(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2007-510338
(P2007-510338A)
(43)公表日　平成19年4月19日(2007.4.19)

(51)Int.Cl.	F I	テーマコード（参考）
H04M 3/44 (2006.01)	H04M 3/44	5K201

審査請求 有　予備審査請求 未請求　（全 16 頁）

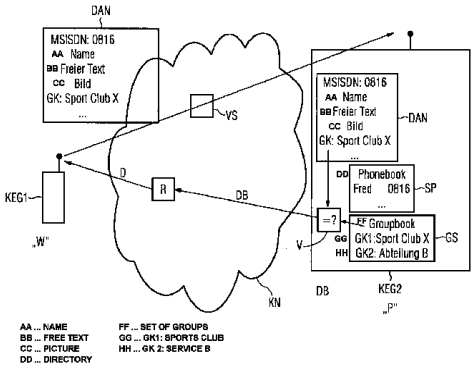
(21)出願番号	特願2006-537054 (P2006-537054)
(86)(22)出願日	平成16年10月26日 (2004.10.26)
(85)翻訳文提出日	平成18年4月27日 (2006.4.27)
(86)国際出願番号	PCT/DE2004/002409
(87)国際公開番号	WO2005/043876
(87)国際公開日	平成17年5月12日 (2005.5.12)
(31)優先権主張番号	10351721.9
(32)優先日	平成15年10月31日 (2003.10.31)
(33)優先権主張国	ドイツ(DE)

(71)出願人　390039413
シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－８０３３３　ミュンヘン　ヴィッテルスバッハープラッツ　２
Ｗｉｔｔｅｌｓｂａｃｈｅｒｐｌａｔｚ　２，　Ｄ－８０３３３　Ｍｕｅｎｃｈｅｎ，　Ｇｅｒｍａｎｙ
(74)代理人　100075166
弁理士　山口　巖

最終頁に続く

(54)【発明の名称】通信加入者のデータの保護された引出し方法

(57)【要約】
本発明は第１の通信加入者によって第２の通信加入者に関係するデータを引出すための方法に関するもので、この方法においては、第１の通信加入者（Ｗ）の第１の通信端末（KEG1）からデータ引出しメッセージ（DAN）が第２の通信加入者（Ｐ）の第２の通信端末（KEG2）に伝送され、その際データ引出しメッセージは、第１の通信加入者に属する通信加入者のグループのグループ識別標識（GK）を含み、第２の通信加入者の第２の通信端末によって、伝送されたグループ識別標識が第２の通信加入者のグループ・メモリ中に記憶されているグループ識別標識と比較され、比較結果が正のときデータが第１の通信端末への伝送のために準備される。



【特許請求の範囲】
【請求項１】
第１の通信加入者（Ｗ）によって第２の通信加入者（Ｐ）に関係するデータを引出すための方法において、
第１の通信加入者（Ｗ）の第１の通信端末（KEG1）からデータ引出しメッセージ（DAN）が第２の通信加入者（Ｐ）の第２の通信端末（KEG2）に伝送され、その際データ引出しメッセージ（DAN）は第１の通信加入者（Ｗ）に属する通信加入者のグループのグループ識別標識（GK）を含み、
第２の通信加入者（Ｐ）の第２の通信端末（KEG2）によって、伝送されたグループ識別標識（GK）が第２の通信加入者（Ｐ）のグループ・メモリ中に記憶されているグループ識別標識と比較され、
比較結果が正のとき、データ（Ｄ）が第１の通信端末（KEG1）への伝送のために準備される
ことを特徴とするデータの引出し方法。
【請求項２】
比較結果が正のときには、第２の通信端末（KEG2）において接続資格管理メッセージが出力され、
第２の通信端末（KEG2）によって正の接続資格確認メッセージが受け取られるとき初めて、データ（Ｄ）が第１の通信端末（KEG1）への伝送のために準備される
ことを特徴とする請求項１記載の方法。
【請求項３】
データ引出しメッセージ（DAN）と共に、さらに加えて第１の通信加入者（Ｗ）の識別子（MSISDN）が第２の通信端末（KEG2）に伝送され、
第２の通信端末（KEG2）によって、さらに加えて伝送された識別子（MSISDN）が第２の通信加入者（Ｐ）のメモリ（SP）中に記憶されている識別子と比較され、
この第２の比較においても正の比較結果が存在するときのみデータ（Ｄ）が第１の通信端末（KEG1）への伝送のために準備される
ことを特徴とする請求項１又は２記載の方法。
【請求項４】
第２の通信端末（KEG2）において、第２の比較の際、負の比較結果が存在するときは接続資格引出しメッセージが出力され、
第２の通信端末（KEG2）によって正の接続資格応答メッセージが受け取られるとき初めて、データ（Ｄ）が第１の通信端末（KEG1）への伝送のために準備される
ことを特徴とする請求項３記載の方法。
【請求項５】
第１の通信端末（KEG1）によって、データ引出しメッセージ（DAN´）が第１の通信加入者（Ｗ）の秘密鍵により署名され、
第２の通信端末（KEG2）によって、第１の通信加入者（Ｗ）の公開鍵を用いてデータ引出しメッセージ（DAN´）の真正性が検査され、
真正のときのみ、データ（Ｄ）が第１の通信端末（KEG1）への伝送のために準備される
ことを特徴とする請求項１～４のいずれか１つに記載の方法。
【請求項６】
第２の通信端末（KEG2）によって、第１の通信加入者（Ｗ）の公開鍵がグループに属する鍵サーバ（PKI）から引出されることを特徴とする請求項５記載の方法。
【請求項７】
第２の通信端末（KEG2）によって、第１の通信加入者（Ｗ）の公開鍵が通信ネットワークのサービス業者によって営まれる鍵サーバから引出され、通信ネットワークを用いてデータ引出しメッセージ（DAN´）が第１の通信端末（KEG1）から第２の通信端末（KEG2）へ伝送されることを特徴とする請求項５記載の方法。
【請求項８】

第２の通信端末（KEG2）によって、第１の通信加入者（Ｗ）の公開鍵が通信ネットワークのサービス業者によって営まれるプロキシ・サーバから引出され、通信ネットワークを介して第１の通信端末（KEG1）と第２の通信端末（KEG2）との間の通信が行われ、その際プロキシ・サーバにおいて多数の通信加入者の公開鍵が一時的に記憶されていることを特徴とする請求項５記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、第１の通信加入者によって、第２の通信加入者に関係するデータを引出すための方法に関する。

【０００２】

通信ネットワークにおける近代的なサービスを実施する場合には、第２の通信加入者に関係するデータが第１の通信加入者の引出しに応じてこの第１の通信加入者に伝送されることがしばしば望ましいか、またはそれどころか必要である。そのようなデータとしては、第２の加入者の（データ保護権的に敏感な）個人的データ、例えば加入者の目下の所在地（例えば都市、市区、通り）、加入者の目下の行動に関する（例えば労働についての、会議、休暇においての）データ、又は電子式通信方法への加入者の目下の加入（例えばテーマ「魚釣り」についてのチャットに申し込まれている、インターネット戦略プレイへの目下の加入）に関するデータが問題となり得る。そのようなデータは、時に「プレゼンス・データともいわれ、「プレゼンス・サービス」によって集められ再配分される。これらのデータは第２の通信加入者に関する個人的な情報を含むから、これらのデータへのアクセスを制限することが望ましい。

【０００３】

本発明の課題は、第２の通信加入者に関係するデータへのアクセスの管理を行い得る方法を提供することにある。

【０００４】

この課題は本発明によれば、第１の通信加入者により第２の通信加入者に関係するデータを引出すための方法において、第１の通信加入者の通信端末から第２の通信加入者の通信端末にデータ引出しメッセージが伝送され、このデータ引出しメッセージは第１の通信加入者に所属する通信加入者のグループのグループ識別標識を含み、第２の通信加入者の第２の通信端末によって、伝送されたグループ識別標識が第２の通信加入者のグループ・メモリ中に記憶されているグループ識別標識と比較され、その比較結果が正の場合にはデータが第１の通信端末への伝送のために準備される。第１の通信加入者に所属するグループには、例えばスポーツクラブ、クラス、ゼミナールグループ、又は第１の通信加入者が所属する企業の部門が対象となり得る。データは、第１の通信端末のデータ引出しメッセージに応じて、第２の通信端末のグループ・メモリに既に記憶されているそのようなグループ識別標識がデータ引出しメッセージにより共に伝送される場合にのみ第１の通信端末に伝送するために準備されるのが有利である。それによって、グループに対する知識を有しまた相応のグループ識別標識を自由に使用できるそのような通信端末（ないしこの通信端末を使用する通信加入者）上のデータへのアクセスが制限される。対応するグループ識別標識を持たない、またそれ故このグループ識別標識をデータ引出しメッセージによって伝達し得ない通信端末には、データへのアクセスが禁じられる。即ちデータはそのような通信端末への伝送のためには準備されない。

【０００５】

本発明による方法は、第２の通信端末において正の比較結果が生じたとき接続資格管理メッセージが出力され、第２の通信端末の側で正の接続資格確認メッセージが受け取られるとき初めて、データが第１の通信端末への伝送のために準備されるようにするのも有利である。それによってアクセス管理及び従って不所望のデータ引出しに対する信頼性がなおいっそう顕著に改善される。何故なら、引出されるデータは、正の比較結果に加えて正の接続資格確認メッセージが第２の通信端末に存在する場合にのみ伝送のために準備され

るからである。

【０００６】

本発明による方法は、データ引出しメッセージによりさらに加えて第１の通信加入者の識別子が第２の通信端末へ伝送され、第２の通信端末によってさらに加えて伝送された識別子が第２の通信加入者のメモリに記憶されている識別子と比較され、この第２の比較においても正の比較結果が存在する場合にのみデータが第１の通信端末への伝送のために準備されるように行われることが可能である。第２の通信加入者のメモリとしては、例えば第２の通信加入者の移動電話の「電話帳メモリ」を対象にすることができる。この方法においては、データアクセスのさらに強い管理を行うことができる。何故なら、グループ識別標識と記憶されたグループ識別標識との一致のほかに、さらに伝送された識別子と第２の通信加入者のメモリ中に記憶された識別子との一致が調べられるからである。第１の通信加入者の識別子が第２の通信加入者のメモリ中に既に保存されている場合にのみデータは伝送のために準備される、即ちこの場合のみデータへのアクセスが可能である。

【０００７】

本発明による方法は、第２の比較において負の比較結果が存在する場合には、第２の通信端末において接続資格引出しメッセージが出力され、第２の通信端末の側で正の接続資格応答メッセージが受け取られるとき初めてデータは第１の通信端末への伝送のために準備されるように有利に形成することもできる。本発明による方法のこの実施形態においては、第１の通信加入者の識別子が第２の通信加入者のメモリ中に記憶されていない場合でさえデータへのアクセスを得ることが第１の通信端末に有利に可能となる。その場合データ保護を維持するため、第２の通信端末側から接続資格引出しメッセージが出力される。即ち引出されるデータは、第２の通信端末によって正の接続資格応答メッセージが受け取られるときのみ第１の通信端末への伝送のために準備される。そのような正の接続資格応答メッセージによって、データ準備のためのはっきり表明された同意が与えられ得る。

【０００８】

本発明による方法は次のように行われることが可能である。即ち、第１の通信端末によりデータ引出しメッセージが第１の通信加入者の秘密鍵により署名され、第２の通信端末により第１の通信加入者の公開鍵を用いてデータ引出しメッセージの真正性が調べられ、真正である場合にのみデータは第１の通信端末への伝送のために準備される。この形をとる場合には本発明によれば特に信頼できる方法が達成される。何故なら、第１の通信加入者の個人鍵による署名及び第１の通信加入者の公開鍵を用いたデータ引出しメッセージの真正性の調査によって、データ引出しメッセージが実際に第１の通信加入者の第１の通信端末により造られたことが保障されるからである。従って、第３の通信端末が権利なしに第１の通信端末であるとの偽りの申し立てをなし得るようなことは有利に回避される。

【０００９】

本発明による方法においては、第２の通信端末によって、第１の通信加入者の公開鍵がグループに属する鍵サーバから引出され得る。それによって、グループメンバー（ないしはそれらの通信端末）の公開鍵をこのグループの独特の鍵サーバへ中央に集めるように記憶させることが可能である。グループに属する鍵サーバにはグループに所属する通信加入者の公開鍵のみが保存されているから、よそのグループの通信加入者の通信端末は簡単且つ有効なやり方でデータへのアクセスを阻まれる。何故ならこれらのデータはそのような通信端末に対しては準備されないからである。

【００１０】

本方法はまた次のように行われることも可能である。即ち、第２の通信端末によって、第１の通信加入者の公開鍵が通信ネットワークのサービス業者によって営まれる鍵サーバから引出され、ネットワークを使用してデータ引出しメッセージが第１の通信端末から第２の通信端末へ伝送される。本発明による方法のこの構成形態においては、公開鍵は通信ネットワーク・サービス業者の中央で管理されている鍵サーバから有利に引出され得るので、通信加入者にとって特に費用少なく本方法を実行し得る代替案がもたらされる。

【００１１】

本発明に従う方法は次のように有利に行われることが可能である。即ち、第２の通信端末によって、第１の通信加入者の公開鍵が通信ネットワークのサービス業者によって営まれるプロキシ・サーバから引出され、通信ネットワークを介して第１の通信端末と第２の通信端末との間の通信が行われ、その際プロキシ・サーバにおいては多数の通信加入者の公開鍵が一時的に記憶される。本発明に従う方法のこの構成形態では、鍵が有利にプロキシ・サーバから引出され、プロキシ・サーバには（例えばそれまでの過程において）それまでにこの過程に関与した通信加入者の公開鍵が一時的に記憶される。そのようなプロキシ・サーバは従って通信ネットワークの自動的に実現する鍵サーバを形成する。

【００１２】

次に本発明を図について説明する。

【００１３】

図１には通信ネットワークＫＮが概略的に示され、このネットワークにおいては移動無線ネットワーク（例えばGSM(Global System for Mobile Communication)又はUMTS(Universal Mobile Telecommunications System)）が問題となっている。しかし本発明方法は移動無線ネットワークの集合に限定されるものではなく、通信ネットワークＫＮとして同様に固定電話ネットワーク（例えばISDNネットワーク）又はコンピュータ・ネットワーク（例えばインターネット）も問題とすることができる。通信ネットワークＫＮについてはただ電話交換局ＶＳ（実施例では移動体交換局(Mobile Switching Center＝MSC)が扱われている）と計算機Ｒ（以下に詳細に説明される）が示されている。通信ネットワークＫＮはネットワーク・オペレータによって管理される。通信ネットワークとは、第１の通信加入者Ｗの第１の通信端末KEG1及び第２の通信加入者Ｐの第２の通信端末KEG2が結合される。第１の通信加入者Ｗのためにその通信端末KEG1によって第２の通信加入者Ｐに関係するデータが引出されようとするものである。そのような第１の通信加入者Ｗは時に「ウオッチャー」と呼ばれ、そのような第２の通信加入者Ｐは「プレゼンター」又は「プレゼンティティ」と呼ばれる。第１の通信端末KEG1と第２の通信端末KEG2として実施例では移動電話が扱われる。他の実施例ではそのような通信端末として、例えば固定ネットワーク電話、インターネット・コンピュータ、又は移動無線インタフェースを持った携帯型計算機も扱うことができる。

【００１４】

移動電話KEG1と通信ネットワークＫＮとの間、移動電話KEG2と通信ネットワークＫＮとの間には、通常のようにいわゆるエアー・インタフェース及びベースステーション（図示されず）を介して通信接続が作り上げられる。即ちそれによってメッセージが例えば第１の通信端末KEG1から第２の通信端末KEG2に伝送され得る。

【００１５】

まず最初に、第１の通信加入者Ｗの第１の通信端末KEG1からデータ引出しメッセージDANが通信ネットワークＫＮの交換局VSを介して第２の通信加入者Ｐの第２の通信端末KEG2に伝送される。このデータ引出しメッセージDANは、具体的に引出すべきデータ（例えば第２の通信加入者Ｐの現所在地及び目下の活動）の指示のほかに、第１の通信加入者Ｗの識別子（この場合第１の通信端末KEG1の移動無線呼出し番号MSISDN）及びグループ識別標識GK（この場合第１の通信加入者Ｗがメンバーであるスポーツクラブのグループ識別標識「スポーツクラブＸ」）を含む。さらに、データ引出しメッセージDANは（オプションで）第１の通信加入者の名前及び画像並びに通信加入者によって任意に選ばれたテキスト（自由テキスト）を含む。このデータ引出しメッセージDANは交換局VSを介して第２の通信端末KEG2に伝送される。第２の通信端末KEG2は、データ引出しメッセージDANを用いてデータが引出されるところの通信加入者Ｐに属している。第２の通信端末KEG2はデータ引出しメッセージDANからグループ識別標識GK（「スポーツクラブＸ」）を読み出し、このグループ識別標識を移動電話KEG2のグループ・メモリGS中に既に記憶されているグループ識別標識GK1、GK2等と比較する。移動電話KEG2の比較ユニットＶによって、伝送されたグループ識別標識GK（「スポーツクラブＸ」）がグループ・メモリGS中に既に記憶されているグループ識別標識GK1即ち「スポーツクラブＸ」と一致することが確認される。この一致

に応じて、即ちこの正の比較結果に応じて、データが第１の通信端末KEG1へ伝送するために準備される。

【００１６】

以上に代えて本方法はまた次のようにも行われ得る。即ち、正の比較結果が出てもデータはまだ伝送のためには準備されず、第２の通信端末から接続資格管理メッセージが出力される。この接続資格管理メッセージは、第２の通信端末の表示ユニットに次の表示が出力される結果となる。即ち、「あなたのデータを、呼び出し番号〈MSIDN〉及び画像〈画像〉を有する加入者〈名前〉に実際に伝送しますか？」（その際名前及び画像の出力は必須ではない）。第２の通信加入者Ｐがこの問いに明確に「はい」と答え、移動電話KEG2の相応するボタンを操作すると、第２の通信端末は正の接続資格確認メッセージを受け取る。この正の接続資格確認メッセージに応じて初めて、引出されるデータが第１の通信端末KEG1への伝送のために準備される。接続資格管理メッセージの出力及び接続資格確認メッセージの受取によるこの方法は、引出されるデータの伝送のための「反応的権限付与」ともいわれ得る。何故なら、第２の通信端末KEG2の側から（即ち第２の通信加入者Ｐの側から）具体的なデータ引出しメッセージDANの受領後データ伝送のための許可（確認）が得られるからである。

【００１７】

データの準備は種々の様式で行うことができる。通信端末KEG1によって要求されたデータは、例えば第２の通信端末KEG2に蓄えておくことができ、このデータは正の比較結果が提示されることに応じて、ないしは接続資格確認メッセージが存在することに応じて、第２の通信端末のメモリから読み出され、データ伝送メッセージ（例えばUSSD-String、図示されず）に書き込まれる。従ってデータはデータ伝送メッセージと共に通信ネットワークKNを介して第１の通信端末KEG1に伝送される。

【００１８】

データはまた、正の比較結果に応じて、ないし接続資格確認メッセージの存在に応じて次のように伝送のために準備されることも可能である。即ち、第２の通信端末KEG2からデータ準備信号DBが通信ネットワークKNの計算機Ｒに送られる。この計算機Ｒには引出されるデータが保存されている。データ準備信号DBは、引出されるデータが通信ネットワークKNを介して通信端末KEG1に伝送されるべきであるという情報を含む。従って計算機Ｒはこのデータを（例えばUSSDメッセージを用いて）第１の通信端末KEG1に伝送する。このようなものとしての計算機Ｒは既知であり、「プレゼンス・コンピュータ」又は「プレゼンス・サーバ」といわれる。この計算機は通信ネットワークKNの一部を形成することができ、あるいは通信ネットワークの外に配置され通信ネットワークと結合されることも可能である。

【００１９】

本発明による方法の他の実施形態においては、第２の通信端末KEG2の比較ユニットＶによってさらに加えて第２の比較が行われる。即ち、データ引出しメッセージDANから、第１の通信加入者の識別子MSISDNが読み出され、第２の通信加入者のメモリSPに記憶されている識別子と比較される。この第２の通信加入者のメモリとしては、例えば電話機において既知の電話帳メモリを扱うことができ、このメモリには電話の使用者が折に触れ通信接続を立ち上げるような通信加入者の例えば名前、電話番号MSISDNが保存されている。伝送された識別子もまたメモリSP中に既に保存されている識別子と一致することを比較ユニットＶが確認するときのみ、データは第１の通信端末KEG1への伝送のために準備される。

【００２０】

しかしながらこの第２の比較において、伝送された識別子がメモリSP中に既に保存されている識別子と一致しない（負の比較結果）場合には、第２の通信端末から接続資格引出しメッセージが出力され、このメッセージは第２の通信端末の表示ユニットに次の表示が出力される結果となる。即ち、「あなたのデータを、呼び出し番号〈MSISDN〉及び画像〈画像〉を有する加入者〈名前〉に実際に伝送しますか？」。この際名前及び画像の出力は必ずしも必要ではない。第２の通信加入者Ｐがこの問いに明確に「はい」と答え、移動電

話KEG2の相応するボタンを操作すると、第２の通信端末は正の接続資格応答メッセージを受け取る。この正の接続資格応答メッセージに応じて、引出されるデータは上述の様式の一つに従って第１の通信端末KEG1への伝送のために準備される。接続資格引出しメッセージの出力及び接続資格応答メッセージの受領によるこの方法は、接続資格管理メッセージ及び接続資格確認メッセージによる上述の流れに類似して、引出されるデータの伝送のための「反応的権限付与」を実行する。何故ならここでも第２の通信端末KEG2の側から（即ち第２の通信加入者Ｐの側から）具体的なデータ引出しメッセージDANの受領後データ伝送のための許可が得られるからである。

【００２１】

図２には本発明による方法の流れの他の例が示されている。図１に類似して、図２には通信ネットワークKN、第１の通信加入者Ｗの第１の通信端末KEG1及び第２の通信加入者Ｐの第２の通信端末KEG2が示されている。第１の通信加入者Ｗと第２の通信加入者Ｐとは或るグループのメンバーであり、この場合両者は企業Ｘ（Ｘ社）に属する。第１の通信端末KEG1からデータ引出しメッセージDAN´が第２の通信端末KEG2に送られ、その際データ引出しメッセージDAN´はグループ識別標識GK（Ｘ社）及び移動無線呼出し番号の形の識別子MSISDN（0816）を含む。第１の通信端末KEG1はデータ引出しメッセージDAN´に対し第１の通信加入者Ｗの秘密鍵を用いて署名を作り、この署名をデータ引出しメッセージDAN´に付加する。従って署名はデータ引出しメッセージDAN´によって第２の通信端末KEG2に一緒に伝送される。

【００２２】

第２の通信端末KEG2におけるデータ引出しメッセージDAN´の受領に応じて、比較ユニットＶは図１による方法におけるようにデータ引出しメッセージDAN´により伝送されたグループ識別標識GKを第２の通信端末KEG2のグループ・メモリGSに既に保存されているグループ識別標識と比較し、グループ識別標識「Ｘ社」が既にグループ・メモリGSに保存されていることを確認する。グループ・メモリGSには、加えて、グループ「Ｘ社」に対しデータ引出しメッセージの真正性の検査が一緒に伝送された署名を用いて行われなければならないという情報が保存されている。従って第２の通信端末KEG2はデータ引出しメッセージDAN´から署名を読み出し、第１の通信加入者Ｗの公開鍵を用いて署名されたメッセージDAN´の真正性を調べる。この検査は例えば第２の通信端末KEG2の比較ユニットＶにおいて実施することができ、この比較ユニットは通信端末KEG2のマイクロプロセッサによって形成される。公開鍵を用いてデータ引出しメッセージの真正性が検査されると直ちに、本方法はさらに図１と関連して述べられたように進行し、その結果最後にデータは上述の仕方で第１の通信端末への伝送のために準備される。

【００２３】

この真正性の検査の際に必要な公開鍵は、第２の通信端末KEG2によって、グループの１つに属する（ここでは例えば企業Ｘによって営まれる）鍵サーバPKIから引出すことができる。そのために、公開鍵は鍵サーバPKI（PKI＝Public Key Infrastructure）からネットワーク・サービス業者/ネットワーク・オペレータの計算機OPを介して第２の通信端末KEG2に伝送される。このことは図２の下部に破線矢印で示されている。

【００２４】

代替の実施形態においては、公開鍵は通信ネットワークKNのネットワーク・サービス業者/ネットワーク・オペレータによって営まれる鍵サーバから引出されることも可能である。この場合には、鍵サーバPKIは例えばネットワーク・サービス業者の計算機OPに直接配置されることになろう。

【００２５】

本発明の第３の実施形態においては、ネットワーク・サービス業者の計算機OPはプロキシ・サーバとして働き、このサーバは第２の通信端末KEG2の引出しに応じて公開鍵を第２の通信端末KEG2に伝送する。プロキシ・サーバOPには通信加入者の多数の公開鍵が一時的に記憶されている。その際本発明による方法の既に完結された方法経過において通信ネットワークKNを介して伝送されている公開鍵が問題となる。第１の通信加入者Ｗの公開鍵が

プロキシ・サーバOPに蓄えられていない場合には、プロキシ・サーバOPはその側でこの公開鍵を企業「Ｘ社」の鍵サーバPKIから引出し、公開鍵を第２の通信端末KEG2へ転送する。このことは図２の下部に破線矢印で示されている。Ｘ社の鍵サーバPKIへのアクセスは、例えば、データ伝送プロトコル“hypertext transfer protocol security”（HTTPS）を用いて保護されたインターネットアクセスを介して行うことができる。

【図面の簡単な説明】

【００２６】

【図１】本発明による方法の流れを示す実施例である。

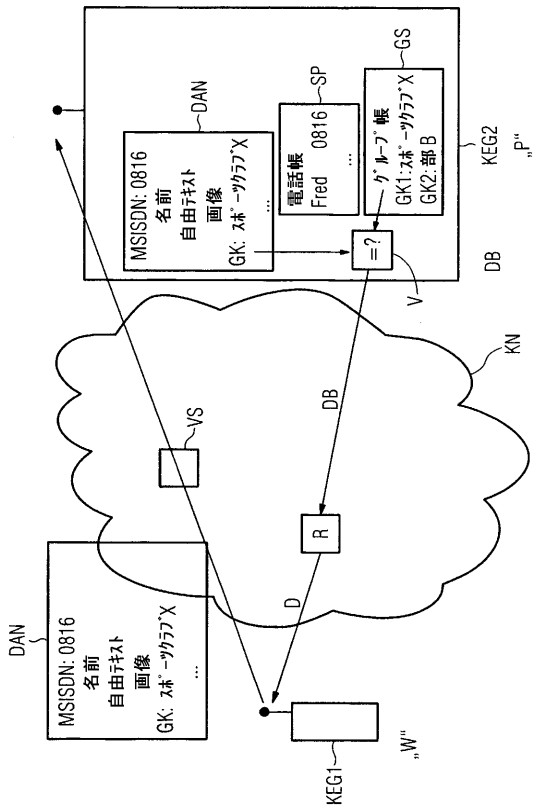
【図２】本発明による方法の流れを示す異なる実施例である。

【符号の説明】

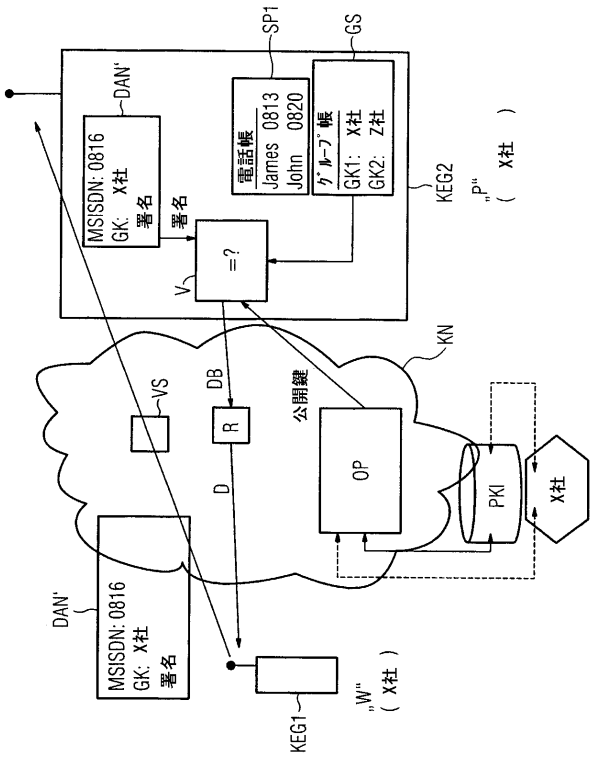
【００２７】

KN　ネットワーク
VS　交換局
Ｒ　計算機
Ｄ　データ
DB　データ準備信号
Ｗ　第１の通信加入者
KEG1　第１の通信端末
Ｐ　第２の通信加入者
KEG2　第２の通信端末
DAN、DAN´　データ引出しメッセージ
SP　メモリ
GK　グループ識別標識
GS　グループ・メモリ
PKI　鍵サーバ
OP　計算機（プロキシ・サーバ）

【図１】


DAN
MSISDN: 0816
名前
自由テキスト
画像
GK: ｽﾏﾎﾞｰﾂｸﾗﾌﾞX
...
電話帳
Fred 0816
...
ｸﾞﾙｰﾌﾟ帳
GK1: ｽﾏﾎﾞｰﾂｸﾗﾌﾞX
GK2: 部 B
GS
SP
KEG2
„P"
DB
=?
V
KN
VS
DB
R
D
DAN
MSISDN: 0816
名前
自由テキスト
画像
GK: ｽﾏﾎﾞｰﾂｸﾗﾌﾞX
...
KEG1
„W"

【図２】


SP1
GS
DAN'
MSISDN: 0816
GK: X社
署名
電話帳
James 0813
John 0820
ｸﾞﾙｰﾌﾟ帳
GK1: X社
GK2: Z社
KEG2
„P"
(X社)
署名
=?
V
KN
VS
DB
R
D
公開鍵
OP
PKI
X社
DAN'
MSISDN: 0816
GK: X社
署名
KEG1
„W"
(X社)

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE2004/002409

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04M3/493 H04M1/663 G06F1/00

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)
IPC 7 H04M G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/152265 A1 (FELMAN HILLEL) 17 October 2002 (2002-10-17)	1-4
Y	paragraph '0011! - paragraph '0017! paragraph '0034! - paragraph '0035! paragraph '0042! - paragraph '0046! paragraph '0050! paragraph '0089! - paragraph '0095! figures 16,17 abstract	5-8
Y	DE 101 18 794 A1 (DEUTSCHE TELEKOM AG; SAP AG) 17 October 2002 (2002-10-17) paragraph '0002! paragraph '0010! - paragraph '0011!	5-8

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in 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 document 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
24 February 2005	02/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Schorgg, A

1

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE2004/002409

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 179 950 A (NEC CORPORATION) 13 February 2002 (2002-02-13) paragraph '0002! - paragraph '0003! paragraph '0008! - paragraph '0009! figure 2	1

1

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE2004/002409

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002152265 A1	17-10-2002	NONE	
DE 10118794 A1	17-10-2002	WO 02086683 A2	31-10-2002
		EP 1384130 A2	28-01-2004
EP 1179950 A	13-02-2002	JP 2002057807 A	22-02-2002
		CA 2354806 A1	08-02-2002
		CN 1337816 A	27-02-2002
		EP 1179950 A2	13-02-2002
		US 2002019225 A1	14-02-2002

Form PCT/ISA/210 (patent family annex) (January 2004)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2004/002409

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04M3/493 H04M1/663 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04M G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2002/152265 A1 (FELMAN HILLEL) 17. Oktober 2002 (2002-10-17)	1-4
Y	Absatz '0011! - Absatz '0017! Absatz '0034! - Absatz '0035! Absatz '0042! - Absatz '0046! Absatz '0050! Absatz '0089! - Absatz '0095! Abbildungen 16,17 Zusammenfassung	5-8
Y	DE 101 18 794 A1 (DEUTSCHE TELEKOM AG; SAP AG) 17. Oktober 2002 (2002-10-17) Absatz '0002! Absatz '0010! - Absatz '0011!	5-8

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
'A' Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
'E' älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
'L' Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
'O' Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
'P' Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
'T' Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
'X' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
'Y' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
'&' Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
24. Februar 2005	02/03/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schorgg, A

1

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2004/002409

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 1 179 950 A (NEC CORPORATION) 13. Februar 2002 (2002-02-13) Absatz '0002! - Absatz '0003! Absatz '0008! - Absatz '0009! Abbildung 2	1

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2004/002409

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 2002152265	A1	17-10-2002	KEINE		
DE 10118794	A1	17-10-2002	WO	02086683 A2	31-10-2002
			EP	1384130 A2	28-01-2004
EP 1179950	A	13-02-2002	JP	2002057807 A	22-02-2002
			CA	2354806 A1	08-02-2002
			CN	1337816 A	27-02-2002
			EP	1179950 A2	13-02-2002
			US	2002019225 A1	14-02-2002

Formblatt PCT/ISA/210 (Anhang Patentfamilie) (Januar 2004)

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,IT,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,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 アンデルセン、フランクーウヴェ
ドイツ連邦共和国 １０６２５ ベルリン マリーーエリザベートーリューダースーシュトラーセ 7
(72)発明者 ハウプトフォーゲル、アンドレアス
ドイツ連邦共和国 １２１０３ ベルリン ゼノックシュトラーセ ２９
(72)発明者 リューデ、トーマス
ドイツ連邦共和国 １２１６９ ベルリン アルトマルクシュトラーセ ３ アー

Ｆターム(参考) 5K201 AA08 AA09 CA04 CB05 CB09 CB13 DC03 EC06 ED05 EE08