは、フレームワークがオペレータか製造者領域のどちらかにあるようにT_2 、信頼された第三者であるようにT_3 、および信じられない第三者であるようにT_4 を取るならば(MExE用語を使用して)、そのようなフレームワークと良く整合する。その結果、初期の認証の後に、移動装置は使用する委任の領域と結果的にその委任動作のモードを自動的に知るだろう。
【０１０７】
１つの主体が別の主体に関して知ることを支持する余分な情報が再送されず、その結果3つのメッセージ交換でさえ、交換されるバイトの総数が減少されるので、実用的なリスクがないとき暗号が使用されないので、および動作環境が可能にするメッセージの長さに動作の異なったモードが減少を許すので、プロトコルの実施例によって提供されたいくつかの利点はデータ通信量の減少である。また、暗号方式の機能の制御用法のため、およびCPUとバッテリーパワーに要求を置く委任鍵の創造が端末よりむしろ委任者によって実行されるので、プロトコルの実施例は計算上比較的安価である。その上、一般に、性能は同報通信への能力によって高められる。
【０１０８】
端末が特定のタスク(例えば、移動商業アプリケーション)をホームＰＣへ委任すると決めるインターネットにアクセスしたPANを入れる移動装置を考えるとする。単一の委任と共にこれを達成することができるが、PCは同じサービス要求をサーバの多数に出して、それらの応答にしたがって最良のものを選ぶことを欲しているかもしれない。これは、PCがいつも同じ行為を使用することを抑制されるので、単一のメッセージ委任で利用可能でなく、そしてサービスがあるなら、または利用可能でないので、別の行為を続ける前に委任が期間切れになるまで、それはサービス要求を拒否するサーバを当てにしなければならないか、または待たなければならない。上述された3つのメッセージ交換プロトコルで委任を同報通信することはそのような困難を軽減することができ、より良い市場の開発とサービスの品質をもたらす。
【０１０９】
プロトコルの安全な態様はいま簡潔に見なおされるであろう。
上述の実施例の動作の全てのモードにおいて、責任と認証は第３のメッセージによって提供される。タイムスタンプおよび/又はその場限りは付随のメッセージの新しさとユニークさが提供されることを確実にすることを助け、回答またはサービスの否定攻撃の危険を減少させる。したがって、２つの通信一団間の適切な時間同期を達成することが困難で

あるいくつかの環境において、その場限りの使用は、タイムスタンプが存在するところでさえ好ましい。

【０１１０】

モードaかbで作動している間、DVK_2 とDT_1 は明白なテキストに送られるが、端末がそれ自身のアイデンティティとA_2 のアイデンティティで委任検証鍵を縛り、その結果、SDT_1 がA_2 の手に値を持つだけであって、本物のDVK_2 が署名された場合だけであるので、安全は提供される。中央の人の攻撃に対する保護がないときはいつも、移動端末は適切なまたは他の委任者の何れが委任要求を受け入れたかを知っている(証拠はないけれども)。しかしながら、そのような場合では、委任はまだその動作において責任がある。詐欺な実体A_2 'がA_2 をまねるように管理し、さらに委任をカスケードすると仮定するならば、この場合最終点ではA_2 のために意図されたSDT_1 をA_2 ’が誤用した事実のもとでサーバが追跡することができるので、これは確認されることができる。

【０１１１】

モードcとモードdの間の違いは、モードdでは委任者が、承認のために返送されたDVK_i が非対称の鍵対の一部であることを明らかに立証するということである。これは、委任者がDVK_i (それが非対称の鍵対のひとりであるところで)を使用するために責任があるようにする。一般に非対称は、共有される必要がある秘密鍵がないとき対称の委任より強健な責任を提供する。

【０１１２】

また、プロトコルの安全はPKIの安全に依存する。委任者の分類は検証フェーズの結果であり、結果として委任が始まる前に認証の過程が行われることが望ましい。一般に、良く定義された規則が証明書権威を治めて、格納と管理を証明することがそのケースである。最終的に、すべての署名動作と応答のために、望ましくは安全および安全な格納で、すべての実体が監査跡を維持することが責任理由で望ましい。

【０１１３】

図７はプロトコルの実施例を実行するのに適当な端末の連鎖500を示す。ここに“端末”は何らかの通信能力でデータ処理システムを示す広い意味で使用され、ポケットPC、移動電話、他の移動通信装置、PDA(携帯情報端末)、パルム-、ラップ-およびデスクトップコンピュータを含む(しかし制限されない)かもしれない。

【０１１４】

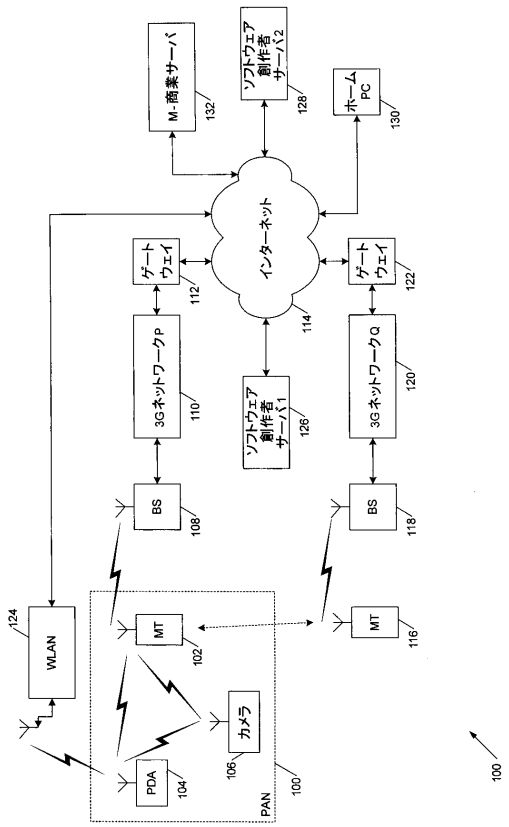
連鎖は移動端末A502で始まり、それは図示された例において第２の端末のB504との通信にあり、最後に連鎖はサーバのような端末Z506で終わる。各端末はメモリと結合されたプロセッサを含み、メモリは対称および/又は非対称の暗号のような暗号方式コードおよび解読コード、および公開鍵証明書(または、他の実施例では、共有された対称鍵)を格納する。また、各プロセッサは、連鎖において何れかの側の端末と無線(または有線)通信リンクを実行するために１つ以上の通信リンクと結合される。図示された例の端末A502は、SIMカードを有する移動端末を含み、それはまた、例えば、デジタル証明書データを格納するかもしれない。

【０１１５】

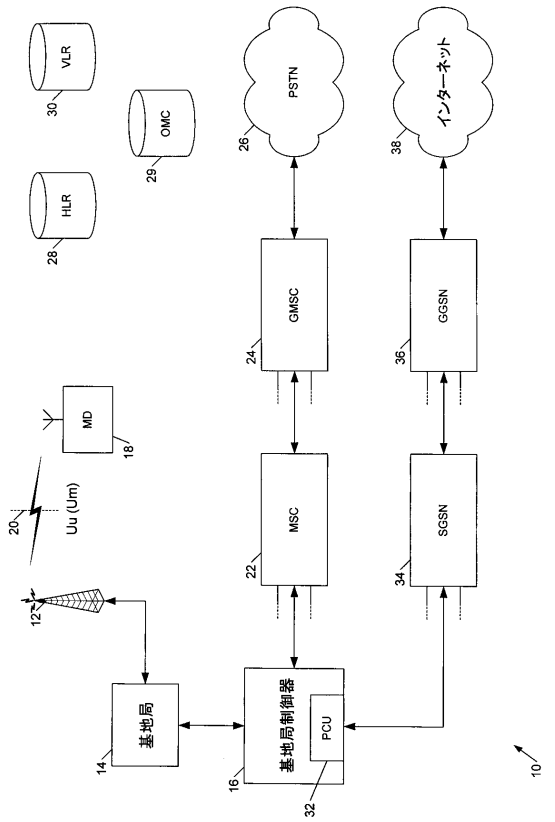
図８は連鎖の端末の1つとして使用に適した汎用計算機システム600を示す。コンピュータシステム600はアドレスおよびデータバス602を含み、それにキーボード608、表示610、およびオーディオおよび/又は丈夫なスクリーンインタフェースなどのマン・マシン・インタフェース(MMI)606が結合される。幾つかの実施例において、暗号方式の処理システムすなわち、メモリと(ことによると専用)プロセッサはSIMカードなどの除去可能なカードに提供されるかもしれない。図８はMMIが一般に欠けているが、そのようなシステムを示す。また、バス602にネットワークインタフェース(サーバのための)、無線または赤外線のインタフェース(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。

【０１１６】
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。
【０１１７】
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。
【０１１８】
移動通信システムおよび有線および無線のコンピュータネットワークの移動端末とサーバが参照されたが、プロトコル態様の実施例のアプリケーションはそのような環境に制限されない。ここに開示されたプロトコルはまた、セルラネットワーク、公共および個人的な有線および無線ネットワーク、信頼されたおよび信頼されないPAN、およびeとm商業サービス提供においてインターネットおよび他のサービスのアプリケーションを持っている。概してここに記述した委任プロトコルの実施例は2つ以上の実体を含み、それらの間で通信する手段を有するどんなシステムでも採用され得る。概して任意の端末またはサーバ、あるいはプログラムコードオブジェクトは委任を開始し、任意の端末またはサーバ、あるいはプログラムコードオブジェクトは連鎖の最終点を形成する。
【０１１９】
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】
【０１２０】
【図１】パーソナル領域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２】3G移動電話システムのための一般的な構造を示す。
【図３】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４】ソフトウェアデファインドラジオ(SDR)ハードウェアとソフトウェア構造の例を示す。
【図５】発明の実施例による適応性のあるプロトコル、およびプロトコルメッセージ選択手順の大要フローチャートに関する概要を示す。
【図６】発明の実施例による適応性のあるプロトコル、およびプロトコルメッセージ選択手順の大要フローチャートに関する概要を示す。
【図７】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８】本発明の実施例による方法を実施するために、図７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】
【０１２１】
１００…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

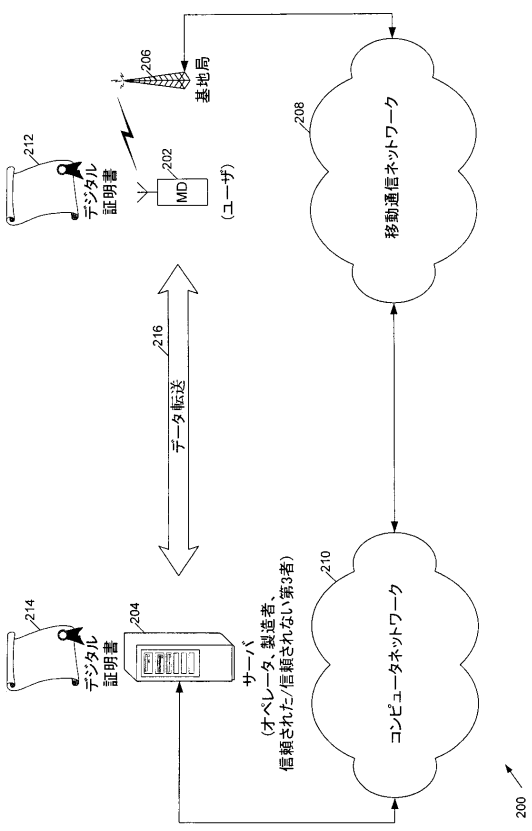
【図１】


M-商業サーバ
132
ソフトウェア創作者サーバ2
128
ホームPC
130
インターネット
ゲートウェイ
112
ゲートウェイ
122
3Gネットワーク P
110
3Gネットワーク Q
120
ソフトウェア創作者サーバ1
126
114
BS
108
BS
118
WLAN
124
MT
102
MT
116
カメラ
106
PDA
104
PAN
100
100

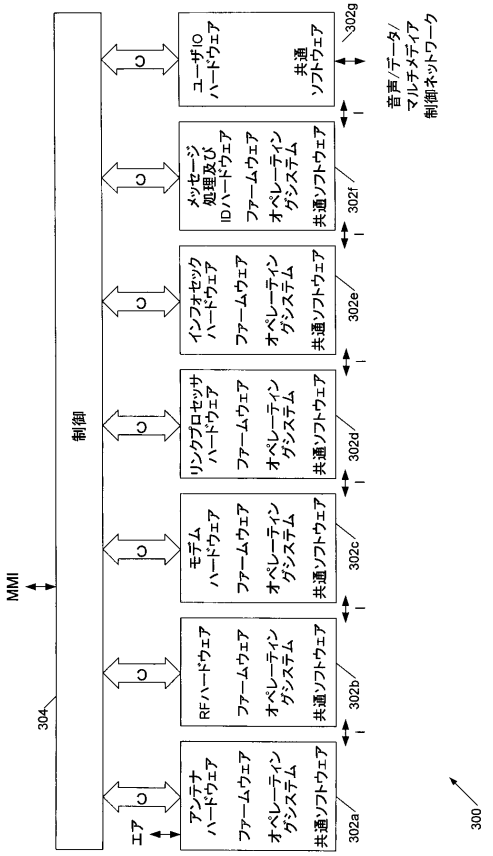
【図２】


VLR
30
HLR
28
OMC
29
PSTN
26
インターネット
38
GMSC
24
GGSN
36
MD
18
20
Uu (Um)
12
MSC
22
SGSN
34
基地局
14
基地局制御器
16
PCU
32
10

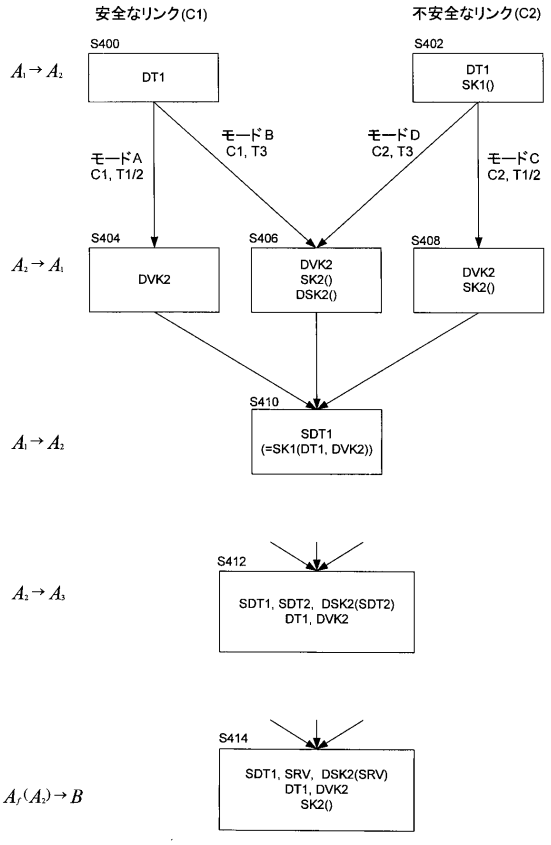
【図３】


基地局
206
デジタル証明書
212
MD
202
(ユーザ)
データ転送
216
移動通信ネットワーク
208
デジタル証明書
214
サーバ
204
(オペレータ、製造者、信頼された/信頼されない第3者)
コンピュータネットワーク
210
200

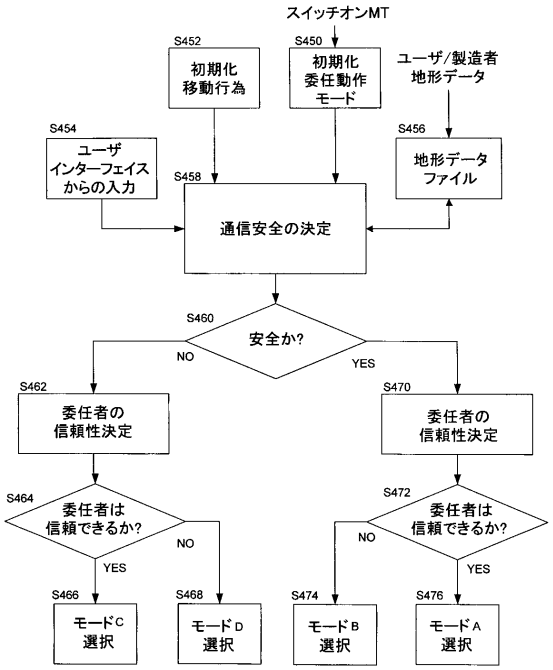
【図４】


制御
MMI
304
エア
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
リンクプロセッサハードウェア
302d
インフォセックハードウェア
302e
メッセージ処理及びIDハードウェア
302f
ユーザIOハードウェア
共通ソフトウェア
302g
音声/データ/マルチメディア制御ネットワーク
300

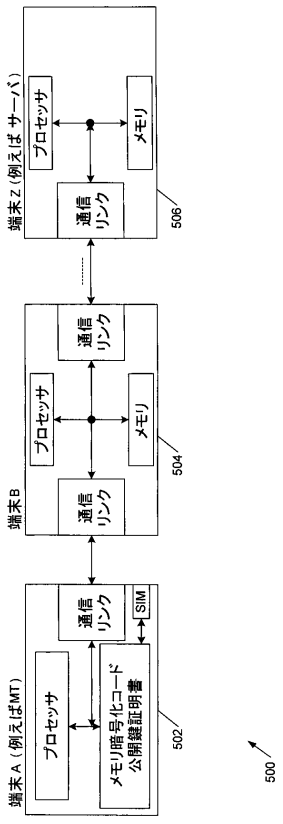
【図５】


安全なリンク(C1)
不安全なリンク(C2)
S400
DT1
S402
DT1
SK1()
モードB
C1, T3
モードD
C2, T3
モードA
C1, T1/2
モードC
C2, T1/2
S404
DVK2
S406
DVK2
SK2()
DSK2()
S408
DVK2
SK2()
S410
SDT1
(=SK1(DT1, DVK2))
S412
SDT1, SDT2, DSK2(SDT2)
DT1, DVK2
S414
SDT1, SRV, DSK2(SRV)
DT1, DVK2
SK2()

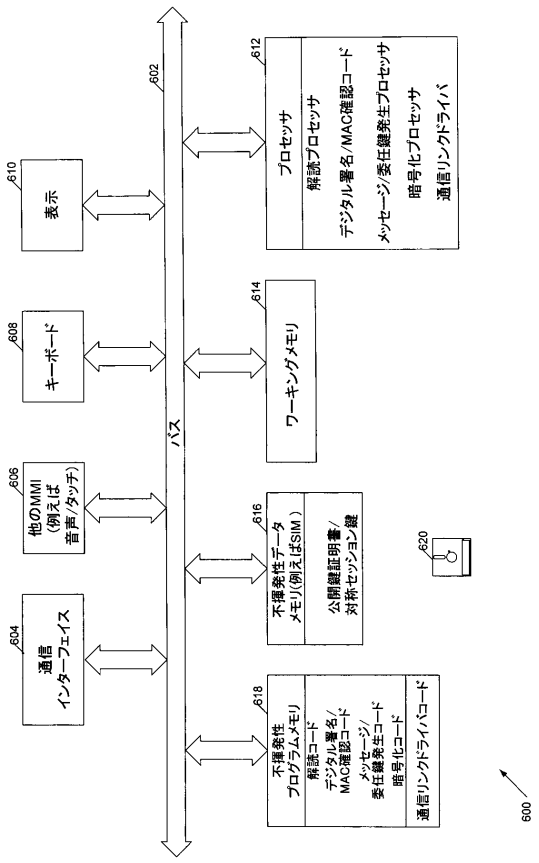
【図６】


スイッチオンMT
S452
初期化
移動行為
S450
初期化
委任動作
モード
ユーザ/製造者
地形データ
S454
ユーザ
インターフェイス
からの入力
S456
地形データ
ファイル
S458
通信安全の決定
S460
安全か?
NO
YES
S462
委任者の
信頼性決定
S470
委任者の
信頼性決定
S464
委任者は
信頼できるか?
NO
YES
S472
委任者は
信頼できるか?
NO
YES
S466
モードC
選択
S468
モードD
選択
S474
モードB
選択
S476
モードA
選択

【図７】


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

【図８】


602
バス
610
表示
612
プロセッサ
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
608
キーボード
614
ワーキングメモリ
606
他のMMI
(例えば
音声/タッチ)
616
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
620
604
通信
インターフェイス
618
不揮発性
プログラムメモリ
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　ジョージオス・カログリディス
イギリス国、　ビーエス１・４エヌデー、　ブリストル、　クウィーン・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　ガリ・クレモ
イギリス国、　ビーエス１・４エヌデー、　ブリストル、　クウィーン・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　チャン・イェオ・イェン
イギリス国、　ビーエス１・４エヌデー、　ブリストル、　クウィーン・スクエア　３２、　トーシバ・リサーチ・ヨーロッパ・リミテッド内

Ｆターム(参考) 5J104 AA09　PA07　PA10