(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-502045
(P2008-502045A)
(43)公表日　平成20年1月24日(2008.1.24)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B285
G06F 1/00	(2006.01)	G06F	1/00	370E	5J104
H04L 9/32	(2006.01)	H04L	9/00	675Z	

審査請求 未請求　予備審査請求 未請求　（全 14 頁）

(21)出願番号　特願2007-514994 (P2007-514994)
(86)(22)出願日　平成17年6月2日 (2005.6.2)
(85)翻訳文提出日　平成18年12月14日 (2006.12.14)
(86)国際出願番号　PCT/SE2005/000851
(87)国際公開番号　WO2005/119399
(87)国際公開日　平成17年12月15日 (2005.12.15)
(31)優先権主張番号　0401411-4
(32)優先日　平成16年6月2日 (2004.6.2)
(33)優先権主張国　スウェーデン(SE)

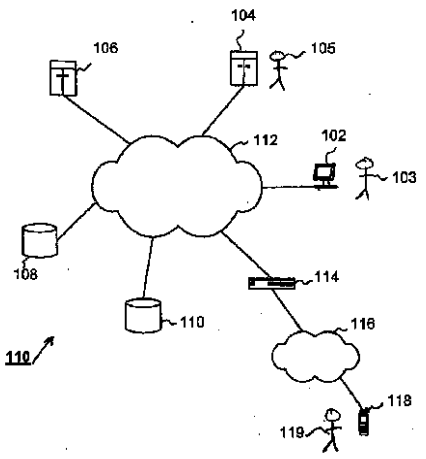
(71)出願人　507344830
ユビクォーセキュリティ　アクチェボラーグ
スウェーデン国、エス－２１２　２８　マルモ、シェーレガータ　９
(74)代理人　100086461
弁理士　齋藤　和則
(72)発明者　ホイジ、フェリペ
スウェーデン国、エス－２１４　３６　マルモ、リステルガータ　２

Fターム(参考)　5B285 AA01 BA03 CA02 CA43 CA44 CB02 CB47 CB62 CB72
5J104 AA07 KA01 PA07 PA10

最終頁に続く

(54)【発明の名称】電子商取引の確保

(57)【要約】
承認サービス（１０６）における方法と、電子商取引の確保のためのユーザＩＤユニット（１０２，１１８）における対応する方法とが開示されている。本方法は、少なくとも1つのユーザＩＤ（１０２，１０３、１１８、１１９）と１つのビジネス・サービスとに関連された商取引を承認する要求の受け取りで始まる多数の段階を含み、その後に前記ビジネス・サービスを使用すべくユーザＩＤの権限付与の検査が実行される。次いでユーザＩＤとの交換が、前記ビジネス・サービスについての少なくとも情報を含む暗号化されると共に署名済み検証書類で実行される。次に商取引はその検証書類の内容に依存して承認される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
電子商取引の確保のための承認サービスにおける方法であって、
少なくとも１つのユーザ・エンティティと１つのビジネス・サービスとに関連された商取引を承認する要求の受信と、
前記ビジネス・サービスを使用すべくユーザＩＤの権限付与の検査と、
前記ビジネス・サービスについての少なくとも１つの情報を含む暗号化されて署名された検証文書の前記ユーザＩＤとの交換と、
前記検証文書の内容に依存しての前記ビジネス・サービスの承認と、を含む方法。
【請求項２】
前記ユーザＩＤの権限付与の検査が該ユーザＩＤに関する識別情報の受信を含み、
前記検証文書の交換が、前記ユーザＩＤと関連された公開証明書のフェッチング、前記認証文書の作成、前記ユーザＩＤの前記公開証明書による前記検証文書の暗号化、前記承認サービスの秘密キーによる前記検証文書の署名、前記検証文書の前記ユーザＩＤへの送信、並びに、前記ユーザＩＤからの前記検証文書の受信を含んでおり、
前記ユーザＩＤからの前記検証文書の受信後に、前記ユーザＩＤの前記公開証明書のフェッチングを為し、前記ユーザＩＤの前記署名の検証を為し、前記検証文書の内容の解釈が追従される、前記ユーザ・サービスの前記秘密キーによる前記検証文書の解読することから成る請求項１に記載の方法。
【請求項３】
前記ユーザに関する前記検証情報が識別情報から成るリスト内で利用可能である請求項１或は２に記載の方法。
【請求項４】
前記証明書がリスト内で利用可能である請求項１乃至３の内の何れか一項に記載の方法。
【請求項５】
前記ユーザＩＤの前記権限付与の制御が、前記承認サービスと、識別情報から成る前記リストを含む第１カタログ・サービスとの間の通信を含み、
前記証明書の前記フェッチングが、前記承認サービスと、証明書から成る前記リストを含む第２カタログ・サービスとの間の通信を含む請求項３或は４に記載の方法。
【請求項６】
前記承認サービスが前記ビジネス・サービスの一部である請求項１乃至５の内の何れか一項に記載の方法。
【請求項７】
請求項１乃至６の内の何れか一項に記載の方法をコンピュータに実行させる命令を含むコンピュータ・プログラム。
【請求項８】
電子商取引の確保のためのユーザＩＤユニットにおける方法であって、
商取引についての少なくとも情報を含む暗号化されて署名された検証文書の承認サービスと交換することと、
前記検証文書の内容に応じて、権限付与データを提供し、その意味が、前記承認サービスに前記承認前記商取引を承認させることが意図されていることである、
を含む電子商取引の確保のためのユーザＩＤユニットにおける方法。
【請求項９】
請求項８に記載の方法をコンピュータに実行させる命令を含むコンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はディジタル通信システムにおける商取引、特に、認証、権限付与、並びに、ア

カウンティングの確保のための方法に関する。

【背景技術】

【０００２】

ディジタル通信システムにおける電子商取引の概念は、標準的には、複数の普通の機能と、ユーザとサービスの供給者における１つ或は幾つかの相互接続されたコンピュータとで協同して実行されるか、若しくは、相互接続されたコンピュータ間だけで実行されるそれら機能の結果とを言及するものである。典型的な例は、銀行サービス、予約サービス、電子商業センタ、いわゆる共同体、並びに、電子メール及びファイル共有等々のサービスに関連したコンピュータへの記録を含む。

【０００３】

たとえユーザ概念が標準的に「人間」連結を有しても、その概念は「非人間」エンティティ、即ち、コンピュータ形態の機械をも含むことが強調される。従って、ユーザＩＤの概念は以下のように使用されて、ユーザの概念と交換可能であると解釈される。

【０００４】

これらサービスの大多数に対する特徴付けは、それらがユーザにとって価値ある情報の処理を含むことである。この種の情報の例としては、銀行口座資産或は他の機密情報を含む。更に、この種の情報は、その情報にアクセスすべく権限が付与されていない人にとって、それを不可能と為すか或は少なくとも非常に困難と為すように管理することが、通常、最も重要である。

【０００５】

多数の相互に異なる安全システム及び方法が、ユーザ情報にアクセスする権限が付与されていない人にとって出来る限り難しくする要件に従うべく、先行技術において作り出されている。認証、権限付与、並びに、アカウンティング等の概念は周知であると共に先行技術において充分に立証されている。

【０００６】

要約すれば、認証が意味することは、商取引システムのユーザのＩＤがそのシステムの他のユーザに対して或はそのシステム自体に対して確保されていることである。権限付与が意味することは、そのシステム内での商取引或はそのシステムによって該システムの他のユーザとの商取引を実行すべく、好適的に権限付与されたユーザの権限付与が確保されていることである。会計が意味することは、そのシステム内でのユーザの措置及び商取引に関する情報が登録されて、権限付与されたユーザＩＤが任意の時点でその情報を読み取って解釈できるように記憶されることである。

【０００７】

今日有効である認証に対する解決策はいわゆる「帯域内」認証であり、それは、認証データが商取引プロセス中に追って送信され、受信されるデータと同一のルートを介して送信されることを意味する。この手続きが暗示することは、ユーザの識別が、例えば、ユーザネーム及びパスワード、使い捨てパスワード、或は、その類によって実行されることである。もしユーザのデータ及び検証の暗号化が証明書を介して実行されるかにかかわらず、システムはそれが使用されているターミナルの背後に着座している本当に正しい人であるかが、そのユーザが一見識別されているようであっても、決して知ることができない。更に殆どの場合、本物のユーザは、彼以外の誰かがそれらの識別情報、いわゆるアカウンティングによって記録又はログオンしたことを見出すことが決してできない。更にこれが意味することは、ユーザの記録情報が普及したか、或は、使い捨てパスワードがそのユーザ自身以外の誰かによって使用されているか（例えば、誰かが使い捨てパスワードのユーザ・リストを複写したか）を、ユーザが知ることは実際上不可能である。加えて、パスワードに関する基本的な問題が存在しており、それらパスワードは、しばしば、いわゆる「ブルート・フォース」／「ディクショナリ」の着手を介して推測或は解決することが容易である。

【０００８】

基本的には、今日の識別及び認可のシステムは不確かであり、その理由は、誤った記録

のロギングがシステム所有者によって実行されて、サービス・アカウント持ち主によっては実行されないからである。たとえ既知システムが使い捨てパスワードを使用したとしても、権限付与されたユーザは権限付与されていないユーザが自信が取得したパスワードを誤用することを防止する可能性は全くない。

【０００９】

認証の「帯域内」処理の使用の例は下記の特許文献１、マイクロソフト社の製品「．ＮＥＴ　Ｐａｓｓｐｏｒｔ」、並びに、ユーザネーム及びパスワードが使用されているネットワークの大多数に見出すことができる。

【特許文献１】米国特許第６，２８５，９９１号

【発明の開示】

【００１０】

発明の概要

結果として本発明の目的は、先行技術における電子商取引と関連して、認証、権限付与、並びに、アカウンティングに関係する問題を解決することである。

【００１１】

この目的は、電子商取引の確保に対する承認サービスにおける一方法による第１局面に従って達成される。そのプロセスは、少なくともユーザＩＤと１つのビジネス・サービスとに関連された商取引を承認する要求を受信することによって始動される多数の段階又はステップを含み、その後に、そのビジネス・サービスを使用するユーザＩＤの権限付与が制御される。ユーザＩＤとの交換は暗号化されると共に署名された検証書面によって予め形成され、それはその商取引についての情報を少なくも含む。次にその商取引は検証書面の内容に依存して認可される。

【００１２】

好適実施例において、ユーザの権限付与の制御は、ユーザＩＤに関する識別情報の受信を含み、検証文書の交換はユーザＩＤと関連された公開証明書のフェッチングを含む。この検証文書は作成され、ユーザＩＤの公開証明書によって暗号化され、そして、承認サービスの秘密キーによって署名される。次いで検証文書はユーザＩＤに送信される。

【００１３】

検証文書はユーザＩＤに送信されと、その検証文書の処理は、本発明の第２局面と関連して以下に議論されるように、ユーザＩＤで実行される。

【００１４】

次いで検証文書はユーザＩＤから受信されて、ユーザＩＤの公開証明書がフェッチされる。ユーザＩＤの署名の検証は実行され、その後、その検証文書は承認サービスの秘密キーによって解読される。次いで、その検証文書における内容の解釈は実行されて、その内容に応じて、商取引を承認する。

【００１５】

ユーザに関する識別情報は、識別情報から成るリストにおいて好適に利用可能であり、ユーザＩＤの権限付与の制御は好適に実行されて、それが承認サービスと識別情報から成るリストを含む第１カタログ・サービスとの間の通信を含むように為す。証明書のフェッチは、好ましくは、承認サービスと、証明書から成るリストを含む第２カタログとの間の通信を含む。

【００１６】

一実施例において、承認サービスはビジネス・サービスの一部である。

【００１７】

第２局面からの本発明の目的は、電子商取引の確保のためのユーザＩＤユニットにおける方法によって達成される。この方法は、暗号化されると共に署名された検証文書の承認サービスとの交換を含み、それは、その商取引についての情報を少なくとも含む。権限付与データはその検証文書の内容に応じて与えられ、その意図は承認サービスにその商取引を承認させようとするものである。

【００１８】

言い換えれば、識別子（例えばユーザ名）だけがビジネス・システムの媒体を介して通過させられるユーザＩＤの「帯域外」認証を用いることによって、高い安全の長所が達成され得る。この種の安全が暗示することは、ユーザＩＤが、例えば承認サービスを介して等の、平行或は補助チャネルを介して、認証及び権限付与の双方を実行することによって商取引を承認することである。この結果は、相当により高い安全が商取引承認と規定されたビジネス・サービスへのアクセスの承認との双方のために提供され得る。非対称暗号化を用いることによって、情報の暗号化及び署名が達成され得る公開証明書及び秘密キーで、安全性と平行或は補助チャネルが外側からは読み取ることができずに獲得される。これによって、ビジネス・サービスの持ち主は、そのサービスのユーザが、商取引承認質問が権限付与されたユーザに送信されるので、そのアカウント／権限付与の権利を所持するものであることを確信できる。権限が付与されたユーザＩＤはシステム内にも構成されて、ユーザＩＤのログオンを承認して、そのシステムが該システムを使用すべく権限付与されたものを知る。しかしながら、ユーザＩＤ自体はそのシステムへのアクセスが付与されるかを承認する。

【００１９】

本発明は複数の相互に異なる適用エリア内で有益に使用され、それらには、電子バイリンガル、システムへのログオン、音声認識、ミクロ支払いシステム、現金引き出し、店舗におけるクレジットカード支払いの承認等の他の支払い承認を含む。本発明は、例えば、ログオン、ハードウェアの検索等の更にしっかりした商取引、ドアの通過等々の、複数の商取引を承認すべく異なるユーザの間での協力を要求する異なる種類のシステムにも適用可能である。

【００２０】

（図面の簡単な説明）

図１は、本発明が具現化されているディジタル通信システムを概略的に示している。

図２ａ及び図２ｂは、本発明に従った承認サービスにおける方法を図示するフローチャートである。

図３は、本発明に従ったクライアントにおける方法を図示するフローチャートである。

【発明を実施するための最良の形態】

【００２１】

先ず、非対称暗号化の簡単な説明が付与されて、本発明が有益に具現化されるシステムの記載が追従される。次いで詳細な説明は本発明に従った方法を続ける。留意されることは、ユーザ概念がユーザＩＤの概念と交換可能であると見なされ、即ち、ユーザは本発明に従って機能するＩＤの人の形状における単なる一例である。

【００２２】

非対称暗号化は公開証明書及び秘密キーに基づくものであり、それらは対の関係で相互に関連されている。公開証明書は誰にでも利用可能であり、そして、公開カタログ・サービスを介して公共に対して利用可能である。公開証明書について重要なことは、その証明書における情報が安全ソースから来ることである。秘密キーにおける情報は常に秘密保持されて、送信或は受信される情報を署名或は解読するものだけが使用されなければならない。

【００２３】

公開証明書によって暗号化されたデータは公開証明書と関連する秘密キーを所持するものだけによって解読され得る。

【００２４】

秘密キーによって署名されたデータはその秘密キーと関連された公開証明書によって検査され得る。この署名が意味することは、元々署名された情報がその署名が公開証明書に対して検査される時点まで同一情報でなければならず、且つ、その情報に署名した人がその署名及び公開証明書が相互に符合する時を知らせられることである。

【００２５】

たとえもし、ディジタル証明書による非対称暗号化が本発明が具現化された際に使用さ

れることが好ましいとしても、本発明が他の種類の暗号解決策によって具現化され得ることを当業者は理解する。

【００２６】

図１は、通信ネットワーク１１２と接続された多数の通信関係者を含むシステム１００を示す。例えばパーソナル・コンピュータ等の第１ユーザ・ユニット１０２はユーザ１０３に、銀行、小売店、或は、その類であり得るビジネス・サービス１０４へのアクセスを提供するように構成されている。第２ユーザ１０５は、より直接的な個人的接触によって、例えば、ビジネス・サービス１０４を制御できる人員を有する銀行オフィス或は小売店等のある箇所に存在することによって、そのビジネス・サービス１０４へのアクセスを有する。第３ユーザ１１９は、移動電話等の移動局１１８を介して、ネットワーク・ブリッジ１１４を通じて携帯電話ネットワーク１１６によってそのビジネス・サービス１０４が接続されている通信ネットワーク１１２と通信するように構成されている。

【００２７】

移動端末を用いる代替方法は、例えば第１ユーザ１０３等のユーザがビジネス・サービスへのログオンの承認のために携帯電話を用いることであり得る。換言すれば、ユーザはパーソナル・コンピュータの形態のユーザ端末を利用して、ビジネス・サービスへのアクセスを要求して、該ビジネス・サービスと通信し、その後に、ユーザは携帯電話を用いて商取引を承認する。

【００２８】

ビジネス・サービス１０４は、コンピュータ内において、複数のソフトウェア・コンポーネントの形態で好ましくは具現化され、そしてそれは商取引を実行すべくユーザから要求を受信するタスクを有し、その商取引を実行するか或はその実行の少なくとも制御のための機能が具備されている。図２におけるフローチャートを参照してより密接に記載されるように、ビジネス・サービス１０４には承認サービス１０６と情報の交換を為す機能が更に具備されている。

【００２９】

承認サービス１０６は通信ネットワーク１１２と接続されている。コンピュータ内におけるソフトウェアによって好ましくは具現化されもするこの承認サービス１０６は、図２におけるフローチャートを参照してより密接に記載されるように、情報やユーザ及びビジネス・サービスの間の情報伝達を処理するタスクを有する。

【００３０】

承認サービスの代替実施例が暗示することは、それがビジネス・サービスの一部を実行することである。

【００３１】

１つ或は幾つかのコンピュータ内おけるソフトウェア・コンポーネントの形態で具現化される、第１カタログ・サービス１０８及び第２カタログ・サービス１１０もまた通信ネットワーク１１２と接続されている。これらカタログ・サービス１０８，１１０はユーザ及び承認サービス１０６にデータを提供する主機能を有する。その最も簡潔な実施例において、第１カタログ・サービス１０８は、ビジネス・サービスを使用すべく権限が付与されているユーザに関する識別情報から成るリスト或はデータベースを備える。その最も簡潔な実施例における第２カタログ・サービス１１０は、ユーザ及びサービス・プロバイダに属する公開証明書から成るリストの形態での情報を備える。これらカタログ・サービスの使用は図２におけるフローチャートを参照してより密接に記載される。

【００３２】

以下、本発明に従った方法が、図１、図２ａ、並びに、図２ｂにおけるフローチャートを参照して記載される。その状況として、即ち第１ユーザ１０３、第２ユーザ１０５、或は、第３ユーザ１１９の内の誰であろうがユーザは、ビジネス・サービス１０４と協力して商取引を実行するつもりである。ユーザが第１ユーザ１０２である場合、ビジネス・サービス１０４との通信は、ビジネス・サービス１０４と関連されたワールド・ワイド・ウェブ上のホームページ等のインターフェースを介して、好ましくはパーソナル・コンピュ

ータ或はその類であるユーザ・ユニット１０２によって生ずる。ユーザが第２ユーザ１０５である場合、ビジネス・サービス１０４との通信は、例えば銀行オフィス或は小売店であるビジネス・サービスの施設との直接的な接触を介して生ずる。ユーザが第３ユーザ１１９である場合、ビジネス・サービス１０４との通信は、電話１１８、携帯電話システム１１６、並びに、ネットワーク・ブリッジ１１４を介して生ずる。

【００３３】

不必要な詳細によって本発明を不明瞭することを回避すべく、より密接な記載、即ち通信が通信システム１１２内において相互に異なるユニットの間でどのようにして生ずるかの詳細が何等提供されない。当業者は、本発明を具現化する点に関して、メッセンジャ・サービス、通信プロトコル等々を選択する形態での行動の適合する進路を選択することになる。

【００３４】

初期ステップ２０２でビジネス・サービス１０４は、ビジネス・サービス１０４と接触状態であり且つ商取引を実行したいユーザに対して彼自身を識別させることを要求する。ユーザはこの要求に遭遇して、識別情報の形態であるデータがユーザによってビジネス・サービス１０４に提供され、次いでそのビジネス・サービス１０４から承認サービス１０６まで送信される。適切には、識別情報は、ネーム、番号組み合わせ、並びに、署名から成るシーケンス等の少なくともユーザＩＤを含む。適切には、識別情報も、懸案である商取引を記述するキャラクタ・ストリングを含む。

【００３５】

検査ステップ２０４で承認サービス１０６は、識別グループが第１カタログ・サービス１０８で利用可能である権限付与されたユーザに対する識別情報のカタログと符合させることによって、送信された識別情報がビジネス・サービス１０４を使用すべく権限付与されたユーザと対応するかを検査する。

【００３６】

もし識別情報が承認されないか或はカタログ内に存しない場合、商取引は判定ステップ２０６で妨害され、承認サービス１０６が送信された識別情報がそのサービスを使用できない旨を返答する。発生した事象に関するメッセージがロギング・ステップ２０８でユーザ・アカウントの持ち主、或は、例えばビジネス・サービス若しくは承認サービスの持ち主に送信され得る。

【００３７】

フェッチング・ステップ２１０で承認サービス１０６は、第２カタログ・サービス１１０から公開証明書をフェッチする。

【００３８】

もし識別情報の公開証明書が存在せず、満了していれば、或は、もしキャンセル（撤回）されるか若しくは無効であれば、商取引は判定ステップ２１２で妨害される。ロギングは、ステップ２０６及びステップ２０８に関連して先に記載されたように、ここで実行され得る。

【００３９】

検証文書は文書作成ステップ２１４で作成され、その文書はタイムスタンプ、一意のキャラクタ・ストリング、並びに、識別情報を含む。確かに、商取引に関する情報識別詳細もその検証文書内に含まれ得る。検証文書はユーザの公開証明書によって暗号化されて、そのユーザのみがそれを解読でき、次いでそれが承認サービス１０６の秘密キーで署名される。

【００４０】

検証文書は、次いで、送信ステップ２１６でユーザに送信される。この送信は、Ｅメール、インスタント・メッセンジャ・サービス、或は、メッセージを送信可能である他の何等かのメッセンジャ・サービス等の適切に選択されたメッセンジャ・サービスによって実行される。

【００４１】

フェッチング・ステップ２１８でユーザは、第２カタログ・サービス１１０から承認サービス１０６の公開証明書をフェッチする。

【００４２】

もし識別サービス１０６の公開証明書が存せず、満了していれば、或は、もしキャンセル（撤回）されるか若しくは無効であれば、その商取引は判定ステップ２２０で妨害される。

【００４３】

解読ステップ２２２でユーザは、署名と承認サービス１０６の公開証明書とによって当該ユーザが制御した際に彼の秘密キーによって検証文書を解読し、そのサービスはユーザによって知られており且つ信頼されている。

【００４４】

判定ステップ２２４でユーザは、承認サービス１０６へのアクセスを承認或は否定すべく選択するか、或は、該ユーザがそのサービスへのアクセスを否定するのと同一の方式で解釈されることになる返事を送信しないように選択する。ここでユーザ自身はその商取引を妨害すべく選択することができる。

【００４５】

処理ステップ２２６でユーザは、承認或は否定についての情報を検証文書内に追加し、それを承認サービス１０６の公開証明書で暗号化して、その文書に彼の秘密キーで署名する。

【００４６】

次いで検証された文書は、判定ステップ２２４に依存しての、認証及び権限付与、或は、否定のように、送信ステップ２２８において承認サービス１０６に戻るように送信される。

【００４７】

フェッチング・ステップ２３０で承認サービス１０６は、第２カタログ・サービス１１０から識別情報の公開証明書をフェッチする。

【００４８】

もしその公開証明書が存せず、満了していれば、或は、もしキャンセル（撤回）されるか若しくは無効であれば、商取引は判定ステップ２３２で妨害される。

【００４９】

処理ステップ２３４において、署名は識別情報と関連されたディジタル証明書に関して認証され、その後、その内容が承認サービス１０６の秘密キーによって解読されて、権限付与データがユーザによって認証された文書から読み取られる。

【００５０】

もし承認サービス１０６に戻されるように送信された検証された文書が否定を含めば、判定ステップ２３６においての商取引は妨害されることになる。

【００５１】

もし承認サービス１０６に戻されるように送信された検証された文書が承認を含むと共に、結果としてユーザが認証され且つ商取引が承認されれば、そのサービスへのアクセスが許諾ステップ２３８で承諾され、それは単純な実施例において、ビジネス・サービス１０４への署名或はメッセージの送信を含む。

【００５２】

ユーザは自信のパーソナル・キーを暗号化し、それは秘密保持されるべきであり、例えば、パスワードによって、ユーザの携帯電話、コンピュータ、或は、その類に格納されて、秘密キーが使用され得るべく認証を要求し、それはそのキーも保護されることを意味する。

【００５３】

ユーザ及び承認サービス１０６の間での情報の送信の際にメッセンジャ・サービスを用いる場合、認証は証明書によって好ましくは実行されるが、これは本発明の範囲外である。

【００５４】
以下に、図１及び図３を参照して、例えば、ユーザが図２ａ及び図２ｂに記載された方法に従って承認サービスと通信する際に彼自身のコンピュータ或はモバイル通信ユニット内で実行される方法の説明が続けられる。以下に説明される方法は、それ故に、システムの他の部分と協力して動作するクライアント方法として名付けられ、それは権限付与及び認証の疑問をユーザに提示してその疑問への答えを戻すように送信するタスクを有する。
【００５５】
「ユーザ」によって意味されることは、例えば、物理的な人間、法人、別のシステム或はサービス、若しくは、受信された情報に基づき判定を下す能力を具備する別のエンティティである。
【００５６】
反復ステップ３０２においてメッセージは、通信インターフェースによって受信され、該通信インターフェースとクライアントが電子的或はその他の方式で接続されている。
【００５７】
解釈ステップ３０４でメッセージ内の情報は、ユーザの通信ユニット或はコンピュータに対して通用するフォーマットに解釈される。
【００５８】
制御ステップ３０６で、メッセージが署名され且つその署名がそのメッセージを送信したと予想されるものによって発せられるように制御される。この制御は公開証明書に対する署名を検査することによって或はその署名の認識によって実行される。
【００５９】
解読ステップ３０８でメッセージの内容は、ユーザの秘密ディジタル・キーを用いることによって解読される。そのメッセージの内容は、商取引／ロギング／投票／認証の疑問に関するメッセージ、その疑問への許諾され／可能性ある返答、商取引ＩＤ等々の内の１つ或は幾つかであり、そしてまた任意選択的な余剰情報である。
【００６０】
提示ステップ３１０で、ユーザの権限付与の方法が提示され、例えば、メッセージに適合するように提示され、その方法はユーザがその提示された権限付与方法に返答することを要求することを含む。
【００６１】
返答ステップ３１２でユーザは、可能であれば商取引ＩＤ及び／或は他の情報と一緒に、新メッセージ内に返答を付加することによって返答代替案の内の１つを提供する。
【００６２】
暗号化ステップ３１４で、メッセージは、（オリジナルの受信者の）受信者のＩＤ関連証明書によって、或は、別の暗号によって暗号化される。
【００６３】
署名ステップ３１６で暗号化されたメッセージは、ユーザの秘密キーによって、或は、別の暗号によって署名される。
【００６４】
送信ステップ３１８で署名され暗号化されたメッセージは、ユーザが接続する選択的な通信インターフェースを介して為された権限付与或は認証疑問への返答としてオリジナルの送信者に送信される。
【００６５】
留意されることは、ユーザは自信のパーソナル・キーを暗号化し、それは秘密保持されるべきであり、例えば、パスワードによって、ユーザの携帯電話、コンピュータ、或は、その類に格納されて、秘密キーが使用され得るべく認証を要求するように為し、それはそのキーが保護されることを意味する。メッセージ・サービスを用いる認証は、例えば、証明書によって実行され得る。しかしながらこれは本発明の範囲外である。
【図面の簡単な説明】
【００６６】

【図１】本発明が具現化されているディジタル通信システムを概略的に示している。
【図２ａ】本発明に従った承認サービスにおける方法を図示するフローチャートである。
【図２ｂ】本発明に従った承認サービスにおける方法を図示するフローチャートである。
【図３】本発明に従ったクライアントにおける方法を図示するフローチャートである。
【符号の説明】
【００６７】
１０２　第１ユーザ・ユニット　１０３　第１ユーザ
１０４　ビジネス・サービス　１０５　第２ユーザ
１０６　承認サービス　１０８　第１カタログ・サービス
１１０　第２カタログ・サービス　１１２　通信ネットワーク
１１４　ネットワーク・ブリッジ　１１６　携帯電話ネットワーク
１１９　第３ユーザ　１１８　携帯電話システム

【図１】

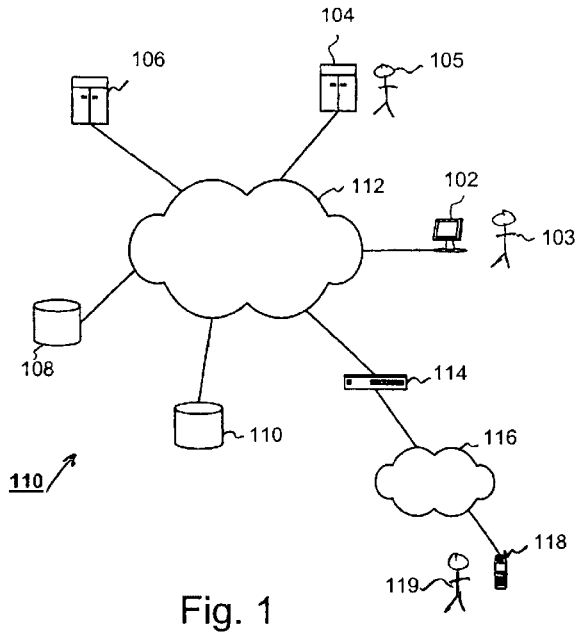


Fig. 1

【図２ａ】

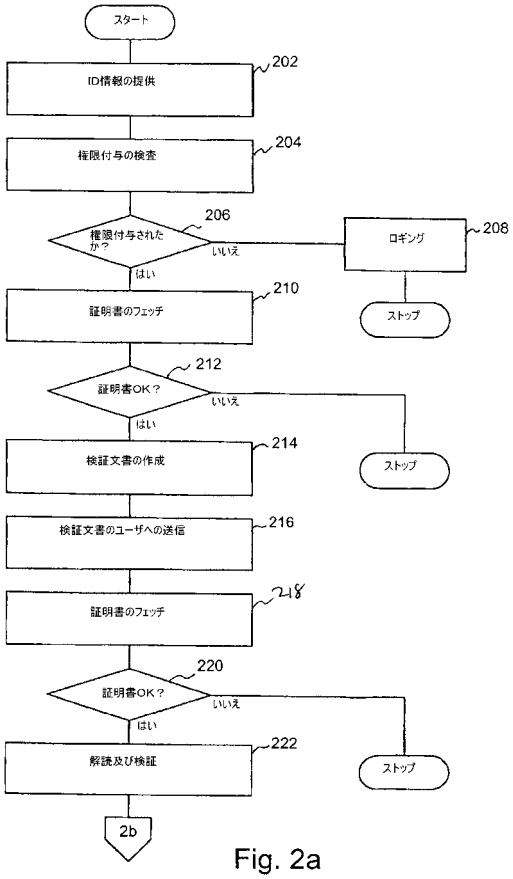


Fig. 2a

【図２ｂ】

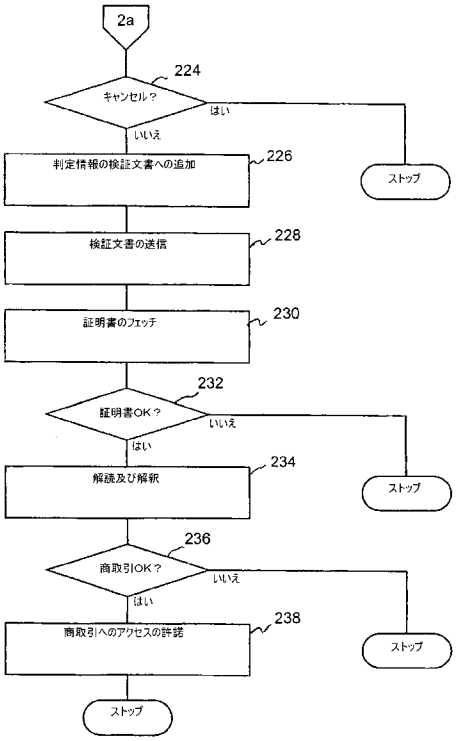


Fig. 2b

【図３】

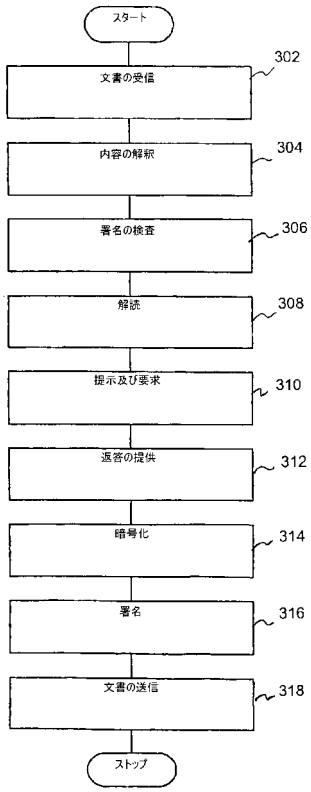


Fig. 3

【国際調査報告】

1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 2005/000851

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, se arch terms used)

EPO-INTERNAL, WPI DATA, PAJ, INTERNET, FULLTEXT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4405829 A (RIVEST, R L ET AL), 20 Sept 1983 (20.09.1983), see the whole document --	1-9
X	US 20020162003 A1 (AHMED, K), 31 October 2002 (31.10.2002), paragraph [0006] --	1-9
X	EP 0798657 A2 (KK TOSHIBA), 1 October 1997 (01.10.1997), column 3, line 14 - column 7, line 1 --	1-9
X	WO 03015370 A2 (CRYPTOMATHIC A/S), 20 February 2003 (20.02.2003), see the whole document --	1-9

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 Sept 2005	13-09-2005
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Patrik Rydman /mn Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/08/2005

International application No.
PCT/SE 2005/000851

US	4405829	A	20/09/1983	NONE			
US	20020162003	A1	31/10/2002	WO	02088957	A	07/11/2002
EP	0798657	A2	01/10/1997	DE	69702162	D,T	01/03/2001
				JP	9265496	A	07/10/1997
				US	6028940	A	22/02/2000
WO	03015370	A2	20/02/2003	CA	2457493	A	20/02/2003
				CN	1565117	A	12/01/2005
				EP	1364508	A	26/11/2003
				EP	1455503	A	08/09/2004
				GB	0119629	D	00/00/0000
				NO	20033407	A	12/11/2003
				US	20050010758	A	13/01/2005

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW