

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4753521号

(P4753521)

(45) 発行日 平成23年8月24日(2011.8.24)

(24) 登録日 平成23年6月3日(2011.6.3)

(51) Int.Cl.		F I
H02J 13/00	(2006.01)	H02J 13/00 311C
H04Q 9/00	(2006.01)	H04Q 9/00 301D
H04Q 9/14	(2006.01)	H04Q 9/00 311A
		H04Q 9/14 K

請求項の数 15 (全 24 頁)

(21) 出願番号	特願2001-577682 (P2001-577682)	(73) 特許権者	500394214
(86) (22) 出願日	平成13年4月17日 (2001.4.17)		エレクトリシテ ド フランス (ソシエ テ アノニム)
(65) 公表番号	特表2004-504791 (P2004-504791A)		ELECTRICITE DE FRAN CE (SOCIETE ANONYME)
(43) 公表日	平成16年2月12日 (2004.2.12)		フランス国 エフー75008 パリ ア ヴェニュー ド ヴァグラム 22-30
(86) 国際出願番号	PCT/FR2001/001173		
(87) 国際公開番号	W02001/080398	(74) 代理人	100123788
(87) 国際公開日	平成13年10月25日 (2001.10.25)		弁理士 宮崎 昭夫
審査請求日	平成20年4月14日 (2008.4.14)	(74) 代理人	100106138
(31) 優先権主張番号	00/05037		弁理士 石橋 政幸
(32) 優先日	平成12年4月19日 (2000.4.19)	(74) 代理人	100127454
(33) 優先権主張国	フランス (FR)		弁理士 緒方 雅昭

最終頁に続く

(54) 【発明の名称】 ネットワークに接続されている電気装置の許可をモニタする方法および装置

(57) 【特許請求の範囲】

【請求項1】

情報メッセージの受信器を装備されていて、かつ、ネットワークに接続されている電気装置の許可を、情報メッセージの特殊化されている送信器を基にしてモニタする方法において、

- ー 許可モニタ・コードに依存している少なくとも1つの符号化されている許可情報項目を含んでいる符号化されている情報メッセージを、特殊化されている送信器から前記電気装置へ送ることと、
 - ー 前記電気装置に装備されている前記受信器により前記情報メッセージを受信することと、
 - ー 復号された許可情報を発生するように、前記符号化された情報メッセージを、前記受信器に組込まれている特定の許可データの関数として復号することと、
 - ー 前記復号された許可情報が前記組込まれている特定の許可データを満たしたならば前記電気装置の許可を指令することと、
 - ー 満たさなければ前記電気装置を許可しないことを指令することとを、
- 有し、

各メッセージは署名され、署名されている各メッセージは、署名が検証された時に、検証されて復号された前記許可情報が前記組込まれている特定の許可データを満たすかどうかを判定可能にする、署名されている認証データのデータ・フィールドを備えている

ことを特徴とする電気装置の許可をモニタする方法。

【請求項 2】

前記許可モニタ・コードが、許可モニタ区域に属している前記電気装置の地理学的場所を表す数値を含んでいる少なくとも 1 つのフィールドを備えていることを特徴とする、請求項 1 に記載の方法。

【請求項 3】

前記許可モニタ・コードが、ユーザーによって署名されていることを表す数値を含んでいる少なくとも 1 つのフィールドを備えていることを特徴とする、請求項 1 または請求項 2 に記載の方法。

【請求項 4】

前記符号化された情報メッセージを前記電気装置へ定期的に送ることを特徴とする、請求項 1 から請求項 3 のいずれか 1 項に記載の方法。

10

【請求項 5】

前記ネットワークが、群ローカル・コンピュータ・ネットワークと、拡張されているコンピュータ・ネットワークと、ローカル・ヘルツネットワークと、セルラー無線電話ネットワークと、搬送波電流によってメッセージを送るようにされている配電ネットワークとからのネットワークの 1 つより成ることを特徴とする、請求項 1 から請求項 4 のいずれか 1 項に記載の方法。

【請求項 6】

各情報メッセージが前記電気装置の許可の期間を表す少なくとも 1 つのデータ・フィールドを備えていることを特徴とする、請求項 1 から請求項 5 のいずれか 1 項に記載の方法。

20

【請求項 7】

前記認証データが、詐欺的応答を避けることを可能にする少なくとも 1 つの単調に増加する時間依存値を備えていることを特徴とする、請求項 1 から 6 のいずれか 1 項に記載の方法。

【請求項 8】

— 前記組込まれている特定の許可データを少なくとも備えている開始メッセージを前記特殊化されている送信器から前記受信器へ送るステップと、
— 前記受信器の要求があると、前記送信器から前記受信器へ許可モニタ除去メッセージを送り、前記受信器は、前記許可モニタ除去メッセージを受け取ると、制約されていない動作にリセットされるステップと、
— 前記電気装置の不可欠な機能のいずれかを不能にさせるオンサイト・ブロッキング・メッセージを、モニタ周辺に属していて、このモニタ周辺の監視を確実にする第三者要素の要求があった時に、前記受信器へ送るステップと、
— 前記送信器の認証のためのメッセージを前記受信器へ定期的に送るステップと、
— 前記受信器の識別コードを備えている忠誠メッセージを前記受信器から前記送信器へ送るステップと、
— 前記送信器による前記忠誠メッセージの検証が無い時に、前記受信器の動作停止固定を指令するメッセージを、前記送信器から前記受信器へ送るステップと、
を少なくとも含んでいる、モニタする方法を管理するためのステップを更に備えていることを特徴とする、請求項 1 から請求項 7 のいずれか 1 項に記載の方法。

30

40

【請求項 9】

搬送波電流による情報メッセージの送りが装備されている配電ネットワークに対して、前記送信器が HT/LT 変圧器、需用者の建物における電力量計などのこのネットワークの場所に置かれることを特徴とする、請求項 1 から請求項 8 のいずれか 1 項に記載の方法。

【請求項 10】

前記情報メッセージが、HT/LT 変圧器または電力量計の識別コードを表す少なくとも 1 つのデータ・フィールドを備えていることを特徴とする、請求項 9 に記載の方法。

【請求項 11】

50

前記情報メッセージが前記電力量計の測定値を表す少なくとも1つのデータ・フィールドを備えていることを特徴とする、請求項9または10に記載の方法。

【請求項12】

情報メッセージの受信器を装備されていて、かつ、ネットワークに接続されている電気装置の許可を、モニタする方法を実施する特殊化されている送信器装置であって、この特殊化されている送信器装置は、許可モニタ・コードに依存している少なくとも1つの符号化されている電気装置の許可情報項目を含んでいる符号化されている情報メッセージを、この電気装置へ送ることを許すようにされており、

- 少なくとも1台の電気装置に組合わされている許可モニタ・コードを計算する手段と、
 - この許可モニタ・コードに依存している前記符号化されている許可情報項目を含んでいる符号化されている情報メッセージを前記ネットワーク上に送る手段と、
- を少なくとも備え、

各メッセージは署名され、署名されている各メッセージは、署名が検証された時に、検証されて復号された前記許可情報が前記組込まれている特定の許可データを満たすかどうかを判定可能にする、署名されている認証データのデータ・フィールドを備えている、

ことを特徴とする、請求項1から請求項11のいずれか1項に記載の方法を実施する特殊化されている送信器装置。

【請求項13】

- 流体またはエネルギーの外部測定のための装置に前記装置を相互に接続できるようにする外部コンピュータ・ソケットと、
 - 該外部コンピュータ・ソケットと前記許可モニタ・コードを計算する手段との間に相互接続されている結合モジュールと、
- を更に備え、前記許可モニタ・コードを計算する手段は前記許可モニタ・コードを符号化することを可能にする測定情報項目を前記流体またはエネルギーの外部測定のための装置から受けることを特徴とする、請求項12に記載の装置。

【請求項14】

ネットワークに接続されている電気装置を装備していて、特殊化されている送信器により送信された、この電気装置のための少なくとも1つの符号化された許可情報項目を含んでいる符号化された情報メッセージを受信する受信器装置であって、

- 前記符号化された情報メッセージを受信する手段と、
 - 前記符号化された許可情報項目を復号して検証する手段と、
 - 前記符号化された許可情報項目の検証の関数として前記電気装置のそれぞれ許可と不許可を指令する手段と、
- を少なくとも備え、

各メッセージは署名され、署名されている各メッセージは、署名が検証された時に、検証されて復号された前記許可情報が前記組込まれている特定の許可データを満たすかどうかを判定可能にする、署名されている認証データのデータ・フィールドを備えている、

ことを特徴とする、請求項1から請求項11のいずれか1項に記載の方法を実施する受信器装置。

【請求項15】

特殊化されている送信器の前記情報メッセージを送る手段に受信器が装備され、電気装置に組合わされている受信器の前記情報メッセージを受信する手段に送信器が装備され、前記特殊化されている送信器と前記電気装置に組合わされている前記受信器との間の通信が双方向であることを特徴とする、請求項12から請求項14のいずれか1項に記載の受信器装置。

【発明の詳細な説明】

【0001】

(技術分野)

本発明は、ネットワークに接続され、または結合されている電気装置の許可をモニタする

10

20

30

40

50

方法および装置に関する。

【0002】

(背景技術)

現在、電気機器はかつてないほど多くの多様な機能の実行またはサービス提供を確実に行うようになっている。

【0003】

特にこの電気機器が、テレビジョン受像機、ビデオ録画機、ハイファイなどの家庭用什器、または冷蔵庫、洗濯機、皿洗い機またはその他の種類の物などの白物家電と呼ばれる家庭用電気機器、あるいはマイクロコンピュータ、およびその周辺機器、プリンタ等などの事務用または家庭用の電気装置で構成されている場合に特にそうである。

10

【0004】

各使用者にとってかなりの財産価値を表す、それら全ての装置に対して、許可という概念は、各装置が意図されている機能またはサービス提供の実行のための契約の始まりの許可の概念のみならず、関連する装置の法的な管理人のためにこの機能の実行またはこのサービス提供のために法律を根拠とする許可の概念も包含するが、この装置を盗んだ侵入者のためではなくて、場合に応じて、この装置に関連するサービス提供へのアクセス権も包含する。

【0005】

(発明の開示)

本発明の目的は、監視周辺内の指定されている場所における、ネットワークに接続されている電気装置の位置の監視のために、特に、機能の実行を許す、電気装置の許可をモニタする方法および装置を実現することであって、この装置の使用の許可は、後者がこの監視周辺内の前記指定されている場所に配置されている時にこの装置に与えられ、配置されていなければこの装置の使用不許可が後者に与えられる。一般に、電気装置が接続されているネットワークの概念は、一方では、通信ネットワークを含み、他方では、電気エネルギーの配電網または送電網を含むことが示されている。したがって、通信ネットワークの概念は、電気装置と、ATMネットワークまたはインターネット・ネットワーク、特にGSMネットワークなどの指定された場所との間のメッセージの交換を確実にすることを可能にするいかなる種類のネットワークも含む。

20

【0006】

同様に、電気装置のための電気エネルギーの配電網または送電網の概念は、メーターの下流の、家庭用配電網と、メーターの上流の配電網とを含む。

30

【0007】

更に、電気エネルギーの配電網または送電網で発生された搬送波電流による通信の技術が使用される時は、この電気エネルギーの配電網または送電網は、更に、通信ネットワークを構成する。

【0008】

本発明の他の目的は、また、サービス提供を期待して使用する1つまたは複数の契約引受けに関する電気装置の使用を監視するため機能の実行を更に許す、この電気装置の許可をモニタする方法および装置を実現することである。引受けはそのような設備によって利益を受けるために許可されているユーザーと、任意の許可実体、すなわち、この引受けまたはそれらの引受けの供与者との間で結ばれ、この装置の使用の許可は、この使用が末尾に署名されている契約引受けを満たす時に後者に与えられ、さもなければこの装置の使用の不許可が後者に与えられる。

40

【0009】

本発明の主題であるモニタ法およびモニタ装置の考え得る応用のうちで、ネットワークに接続されている電気装置の特に盗難防止と、オンライン・サービスへのアクセスのモニタ、特に出資の支払い時またはある時間スロット内で、中央場所に関して遠方にあるサービス提供とについて述べることができる。

【0010】

50

本発明の主題である、ネットワークに接続されている電気装置の許可をモニタする方法は、情報メッセージの特殊化されている送信器を基にして実現され、許可されている電気装置には情報メッセージの受信器が装備されている。

【0011】

本発明の方法は、許可モニタ・コードに依存している少なくとも1つの符号化された許可情報項目を含んでいる符号化された情報メッセージを、特殊化されている送信器から電気装置へ送ることと、この情報メッセージを電気装置に装備されている受信器によって受けることと、復号された許可情報を発生するようにこの符号化された情報メッセージを受信器に組込まれている特定の許可データの関数として復号することと、組込まれている特定の許可データを復号された許可情報が満たすならばこの電気装置の許可を指令することと、さもなければこの電気装置を許可しないことを指令すること、を有し、各メッセージは署名され、署名されている各メッセージは、署名が検証された時に、検証されて復号された前記許可情報が前記組込まれている特定の許可データを満たすかどうかを判定可能にする、署名されている認証データのデータ・フィールドを備えていることことに注目すべきである。

10

【0012】

本発明の主題である、ネットワークに接続されている電気装置の許可をモニタする方法および装置は、説明を読み、以下の図面を見るとより良く理解されるであろう。

【0013】

(発明を実施するための最良の形態)

20

ネットワークに接続されている電気装置の許可をモニタする本発明の方法またはプロトコルを図1および引き続く図面に関連して以下に説明する。

【0014】

一般的なやり方で、本発明の主題である方法は、ネットワークに接続されており、かつもちろん動作モードにある、電気装置の許可の全ての概念を包含し、この電気装置の場所を監視する機能の実行、またはサービス提供の目的で1つまたは複数の契約の引受けまたは使用諸条件に関してこの電気装置の監視機能の実行を行えるようにし、この電気装置の使用許可が末尾に署名されている契約引受けを満たす時に後者と協議され、逆の場合にはこの装置の不許可が後者と協議されることが示されている。本発明の主題である、電気装置の許可をモニタする方法の実現のために、この方法は特定の特殊化されている送信器を基にして実現できるが、電気装置には情報メッセージの受信器と、かつ場合に応じて、前記特殊化されている送信器への応答メッセージの送りを確実に可能にする再送信器とが装備されており、特殊化されている送信器とデータ処理装置、およびもちろん情報メッセージの受信器ならびに再送信器は1つの同じネットワークに接続されていることが示されている。

30

【0015】

ネットワークというのは、任意の種類の通信ネットワーク、特に、ローカル・コンピュータ・ネットワークと、拡張されているコンピュータ・ネットワークと、ローカル・ヘルツネットワークと、セルラー無線電話ネットワークと、もちろん非限定的に、低電圧搬送波電流によるメッセージの送信を備えている電気エネルギー配電ネットワークとを意味するものと理解される。

40

【0016】

前記通信ネットワークは、本発明の主題である方法の実現によって、許可された任意のモニタ実体と、情報メッセージの受信器を装備されている電気装置の少なくとも1つとの間のメッセージ交換と、またもちろん本発明の主題である方法の実現を行えるようにする情報メッセージの特殊化されている送信器とのメッセージ交換を可能にすることが理解される。

【0017】

以下のもの、すなわち、場合に応じて再送信器またはローカル化された送信器E Lが設けられている受信器Rと、特殊化されている送信器E Sとを含んでいる電気装置E Aを使用

50

できることが示されている図1を参照する。それらは前記通信ネットワークによって接続されている。

【0018】

それらの条件の下で、本発明の主題である方法は、ステップAで、特殊化されている送信器から電気装置EAへ、許可モニタ・コードに依存する少なくとも1つの符号化された情報メッセージMIを電気装置EAへ送ることと、その後で、ステップBで、受信器Rのレベルで、後者により、前記符号化された情報メッセージMIを受けることとにある。

【0019】

ステップBの後にステップCが続く。ステップCは、受信器Rのレベルにおいて、特定の許可データの関数として受信器Rに組込まれている符号化された情報メッセージMIを、符号化された許可情報を発生するように、復号することにある。この復号された許可情報はDISと示されている。

10

【0020】

ステップC自体の後に、受信器Rの、したがって、電気装置EAのレベルにおいて、復号された情報DISが受信器Rに組込まれている特定の許可データDSと同一であることを検証することにある試験手順Dが続く。試験Dに対して肯定応答がされると、電気装置EAの許可がステップEで行われる。試験Dに対して否定応答がされると、電気装置EAの不許可がステップFで行われる。

【0021】

許可モニタ・コード、この許可モニタ・コードはたとえばモニタまたは監視する周辺すなわち区域を定義することを可能にする、の関数として符号化された許可情報に関連する種々の指示について、図2aを参照して以下に説明する。

20

【0022】

モニタ区域の概念、または場合に応じて許可モニタ周辺の概念は、ハードウェア的に限られていないで、所与の電気装置に割当てられている1組のモニタ・コードによって少なくとも定められる区域として理解すべきである。この電気装置は、後者が通信ネットワークに接続されると、この電気装置がそれに割当てられたモニタ・コードのセットに対応するモニタ・コードのみを受けることができ、かつ受けることができる場合のみ、それに割当てられた許可モニタ区域にあるといわれている。

【0023】

したがって、所与の電気装置EAに対して、図2aは、電気装置EA₁のための区域Z₁と、許可モニタ・コードCGL_{n+1}ないしCGL_{n+p}が割当てられている電気装置EA₂のための区域Z₂と、最後に許可モニタ・コードCGL_{n+p+1}ないしCGL_{n+m}が割当てられている電気装置EA₃のための区域Z₃とがあることを示す。

30

【0024】

特に、地理学的場所と、ネットワークの性質と、各前記電気装置EA₁ないしのEA₃に割当てられている許可モニタ・コードを送ることができる各特殊化されている送信器との関数として、各装置に割当てられたモニタ・コードのセットはしたがって地理学的場所すなわち監視区域に対応することが理解される。

【0025】

一般的なやり方で、関係する各電気装置の連続監視を確実にするように、符号化されたメッセージMIを送るステップAを定期的に反復できる。

40

【0026】

その後で、たとえば、意図されたいかなる盗難も避けるように、符号化されたメッセージMIの定期的送信の中断の後に、関連する電気装置の施錠操作、これについてはこの説明の次に詳しく説明する、を続けることができるので有利である。

【0027】

したがって、図2aに関連して先に述べた諸条件の下に、対応する電気装置EAが属している、地理学的場所を表す数値を含んでいる少なくとも1つのフィールドを許可モニタ・コードCGL_iが含むことができることが示されている、図2bを参照する。

50

【0028】

更に、図2bを参照して、この説明の次に説明するように、許可モニタ・コードが、ユーザーによって署名されたある条件を表す数値を含んでいる少なくとも1つのフィールド、CPHと示されている、を有することができることが示されている。

【0029】

ここで、本発明の主題に従う、ネットワークに接続されている電気装置の許可をモニタする方法についてのより詳細な説明を、この方法に従う電気装置の集合についての高度の安全を協議することを可能にする特定の実施形態で図3aに関連して行うことにする。

【0030】

この目的で、各符号化されたメッセージMIは電子的に署名され、署名された各メッセージは、電気装置EAの受信器Rによる署名の検証時に、この検証されて復号された情報が、受信器Rに組込まれている特定の許可データを満たすかどうかを判定可能にする署名された認証データのデータ・フィールドを含んでいることが示される。

10

【0031】

特殊化されている送信器ESは、それが送信する符号化されたメッセージMIを認証可能にする秘密の鍵を有し、したがって、たとえば、携帯型コンピュータでエミュレートすることにより侵害者が特殊化されている送信器の製作と動作を避けることが示されている前記図3aを参照する。

【0032】

以下に図3aに関連して説明する手順のモードは、実行すべきサービスの性質に依存して受信器Rがそれを元にして反応できるような認証メッセージを構成している符号化されたメッセージMIの定期的な放送を確実に行う特殊化されている送信器ESに属しているので、有利である。

20

【0033】

図3aの場合における手順のモードはたとえば一方向動作モードに対応する。

【0034】

一般的なやり方で、組立体は個人鍵 K_{ACPR} と公衆鍵 K_{ACPU} が提供されている認証機関ACのモニタを受ける。各特殊化されている送信器ESには次の情報が提供される。

- 製作によって特殊化されている送信器ESに特有の情報；
- 特殊化されている送信器ESの製作者により付与された独特の識別番号、この番号は図3aに参照記号INESにより表されている；
- 特殊化されている送信器ESのクロック回路により供給される日時に対応する、HOで示されている、時間スタンプ値。時間スタンプ値HOはYY、DD、HH、min、SS、CCの形で符号化できる。ここにYYは年を示し、MMは月を示し、DDは日を示し、HHは時間を示し、minは分を示し、SSは秒を示し、CCは100分の秒を示す。

30

【0035】

更に、各特殊化されている送信器ESには、各特殊化されている送信器ESに特有の個人鍵 K_{ESPR} と公衆鍵 K_{ESPU} を持つ署名システムを基にして符号化されたメッセージMIのデータの署名された値を計算することを可能にする署名計算モジュールが設けられている。したがって、計算署名INES、HOおよび場合に依りて補助データDA1を各特殊化されている送信器ESのレベルで実行できるので有利であり、この署名された値の計算動作は

40

$$S_{ES} = S_{KESPR}(HO, INES, DA1)$$

と示されており、この理由で閉じられているループ矢印により表され、署名された値の計算動作は単一の特殊化されている送信器ESのレベルで実行される。補助データDA1は特定のデータで構成できる。それについてはこの説明に続いて明らかにされるであろう。

【0036】

署名を計算するためのパラメータに関する限りは、この署名値は個人鍵 K_{ESPR} から計算でき、公衆鍵 K_{ESPU} はこの説明に続いて説明するように、署名された値を検証するために使

50

用できる。したがって、署名されるフィールドは特殊化されている送信器の識別番号 I N E S と、時間スタンプ値 H O と、場合に応じて補助データ D A₁ とを有する。

【0037】

したがって、得られた署名値 (2) は前記平文情報 (1) の電子署名を構成することが理解される。更に、各特殊化されている送信器 E S には、特殊化されている送信器の公衆鍵、K_{ESPU}、認証機関の名称 N A C、公衆鍵の有効日付 D V、認証機関の公衆鍵 K_{ACPU}、およびデータフィールド X を構成している、補助データ D A₂ などの複数の許可データが提供される。

【0038】

最後に、それらの許可データは前記データの署名 S_{AC} を有する。署名 S_{AC} は認証機関 A C によって計算され、各特殊化されている送信器 E S のメモリにデータフィールド X でインストールされる。署名 S A C は関係

$$S_{AC} = S_{KACPR}(X)$$

を満たす。ここに S_{KACPR} は認証機関の個人鍵 K_{ACPR} を基にした署名の動作を示す。

【0039】

たとえば、特殊化されている送信器 E S のバージョンと、たとえば、補助データ D A₂ の外観で送られたメッセージの長さなどの他のパラメータを署名値 S_{AC} の計算に組み込むことができる。

【0040】

その後で、図 3 a に表されている特殊化されている署名された値 S E S の送信器 E S のレベルにおける計算が符号化された周期的メッセージ M I の各送信の前に実行されるので有利である。

【0041】

したがって、前記図を参照して、このメッセージは送られ、平文として送られた少なくとも時間スタンプ情報 H O と、特殊化されている送信器 E S の識別番号 I N E S についての情報と、署名動作にさらされる時間スタンプ情報 H O と、特殊化されている送信器 E S の識別番号 I N E S についての情報と、データ X のセットと、下記の平文情報を含んでいる証明書 C e r t を構成する S_{AC} とを有する。

- 特殊化されている送信器 E S の公衆鍵 K_{ESPU}、
- 認証機関の名称 N A C、
- この説明で先に示した形で与えられる日付 D V、
- および認証機関の公衆鍵 K_{ACPU}、
- 場合に応じて、補助データ D A₂。

【0042】

更に、特殊化されている送信器 E S のバージョンについての情報の項目に関連するフィールドと、送られるメッセージの長さとを提供できる。それらのデータはたとえば前記補助データを構成している。後者の場合には、メッセージがバージョン内でフィールドに告知される長さであるようにフリーバイトが更に付加される。

【0043】

符号化されたメッセージ M I を受けると、受信器 R は、図 3 a に表されているように、前記認証機関の公衆鍵 K_{ACPU} により、署名検証、 θ_{KACPU} で示されている、の第 1 の動作へ進むことができる。異なる実施形態では、受信器は符号化されたメッセージ M I を、前記署名検証動作を行うようにされている遠隔のサーバへ送ることができることが示されている。図 3 a で、署名検証動作は、受信器 R のレベルで行われた時に

$$\theta_{KACPU}(S_{AC})$$

と示され、第 1 の閉じたループ矢印 (I) により表される。この動作は受信器 R のレベルで行われる。正常モードでは、動作 I で使用される公衆鍵 K_{ACPU} の値は受信器 R において、優先モードに従って、以前に構成されているが、簡単にされたモードでは、メッセージ M I に含まれている公衆鍵 K_{ACPU} の値を使用することが可能であろう。前記署名検証動作 I によって、受信器 R はその後で、一方では、特に、前記署名検証の真の値に対して、符

10

20

30

40

50

号化されたメッセージ $M I$ を出す特殊化されている送信器 $E S$ の公衆鍵 K_{ESPU} を含んでいる、データ・フィールド X のデータが真正であることの検証へ、場合に応じて、受信器 R にこの値が前もって提供されていた時に、公衆鍵 K_{ACPU} の値の検証へ、進むことができ、その後で、他方、特殊化されている送信器 $E S$ の公衆鍵 K_{ESPU} の値、その値とそれが真正であることは検証されている、を基にして、署名された値 $H O$ 、 $I N E S$ 、 $D A_1$ の署名検証の第 2 の動作 $I I$ へ進むことができる。この動作は

$$\theta_{KESPU}(S_{KESPR}(H O, I N E S, D A_1)) = \theta_{KESPU}(S_{ES})$$

で示されている。この第 2 の検証動作 $I I$ は受信器 R のレベルにおいて第 2 の閉じたループ矢印 $I I$ により表されている。このプロセスは、時間スタンプ情報プラス特殊化されている送信器 $I N E S$ の識別番号が有効で、証明書 $C e r t$ に含まれている、特殊化されている送信器の公衆鍵 K_{ESPU} に組合わされている個人鍵 K_{ESPR} によって署名を実際に受けられていた。

【0044】

本発明の主題である方法の手順のモードは、認証機関 $A C$ または各特殊化されている送信器 $E S$ の公衆鍵、個人鍵で構成されている対を構成したやり方にいかにしても依存しない。限定しない例によって、署名アルゴリズムはそのようなものであることが知られている $R S A$ アルゴリズムとすることができ、かつ署名すべきデータに直接適用でき、またはそれらのデータにハッシュ関数を適用することによって計算されるそれらのデータの要約に適用される。限定しない例によって、ハッシュ関数で使用されるアルゴリズムは、そのようなものとして知られている、 $M D 5$ アルゴリズムのことがある。一対の鍵 K_{ESPR} 、 K_{ESPU} はいくつかの受信者送信器 $E S$ に共通のことがある。しかし、個人鍵 K_{ESPR} が妥協されると、関係する全ての受信者送信器の安全度がそれで危うくされる。したがって、各受信者送信器 $E S$ にとっては、妥協の危険を抑えるように一対の鍵を提供することが好ましい。

【0045】

特殊化されている送信器 $E S$ の実現に関する限りは、送信器によって供給される認証部 $C e r t$ が関連する特殊化されている送信器によって与えられた認証の質を定めることが示されている。

【0046】

この認証は構造に含めることができ、認証機関 $A C$ は独立しているか、製造者自身である。

【0047】

この特殊化されている送信器 $E S$ を調整するために、認証 $C e r t$ をオペレータによって特殊化されている各送信器 $E S$ に更に含ませることができる。

【0048】

図 3 a に示されている本発明の主題であるこの方法の特定の実現についてのより詳細な説明を、ここで図 3 b を参照して、特殊化されている送信器 $E S$ が、たとえば、電力量計などの、計量装置に組合わされているより特定な場合について行うことにする。

【0049】

それらの条件の下では、および本発明の主題であるこの方法の特に注目すべき面に従って、計器 $C O$ は、計器の製作者によって付けられた独特の識別番号、 $N C O$ と示されている、および計器により記録された消費量を表す指数 $I C O$ を特殊化されている送信器 $E S$ に提供する。

【0050】

それらの条件の下で、符号化されたメッセージ $M I$ は図 3 a を参照して説明したものと同一素子で構成されているが、それに、一方では、計器番号が、他方では、計器インデックス、すなわち、加入者、場合によっては電気装置 $E A$ 、によって消費された量を表す情報、が付加される。計器番号 $N C O$ とインデックス $I C O$ 情報はメッセージの平文部のレベルと、その署名された部分のレベルで、たとえば、補助データ $D A_1$ の外観で、導入される。

【0051】

受信器Rが符号化されたメッセージMIを受けた後で、署名検証動作IとIIが図3aの場合におけるのと同様にして行われる。

【0052】

しかし、この実施形態の特に有利な面に従って、受信器Rは、前記署名検証動作の後で、計器番号とインデックス情報が有効であることを確保することを可能にし、認証Certに含まれている、特殊化されている送信器ESの公衆鍵 K_{ESPU} に対応する個人鍵 K_{ESPR} によって暗号化されている。

【0053】

その後で、計器番号NCOと、配電網におけるこの計器の場所との間で関係、この場合には場合に応じて加入者需要者の同一性、が成立すると場所の認証が終わる。

10

【0054】

時間スタンプ値HO、場合に応じて計器インデックスICO、それらは単調増加時間依存値である、がメッセージMIと署名 S_{ES} とに存在すると、特殊化されている送信器ESの存在をシミュレートする目的でメッセージMIの詐欺的再生を避けることを可能にすることが特に示されている。

【0055】

最後に、図3bの実現の異なる実行において、各符号化された情報メッセージMIは、電気装置の使用許可の期間を表す少なくとも1つのデータ・フィールドを有することもできることが示されている。前記図3bには、この許可の期間はFAで示されている。電気装置EA用の、または場合に応じて、計器COによって管理される電気装置の群用の、計器COの電気回路に保存されている署名の始まりの日と終りの日に対応することが好ましいことがある。その場合には、電気装置の許可の期間、すなわち、フィールドFA、は符号化された情報メッセージMIの、平文部とそれの署名されている部分に、組み込まれるので有利である。許可の期間は、新しい認証メッセージの送信をより初期の認証メッセージから、分離する時間間隔に限定することもある。

20

【0056】

本発明の主題である方法の種々の代わりの実施形態をここで図4aおよび図4bを参照して詳細に説明する。

【0057】

一般的なやり方で、本発明の主題であるこの方法を、特殊化されている送信器ESから関連する電気装置EAの受信器Rまで一方向に実施でき、または逆に双方向に実現でき、受信器RESが設けられている関連する特殊化されている送信器ESと、局所化されている送信器、ELと示されている、がその時に設けられている電気装置EAの間の交換がその時に開始されることが思い出される。

30

【0058】

図4aに例示的に示されているのは特殊化されている送信器ESと電気装置EAの間の情報メッセージの交換である。異なる性質の情報メッセージが一方向交換に従って非同期的に先験的に送られ、または場合に応じて、特殊化されている送信器ESと電気装置EAの間、すなわち、一方では、受信器Rと、他方では、対応する付属されている送信器ELとの間の情報メッセージの双方向交換のためのプロトコルで先験的に送られ、以下に明らかになるであろう諸条件の下で特殊化されている送信器ESにより促す。

40

【0059】

前記双方向交換は、後者が特殊化されている送信器ESによる促進で実行される時に、実際に前記特殊化されている送信器を基にして前記特殊化されている送信器と各電気装置EAの間の情報メッセージ交換のためのプロトコルをモニタすることを可能にすることが特に理解される。

【0060】

一層特定のやり方で、多様な機能のメッセージの交換が一方向キャラクタ、または逆に、図4aに示されているように、電気装置EAのレベルで実行される機能がそのように求め

50

る時に双方向キャラクタを示すことがあることが示されている。この理由から、および前記図において、各多様な機能を実行するように、種々雑多な機能および特に受信者送信器 E S と電気装置 E A の間のそれらのメッセージの交換を示し、かつその実行を可能にする種々のメッセージが分離されていることが破線によって示されている。

【0061】

前記図を参照して、本発明の主題に従って電気装置 E A をモニタする方法が、特殊化されている送信器 E S からこの電気装置の受信器 R へ、この説明で先に述べた特定の組み込まれた許可データを少なくとも含んでいる初期化メッセージ、M I D で示されている、を送ることにあることができることが示されている。この送りは、ネットワークを受信メッセージの知識で過負荷にしないように、一方向タイプのものにできることが示されている。初期化メッセージ M I D の送りは図 4 a の点 (1) に表されている。そのように知られているやり方で、電気装置 E A の受信器 R による組み込まれた特定の許可データの受取りに続いて、およびこの装置によるそれらのデータの検証に続いて、同じ図 4 a の点 (2) ないし (5) とともに明らかにされる種々の機能を確実にするように、受信器 R に待機モードで前もってインストールされている、この検証に対する肯定応答が受信器 R の、および場合に応じて、電気装置 E A に装備されている付属されている送信器 E L の、全ての機能を起動することを可能にする。

【0062】

更に、前記図の点 (2) に表されているように、本発明の主題である方法は、受信器 R からの要求に応じて、特殊化されている送信器 E S からこの受信器 R へ、電気装置 E A の許可のモニタを除くためのメッセージ M L C H を送ることにあるステップを有することができ、受信器 R と電気装置 E A は許可モニタ除去メッセージを受けると、その後で制約されない動作にリセットされる。

【0063】

図 4 a の点 (2) に表されている実施形態では、電気装置 E A の付属されている送信器 E L は許可除去要求メッセージ、M R L H、を特殊化されている送信器の受信器 R へ送り、それに、除去情報メッセージ、M L I と示されている、を電気装置 E A の受信器 R に以前にアドレスした特殊化されている送信器 E S によって促進することが続く。この除去情報メッセージ自体は第三者により送られた要求により、特殊化されている送信器 E S によって送られていた。この第三者は、この説明の後で説明するように、もちろん信頼されている第三者または許可されている管理主体である。特に、要求メッセージ R E T は通信ネットワークとは異なるネットワークによって伝えることができ、それには特殊化されている送信器 E S と電気装置 E A およびそれに装備されている受信器 R および付属されている送信器 E L が接続されていることが理解される。しかし、要求 R E T は信頼されている第三者を認証するプロセスと、従来のものであるという理由からここでは説明しない従来の認証プロセスとによって確実に行うことが示されている。簡単にされたプロセスは、要求 R E T を関連する特殊化されている送信器 E S をアクセスするコードにすることによってできる。この安全プロセスは信頼されている第三者の同一性のいかなる侵害も避けることを可能にする。

【0064】

電気装置 E A の受信器 R による許可モニタ除去メッセージ M L C H の受取りに続いて、制約されない動作への電気装置 E A のリセット手順は、図 4 a の点 (2) に表されているように、内部で実行される。

【0065】

更に、本発明の主題である方法は、図 4 a の (3) に示されているように、第三者素子、すなわち、モニタ周辺のためおよびこのモニタ周辺の監視を確保するために定められている信頼されている第三者からの要求に応じて、電気装置 E A の現場ブロッキングのメッセージ、M V E R と示されている、を特殊化されている送信器 E S から電気装置 E A の受信器 R へ送ることにあるようにできる。電気装置 E A の場所においてブロッキングのためのメッセージ M V E R を受けると、内部で進んで前記電気装置のいかなる必須の機能も不能

にすることが可能にされる。特に、現場ブロッキング・プロセスは電気装置または複数の電気装置E Aの所有者によって実行できるので有利である。その所有者は、家を長期間留守にする時は、彼の留守を信頼できる第三者に知らせることができ、後者は彼の求めRETによってブロッキング・メッセージM V E Rを特殊化されている送信器E Sを介して送ることにより、電気装置の、または関係する電気装置E Aのいかなる必須の機能もこの留守期間中確実に不能にする。

【0066】

更に、図4 aの(4)に示されているように、本発明の主題である方法は、関連する特殊化されている送信器の認証のためのメッセージMAを、特殊化されている送信器E Sから電気装置WAの受信器Rへ送ることにあるようにできる。

10

【0067】

前記図の点(1)を参照して、認証メッセージMAは、初期化メッセージM I Dと同様にして、それらの同じ許可データに統合されている少なくとも特定の許可データを含むことができること、および電気装置E Aの受信器Rのレベルで許可をモニタを起動する手順は、しかし、許可メッセージを受けた時はこの電気装置のレベルおよびこの受信器のレベルにおいて実行されないことが示されている。特に、前記図の点(4)で説明したメッセージなどの許可メッセージMAは決定されている周期で、または、本発明の主題である方法の管理を行う信頼されている第三者からの簡単な求めに応じて、送ることができる。特に、許可メッセージMAは定期的または不定期に修正でき、それによって、たとえば、詐欺にかからないように、特定の統合されている許可データは結果として修正される。

20

【0068】

最後に、本発明の主題である方法は、図4 aの点(5)に表されているように、電気装置E Aから、すなわち、後者に装備されている付属されている送信器E Lから特殊化されている送信器E Sへ、電気装置E Aの識別コードを含む忠誠メッセージMALを送ることにある。

【0069】

好ましくは、前記図4 aに示されているように、特殊化されている送信器E Sから電気装置E Aへ送られた忠誠要求メッセージMRALを受けた電気装置E Aにより忠誠メッセージMALは送られ、したがって、忠誠メッセージMALは忠誠要求メッセージMRALの受取りに応じて送られる。

30

【0070】

特殊化されている送信器E Sの受信器RESによる忠誠メッセージMALの受取りに続いて、後者は前記忠誠メッセージの検証に進む。特殊化されている送信器E Sのレベルで内部的に実行される検証手順は、忠誠メッセージMAL内で送られた電気装置E Aの識別コードの値を検証することに本来は存する。

【0071】

検証手順に対する肯定応答、 θ (MAL)で示されている、があると、本発明の主題である方法は、特殊化されている送信器から電気装置E Aの受信器Rへ、検証の無い時に、この検証不存在は θ (MAL) = 0で示されている、受信器と電気装置E Aとの固定を命令するメッセージを送ることにあるものとできる。固定動作はもちろん前記電気装置のレベルで内部的に実行される。

40

【0072】

特に、忠誠メッセージを送る手順と、この忠誠メッセージの検証が無い時に応答する手順は、忠誠という概念が特殊化されている送信器E Sに関する電気装置E Aの適正な動作のみならず、合法的な持主すなわち所有者から盗まれたどのような電気装置E Aのモニタも含み、したがって、モニタ領域 Z_1 で動作することを許可され、この説明で以前に述べたように、許可モニタ・パラメータが異なるモニタ領域 Z_2 へ送られる限り特に有利であることが特に理解される。この最後の仮定の下では、電気装置E Aの全面的な固定、この全面的な固定はおそらく電気装置E Aのいかなる必須の機能も不可逆的に不能にすることより成る、が、盗まれてはいるが、本発明の主題である、許可モニタ・プロトコルに管理さ

50

れているいかなる電気装置 E A の使用も不可能であるという理由によって、意図された盗難に関して、特に良い抑制力であることが判明している。

【0073】

したがって、図 4 a の点 (5) に表されているように、忠誠要求メッセージ M R A L の受取りに続いて忠誠メッセージを送る手順は、図 4 a の点 (1) に表されているように、特殊化されている送信器 E S による初期化メッセージ M I D の各送りの後で系統的に開始できるので有利であり、この状況で忠誠メッセージを送る手順は、電気装置 E A の起動後に許可モニタを受ける後者の適正な動作の検証を確保することを可能にする。

【0074】

更に、本発明の主題である方法の注目すべき面に従って、忠誠メッセージ M A L を送る同じ手順は、図 4 a の点 (4) に示されているように許可メッセージ M A の各送りの後で実行できるので有利であることが示されている。そのような状況では、忠誠メッセージ M A L の送りと、後者の検証との成功が、電気装置 E A が、関係する電気装置へ許可メッセージ M A によって以前に送られた新しい許可データに一致することを検証することを可能にする。

10

【0075】

説明し、かつ前記図の点 (2) と (3) に示されているものなどの、許可のモニタを除去することを求めるメッセージを送る手順と、ブロッキング・メッセージを送ることを求める手順とは、第三者、信頼される第三者、の要求メッセージ R E T を受けた時に行うことが好ましいが、忠誠メッセージ M A L を送る手順は特殊化されている送信器 E S の唯一の主導権の下に行うことが好ましいことがあり、後者はそれをモニタする許可を確保する各電気装置 E A の忠誠をモニタする主導権を享受している。それらの条件の下で、初期化メッセージ M I D または認証メッセージの送りに続く特殊化されている送信器 E S の送信とは別に、徹底的なモニタを確実に行うように、忠誠要求メッセージを送り、したがって、関連する各電気装置 E A によって忠誠メッセージを定期的に送るための手順を実行するようにして、特殊化されている送信器 E S をプログラムすると有利である。

20

【0076】

一方では、特殊化されている送信器 E S が接続され、他方では、受信器 R と付属化されている送信器 E L が装備されている電気装置 E A が接続されているネットワークが低電圧電気エネルギー配電網、L T 網、で構成されている時に、本発明の主題である方法の制約されない特定の実施モードについての詳細な説明をここで図 4 b を参照して行う。

30

【0077】

前記図に示されているのは、搬送電流によりメッセージを送れるようにする集中装置が装備されている高電圧／低電圧変電所、H T／L T 変電所である。低電圧電気エネルギー配電網は主 L T 網と二次 L T 網、いくつかの二次 L T 網がおそらく設けられる、に分けることができ、それらの二次網は主 L T 網の H T／L T 変電所に相互に接続されていない。H T／L T 変電所自体は切り替えられる公衆電話回線網 S P T N により、信頼できる第三者によって維持されている管理センターに相互接続できる。主 L T 網と各二次 L T 網、二次 I L T 網、二次 I I L T 網、二次 I I I L T 網と示されている、搬送電流によるメッセージの送受信を行えるように、対応する L T 網に接続されている各加入者には、電力量計と、もちろん、相導体の 1 つと網の中性点との間に接続されている通信顧客インタフェース回路、回路 I C C と示されている、とが備えられている。したがって、図 4 b では、計器と I C C 回路とで構成されている各組立体は、関連する L T ネットワークに置かれている白丸で表されている。更に、図 4 b に示されているように、L T 網と、主網または二次網の各分岐には低電圧搬送電流／無線周波数双方向リンクをインタフェースするための少なくとも 1 つの装置を設けることができ、したがって、各装置はヘルツ空間を通じて搬送電流によりメッセージを確実に双方向に送る。それらの条件の下では、低電圧搬送電流／無線周波数双方向リンク・インタフェース装置は、網の各分岐に接続されている I C C 回路の数とは無関係に、特に有利な条件の下に前記メッセージの双方向伝送を確実に行うことを可能にする。それらの条件の下では、H T／L T 変電所の集中装置と各 I C C 回路、お

40

50

よび最終的には各加入者、との間の通信メッセージが、搬送電流によって運ばれる情報に関してほぼ完全な透明性をもって送られる。したがって、それらのメッセージは、L T 網の周囲を流れる搬送電流によって運ばれる任意の情報フレームの実時間再送によって送られる。情報メッセージまたはフレームあるいはデータの前記送りはその後で、送信クレジットを割当てられたリップルにより反復のプロセスに従って実行される。そうすると送信の双方向キャラクタが確保される。H T / L T 変電所集中装置と低電圧搬送電流／無線周波数双方向リンクのインタフェース装置との間のメッセージの双方向伝送の手順モードについてのより詳細な説明については、「1998年4月23日にエレクトリシテ・デ・フランスの名称で公告された「低電圧搬送電流／無線周波数双方向リンクをインタフェースする装置 (Device for interfacing a low-voltage carrier currents / radio frequency bidirectional link)」という名称のPCT特許出願WO 98 / 17013を参照できるので有用である。

10

【0078】

それらの条件の下では、特殊化されている送信器E Sと、受信器Rと付属されている送信器E Lが装備されている任意の電気装置E Aとの間のメッセージの双方向交換は、前記インタフェース装置、I C C - Rで示されており、図4 bの線画にL T 網の分岐に隣接する十字を含んでいる丸によって表されている、により満足できるやり方で実行できる。

【0079】

図4 bに全体として説明されているシステムは、図4 aを参照して先に説明したメッセージの経路指定を行えるようにすることが特に理解される。もちろん、特殊化されている送信器E SがH T / L T 変電所の集中装置のレベルに置かれると、複数の電気装置E Aを各加入者のレベルに有する家庭用電気設備のセットの管理は、1つの同じ特殊化されている送信器E Sによって確保できる。それらの条件の下では、特殊化されている送信器E Sは、一方では、切り替えられる公衆電話回線網S P T Nに、他方では、この説明で先に述べたものなどの、低電圧搬送電流／無線周波数双方向リンクおインタフェース装置によって直結されている。

20

【0080】

本発明の主題である方法の種々のサービス設備への特定の応用についてのより詳細な説明を、ここで図5 aおよび図5 bを参照して行う。

30

【0081】

図5 aは、受信器を装備されている電気装置E Aが受信器を装備されている電気装置E Aが提供債務者の電気装置を備える時の、特殊化されている送信器E Sと、本発明の主題である方法との第1の実現例に関するものである。前記図に関連して与えられている例では、電気装置E Aはマイクロコンピュータで構成され、提供債務者ユーザーは、遠方の場所に居て、おそらくモニタ機関を構成している債権者を尊重して、たとえば、在宅作業提供を行うことを求められる。本発明の主題であるプロトコルに従う電気装置E Aの構成マイクロコンピュータは、その後で、たとえば、A T Mネットワークまたはインターネット・ネットワークによってモニタ機関の遠隔場所にリンクできる。

【0082】

40

特に、この用途では、特殊化されている送信器E Sは認証メッセージM Aを受信器Rへ定期的に送ることができ、この認証メッセージはおそらく提供債務者サービス提供者が、アクセスがモニタ機関によって合意された作業の正常な場所から実際に起きることを、遠隔の場所に、すなわち、提供の債権者に立証することを許す。

【0083】

組立の手順のモードを以下に説明する。

【0084】

どのような組の装置、すなわち、電気エネルギー配電網に接続されている任意の電気装置E A、と同様に、提供債務者のワークステーションを構成しているマイクロコンピュータは、特殊化されている送信器E Sによって提供された定期的メッセージを受ける。

50

【0085】

ワークステーションを構成しているマイクロコンピュータが遠隔の場所に接続するやいなや、識別プロセスの後で、マイクロコンピュータは特殊化されている送信器ESから受けたメッセージの内容の全てまたはいくらかを遠隔の場所へ送る。

【0086】

そのようなプロセスは以下の動作の実行を許す。

【0087】

遠隔の場所による特殊化されている送信器ESの認証の検証：

遠隔の場所は、特殊化されている送信器ESにより使用される保証機関の公衆鍵K_{ACPU}を通常有しなければならない。したがって、電気装置EAの受信器Rによって実行される方法に類似する方法によって、前記したようにメッセージMIを受けると、遠隔の場所は提供債務者のマイクロコンピュータによって、特殊化されている送信器ESから、または場合に依じて、特殊化されている送信器ESが計器に組合わされている場合にはメッセージで特定されている計器から、最初に送られてきたものとしてそのメッセージを真正なものと認証できる。遠隔の場所はユーザー、すなわち、提供債務者の、および特殊化されている送信器ESの、または後者に組合わされている電力量計の、同一性の関連を更に検証できる。

10

【0088】

遠隔の場所が保証機関の公衆鍵K_{ACPU}を有していない場合には、かつ、遠隔の場所が危険を受ける場合には、それは特殊化されている送信器ESによって供給されたメッセージまたはメッセージ部分に含まれているその鍵を使用し、提供債務者のマイクロコンピュータによって再送りする。保証機関のこの公衆鍵K_{ACPU}はしたがって保存でき、その後で遠隔の場所のレベルで検証と再使用との少なくとも一方を受けることができる。特殊化されている送信器ESによって供給されたメッセージに含まれている公衆鍵K_{ACPU}の受入れにおける危険は、偽の認証機関によって制作されたメッセージが有効なものとして受入れられることがあるという事実に存する。この危険はアクセスされる遠隔場所の安全政策に含ませなければならない。その政策はこの動作手順のために留保すべき運命を支配せねばならない、すなわち、警報で拒絶または受け入れを選択するか、さもなければたとえば、確認の要求で受入れなければならない。

20

【0089】

特殊化されている送信器ESから来るメッセージの送り：

遠隔の場所における提供債務者の同一性を認証する手順は、通常の認証の代わりまたはそれを補充するものとして特殊化されている送信器ESから出るメッセージの送り出しを明らかに考察できる。

30

【0090】

手順のこのモードは主として、技術水準に存する認証プロトコルの修正へ導く。しかし、既存のプロトコル内で特殊化されている送信器ESによって送られた認証メッセージの経路を指定するために、提供債務者のワークステーションから遠隔の場所へ送られた他のメッセージにこのメッセージを隣接することを考察することが可能である。特に、パスワードによる認証モードでは、パスワードの代わりに特殊化されている送信器ESによって供給されたこの認証メッセージ、このパスワードに添付されているこの認証メッセージ、またはさもなければパスワードと、特殊化されている送信器ESによって供給されたメッセージとの予め設定された規約に従った組合わせを送ることが可能である。

40

【0091】

本発明の主題である方法の第2の用途をここで図5bを参照して説明する。

【0092】

この用途は、たとえば、電気エネルギーまたは固定されているネットワークを通じて計器を介して供給されるその他の任意の流体の新しい販売モードで、特殊化されている送信器ESを使用した時に実現できる。

【0093】

50

図5bに表されているように、エネルギー、たとえば電気エネルギーの分配と販売のためのサービスへの加入者に、少なくとも1つの受信器が組合わされている電気装置EAが提供される。電気装置EAは、需用者の屋内設備の各電気装置EAに電気エネルギーを供給することを可能にする分岐線と計器を介して低電圧電気エネルギー配電網に相互接続されている。この場合にはユーザーは提供債権者である。

【0094】

従来のやり方で、分配ネットワークを通じる流体の供給は前記計器で供給点において計量される。加入者へ、すなわち、提供債権者への請求書が計器における消費量と、彼の供給契約に関連する料金との関数として作成送達される。自由市場経済の枠組み内で、ネットワークのマネジャーによって確保される、分配サービスの提供と、流体の製造者または充填者によって確保される供給サービスの提供とは別である。同じ供給点は、種々の供給者から出る供給の場所とすることができる。限定しない例によって、1本の同じ電話線からの種々の電気通信オペレータによって実行されるサービスの提供が示される。それらの条件の下では、使用に従って異なる供給が明らかである。そのような状況は、電気エネルギー供給契約に関連する電気装置を販売する場合に起きる。そうすると電気エネルギー供給は特殊化された従量料金または均一料金を基にして請求される。所与の供給点に関する供給場所の認証がそうすると必要である。

【0095】

この目的で、図5bに示されているように、特殊化されている送信器ESは位置を示すメッセージを各供給者自身の計器および機器へ放送することによってこの認証を確保することを可能にする。

【0096】

その後で、関連する供給者は位置と、提供の債権者と個々に結ばれた契約との関数として適用できる彼の料金条件を定めることができる。そうすると、供給点において供給されたエネルギーと、顧客に供給されたエネルギーとの間の釣合いを確実にとることができる。それらの条件の下で、特殊化されている送信器ESの各電気装置EAとの通信モードは図5aの枠組み内で説明したものに匹敵するが、提供債権者は今はユーザーであり、提供債務者は電気エネルギーまたはそれに類似するものの分配のために編成されたサービスを供給する遠隔の場所である。それらの条件の下では、たとえばATMまたはインターネットのネットワークによるリンクを提供債権者とサービス提供者の遠隔の場所との間で行うことができる。

【0097】

更に、図5bは、遠隔サービスが遠隔の提供債務者場所から実行されるような類似の状況にも相当し、提供債権者は、たとえば、電気エネルギー配電網に接続されている受信器が設けられている電気装置EAの任意のユーザーである。

【0098】

一般的なやり方で、そのような状況における遠隔サービスは、顧客による何等かの介在が、通常、存在しない場合にこの顧客の設備にサービス提供者によって遠隔で行われる活動のことである。

【0099】

前記サービスを実行するために、提供者は、しかし、顧客の正確な所番地における介在が含まれるように努めなければならない。彼のサービスに対する請求書を発行するために、提供者は、彼が顧客の設備に遠方から実際に介在したことを証明せねばならず、かつ彼はもちろん介在の長さ、後者の日付との証明を行わなければならない。両方の場合に、提供者は、彼が介在する設備の実際の場所と、介在の現実性とをある程度保証せねばならない。

【0100】

そのような状況では、提供はサービス提供者によってたとえばコンピュータにおける介在のためにインターネットまたはATMネットワークを介して行うことができるが、介在が開始されると、介在の主体であるコンピュータ、すなわち、このコンピュータによって構

10

20

30

40

50

成されている電気装置E Aが、遠隔の場所にあるサービス提供者に、後者の付近に、すなわち、電気設備が関連している場合には計器の付近に、設置されている特殊化されている送信器E Sによって送られた認証メッセージを直ちに送る。したがって、サービス提供者は受けられたメッセージが真正なものであることを検証でき、たとえば介在の長さ、日付との証明を特に提供する。そうすると、特殊化されている送信器E Sの通信モードは図5 aの枠組み内で説明したものに匹敵する。

【0101】

本発明の主題に従ってネットワークに接続されている電気装置に関連させられている特殊化されている送信器と、受信器とのそれぞれのより詳細な説明を、図6 a、図6 bおよび図7 a、図7 bを参照して行うことにする。この説明で以前に述べたこの特殊化されている送信器装置とこの受信器装置はもちろん本発明の主題である方法の実施を許すものである。

10

【0102】

一般的なやり方で、所与のネットワークに接続されている電気装置に関連させられている前記特殊化されている送信器と受信器との間の、一方向通信の実現を行えるようにする最も簡単なものを、図6 aに示されているように、一辺が約20 cmの立方体を超えない、小型の一体式機器の形で製作できることが示されている。

【0103】

それらの条件の下では、図6 aに示されているように、特殊化されている送信器E Sは、外部電気エネルギー供給源、A L₁で示されている、に加えて、計算ユニット、またはマイクロプロセッサ、Pで示されており、かつ参照番号1₀が付けられている、と、署名および証明計算のための、参照番号1₁を付けられているコプロセッサ、または前記マイクロプロセッサ1₀に接続されているROM型の読出し専用メモリとを含んでいる電子カード1を備えることができる。プロセッサ1₀とコプロセッサまたは読出し専用メモリ1₁は内部バス1₂によって1₃で示されている作業用メモリにリンクされている。作業用メモリは、たとえば、署名計算動作と検証動作を行うためにROM型の読出し専用メモリ1₁から署名計算プログラムと検証プログラムをロードできるRAMメモリで構成できる。

20

【0104】

更に、特殊化されている送信器E Sは参照番号1₄ aを付けられている一方向通信ユニットと、参照番号1₅ aを付けられている送信器モジュールとを含んでいる。この送信器モジュールは、実行されるアプリケーションと、使用される通信ネットワークの形式との関数として、ヘルツ送信器、または逆に、たとえば、低電圧電気エネルギー配電網での搬送電流による送信器で構成できる。一方向通信ユニット1₄ aは内部バス1₂と送信器モジュール1₅ aに相互接続されている。この送信器モジュール自体は、送信器がヘルツ送信器までである場合にはアンテナにリンクされ、または送信器が搬送電流を基にした送信器である場合には接続モジュール1₆によって電気ネットワークに接続される。

30

【0105】

署名と、符号化された許可情報項目を構成するための符号化された値を計算するために、電気装置のために意図されている、プログラムを呼出すと、それらのプログラムはROM型の読出し専用メモリ1₁に保存され、署名計算動作と検証動作は作業用メモリ1₃と計算ユニット、すなわち、マイクロプロセッサ1₀、から実行できる。符号化された情報メッセージ、すなわち、符号化された許可情報項目を含んでいるメッセージ、を構成するように、符号化された許可情報項目を構成するための符号化された値はその後で一方向通信ユニット1₄ aへ送られる。その後でそれらのメッセージの伝送が、ヘルツ形、または搬送電流形の送信器モジュール1₅ aにより、アンテナ、または低電圧ネットワーク1₆に接続するモジュールを介して行われる。

40

【0106】

好ましくは、および図6 aに表されている特定の実施形態で、特殊化されている送信器E Sは、特殊化されている送信器E Sと流体またはエネルギーを計量する外部装置、C Oで示されている、との相互接続を行えるようにする、外部コンピュータ・ソケット、1₇で

50

示されている、を更に有する。外部コンピュータ・ソケットは、限定しない例によって、たとえば、RS232直列リンクにより具体化できる。更に、計器COと通信するためのユニットを構成しているリンク・モジュール 1_8 が外部コンピュータ・ソケット 1_7 と、マイクロプロセッサ 1_0 と署名計算コプロセッサ 1_1 または対応するROM型の読出し専用メモリと、ランダムアクセスメモリ 1_3 で構成されている計算モジュールとの間に設けられている。このリンクは内部バス 1_2 によって行われる。したがって、前記計算モジュールおよび特にマイクロプロセッサ 1_0 は流体またはエネルギーの計器COから計量情報項目を受けて、送られた情報メッセージを構成するように許可モニタ・コードを符号化することを可能にする。

【0107】

10

図6bに示されているのは、電気装置EAに組合わされている受信器R自体に送信器モジュールが装備されている時に、許可モニタを受けるこの電気装置に双方後リンクを行えるようにする特殊化されている送信器である。

【0108】

その場合には、特殊化されている送信器ESはその後でコンピュータに組合わされる専用カードの形で具体化できる。

【0109】

図6bで、同じ参照番号が図6aにおけるものと同じ素子を示す。しかし、送信モードまたは受信モードとして、特殊化されている送信器の手順モードを選択できるようにする双方向通信ユニットを示すために、通信ユニットには参照番号 1_4b が付けられている。同様に、伝送モジュールには参照番号 1_5b が付けられている。この伝送モジュールにはヘルツ受信モジュールまたは搬送電流をベースとする受信モジュールが更に装備されている。したがって、採用されている手順、特に、図4aを参照した説明で既に表されているように、双方向メッセージの交換のための、手順のモードの関数として、送信モードから受信モードへの切り替えはマイクロプロセッサ 1_0 と特定のプログラムによって行われる。

20

【0110】

図6bの場合には、この説明で先に述べた切り替えられる公衆電話回線網SPTNへの相互接続を確実にできるように、特殊化されている送信器には、参照番号3が付けられているグラフィックス・カードを備えた表示スクリーンと、参照番号4が付けられているキーボードと、参照番号5が付けられているモデムなどのマイクロコンピュータの装備のために通常実現されているより特定の素子を装備できる。

30

【0111】

図6bに示されている実施形態では、計器COは特殊化されている送信器ESの構成専用カード1に直接組み込むことができることが示されている。この場合には、特定の計量ユニットで構成されている計器COには、たとえば、電気ネットワークなどの流体またはエネルギーの配給網に直接接続されている測定センサが組合わされている。測定センサには参照番号8が付けられている。

【0112】

最後に、他の特定の機能を実現できる。この機能はおそらく、参照番号6が付けられている獲得および警報リンクカードにリンクされている、参照番号7が付けられている外部警報器で構成されている。外部警報モジュール7は獲得および警報リンクカード6によって内部バス 1_2 にリンクされている。

40

【0113】

本発明の主題に従う電気装置に組合わされている受信器Rのアーキテクチャについてここで図7aと図7bを参照して説明する。

【0114】

図7aの実施形態は、マイクロプロセッサによる電気装置の諸機能のインテリジェント管理のための機能を有するか、有しない電気装置について特に意図されている最小実施形態である。この受信器は、外部電源AL₂によって電力を供給される、または場合に応じて

50

たとえば電気装置への電源によって電力を供給される、特定の電子カードで実現できる。

【0115】

図7aで、マイクロプロセッサ 2_0 と、コプロセッサまたはROM型読出し専用メモリ 2_1 と、内部バス 2_2 と、ランダムアクセスメモリ 2_3 とで構成されている部品が専用電子カードに付加され、たとえば、説明で先に述べたように、遠隔作業への応用で電気装置EAがマイクロコンピュータで構成されている時に、プロセッサ 2_0 と、内部バス 2_2 と、メモリ 2_3 とは電気装置EAの素子でおそらく構成されている。

【0116】

図7aに示されている受信器は、一方向通信ユニット 2_4a と、参照番号 2_5a を付けられているヘルツ受信器または搬送電流を基にした受信器と、外部アンテナ、または受信が搬送電流によって行われる場合には電気ネットワークに接続するためのモジュールとをほぼ備えている、符号化された情報メッセージを受けるモジュールを更に備えている。このアンテナまたはこの接続モジュールには参照番号 2_6 が付けられている。素子 2_6 、 2_5a 、 2_4a は縦続接続され、一方向通信ユニット 2_4a はそれ自身内部バス 2_2 に接続されている。

10

【0117】

図7aから更に観察されるように、受信器装置Rは、受けた各情報メッセージに含まれている符号化された許可情報項目を復号および検証するモジュールを備えている。この復号および検証モジュールは計算マイクロプロセッサ 2_0 、もちろんRAM型作業メモリ 2_3 と、参照番号 2_1a を付けられて、この説明で先に述べたように、署名計算および検証プログラムを保存するコプロセッサすなわちROM型読出し専用メモリ 2_1 で構成されるので有利である。

20

【0118】

更に、電気装置EAの許可または不許可を、符号化された許可情報の検証の関数として命令するモジュールも設けられる。このモジュールはマイクロプロセッサ 2_0 と、参照番号 2_1b を付けられているROM型読出し専用メモリと、もちろん作業メモリ 2_3 とで構成されている。この命令モジュールは参照番号 2_7 が付けられていて、命令コマンドを電気装置EAにおよび特にその必須の機能に発することを可能にするコンピュータ・ソケットが補充されている。ソケット 2_7 は、たとえば、直列リンク型ソケットで構成できる。それは、図4aを参照して先に述べたように、許可モニタを受ける電気装置の必須の機能をブロッキングする、すなわち、不可逆的に不能にすることを命令するメッセージの経路を指定することを可能にする。

30

【0119】

ROM型読出し専用メモリ 2_1b は、電気装置EAのために意図されているブロッキングすなわち不可逆的に不能にする命令のセットを有することができるので有利である。

【0120】

図7bに示されているのは電気装置に組合わされている受信器である。その図では同じ参照番号が図7aの実施形態の場合におけるのと同じ素子を表す。しかし、この受信器はより高度な受信器であってそれは特殊化されている送信器と電気装置EAに組合わされている受信器との間の双方向リンクの実現を許す。図7aに表されている受信器の実施形態についての違いは、双方向通信ユニットである、参照番号 2_4b が付けられている通信ユニットと、関連する参照番号 2_5b が付けられている、ヘルツ受信器モジュール、このモジュールには今は送信器が装備されている、とに関連する。そうすると受信器送信器モジュール 2_5b はヘルツまたは搬送電流を基にした受信器／送信器モジュールである。

40

【図面の簡単な説明】

【図1】 ネットワークに接続されている特殊化されている送信器と電気装置との間の本発明の主題であるプロトコルを実行するステップの流れ図を、例によって、表す。

【図2a】 本発明の主題であるプロトコルを実行するネットワークに接続されている任意の電気装置に対する許可モニタ区域または許可モニタ周辺を定める線図を、例によって、表す。

50

【図 2 b】 本発明の主題であるプロトコルの実行を許す電気装置と特殊化されている送信器の間の符号化されたメッセージの優先的な特定の形態を、例示的なやり方で、表す。

【図 3 a】 本発明の主題であるプロトコルの枠組み内で、ネットワークに接続されている特殊化されている送信器とネットワークに接続されている電気装置によってそれぞれ実行される種々の署名プロセスおよび署名検証プロセスを、例によって、表す。

【図 3 b】 電気装置が、加入者において、流体源またはエネルギー供給源に連結されているサービス提供を確保することを電気装置が可能にする一層特定の場合に、本発明の主題であるプロトコルの枠組み内で、ネットワークに接続されている特殊化されている送信器とネットワークに接続されている電気装置によってそれぞれ実行される種々の署名プロセスを、例によって、表す。

10

【図 4 a】 ネットワークに接続されている特殊化されている送信器と電気装置の間のメッセージの種々の交換、それらのメッセージの交換モードは一方向または双方向である、を、例によって、表す。

【図 4 b】 低電圧電気エネルギー配電網であって、それに接続されている特殊化されている送信器と電気装置との間の搬送電流によるメッセージの交換を特に行うのに適する前記配電網型の、網の好適な実施形態を、純粋に例によってのみ、表す。

【図 5 a】 遠隔作業などのサービス提供用途の枠組み内で本発明の主題であるプロトコルの実行例を、例によって、表す。特殊化されている送信器は設置されて、電気エネルギー分配計のレベルで、低電圧電気エネルギー配電網に接続され、かつ電気エネルギー分配サービスへの加入者の電気装置と遠隔作業サービスとに接続され、それらのうちの後者は、たとえば、A T M ネットワークによって、遠隔作業サービス提供をモニタする機関の役割を演ずる遠隔場所にリンクされているコンピュータで構成されている債務者、または少なくともこのサービス提供の債権者である。

20

【図 5 b】 遠隔介在などのサービス提供用途の枠組み内で本発明の主題であるプロトコルの実行例を、例によって、表す。特殊化されている送信器は設置されて、加入者の電気エネルギー分配計のレベルで、遠隔介在サービスに接続され、それらのうちの後者は債権者であって、この遠隔動作のための任意の電気装置ケーターリングと、この電気装置の消費量の定期的な遠隔読取りと、この装置がコンピュータ装置である場合に補修介在などの動作とで構成され、この装置は、たとえば、A T M ネットワークによって、サービス提供者から遠い場所にリンクされている。

30

【図 6 a】 一方向通信の下にメッセージの送りに特に適する本発明の主題に従って特殊化されている送信器のアーキテクチャを、例によって、表す。

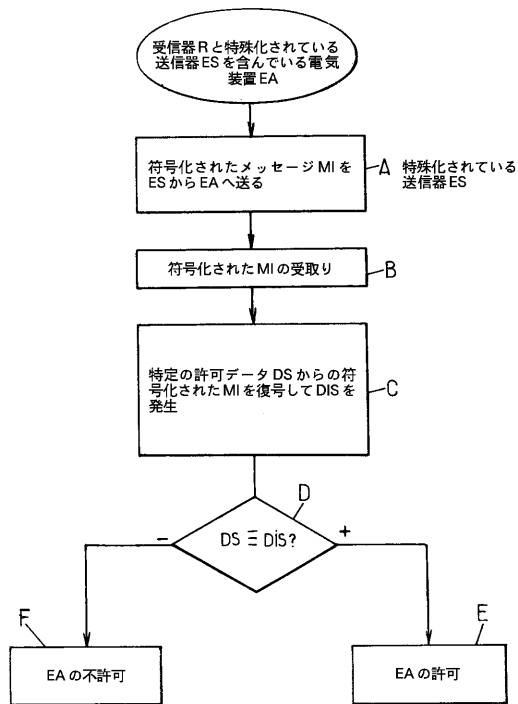
【図 6 b】 双方向通信の下にメッセージの送りと受取りに特に適する受信器を装備されている、本発明の主題に従って特殊化されている送信器のアーキテクチャを、例によって、表す。

【図 7 a】 本発明の主題に従って、かつ電気装置に組合わされている受信器のアーキテクチャを、例によって、表す。この種の受信器は、たとえば、図 6 a を参照して説明する特殊化されている送信器によって送られる一方向通信の下でメッセージの受取りに特に適する。

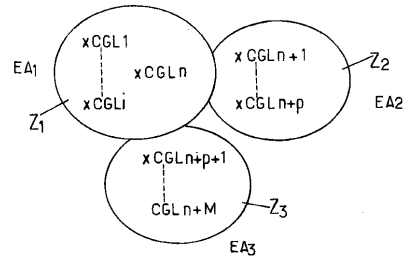
【図 7 b】 本発明の主題に従って、かつ電気装置に組合わされている受信器のアーキテクチャを、例によって、表す。この種の受信器は、たとえば、図 6 b を参照して説明するものなどの受信器が装備されている特殊化されている送信器で双方向通信の下でのメッセージの交換に特に適する。

40

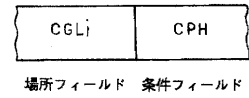
【図 1】



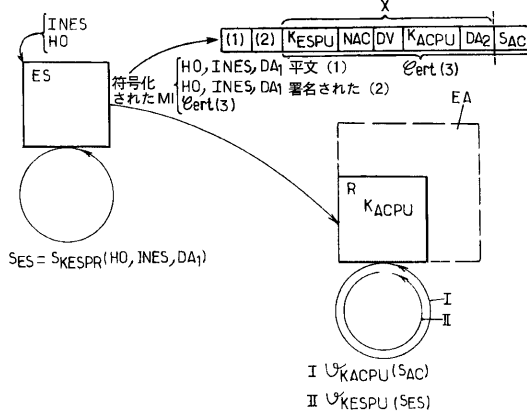
【図 2 a】



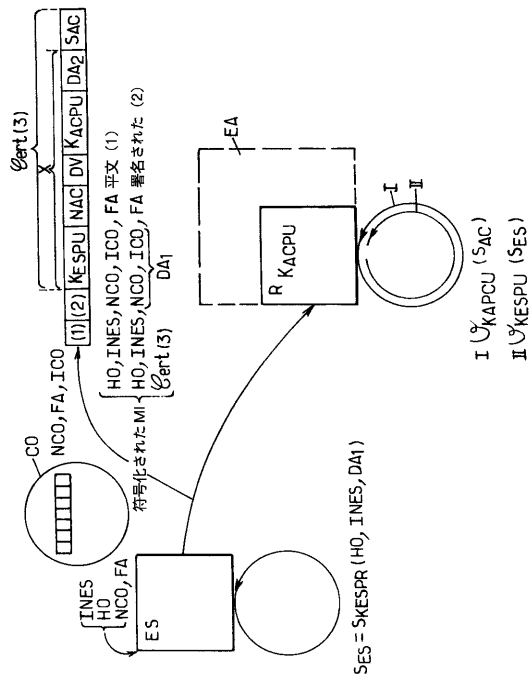
【図 2 b】



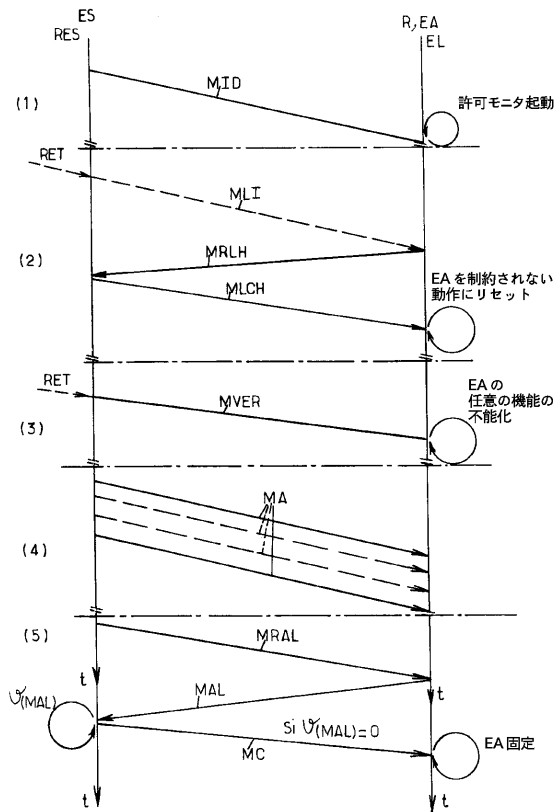
【図 3 a】



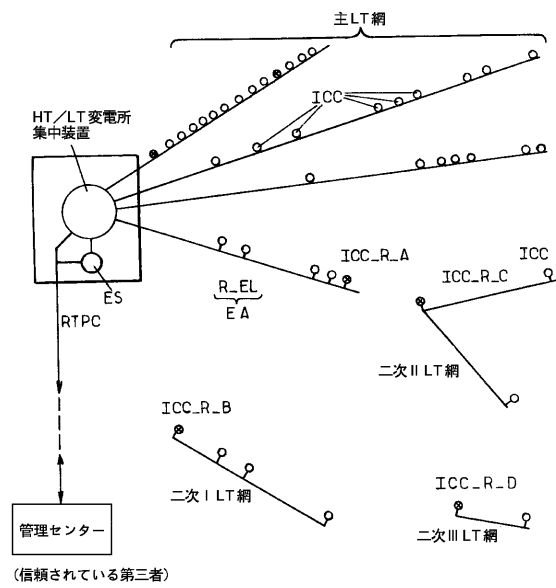
【図 3 b】



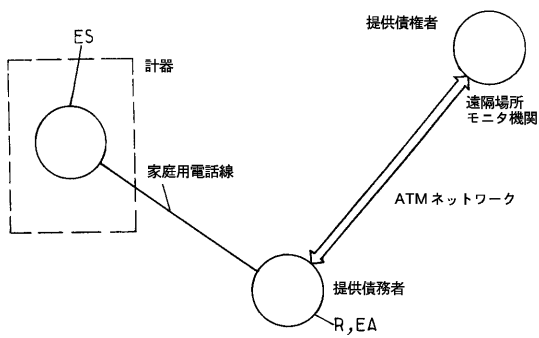
【図 4 a】



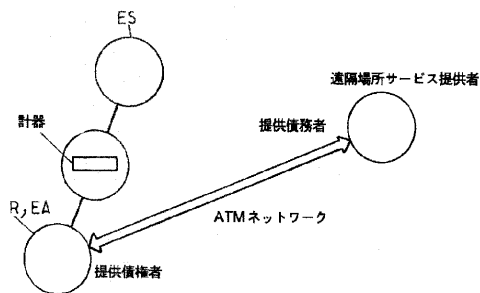
【図 4 b】



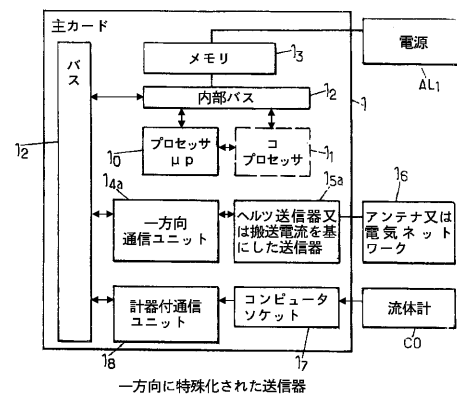
【図 5 a】



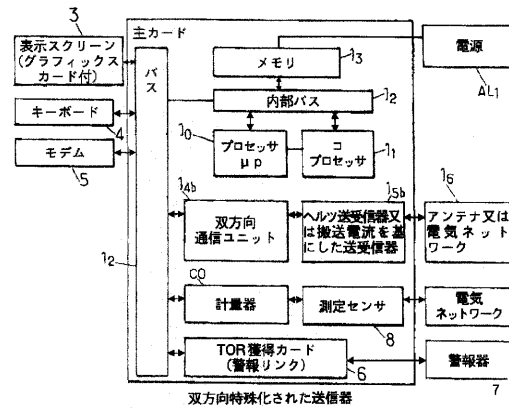
【図 5 b】



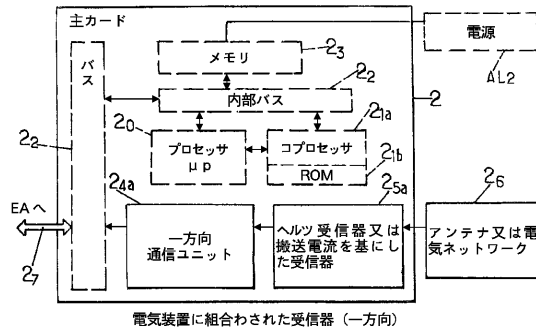
【図 6 a】



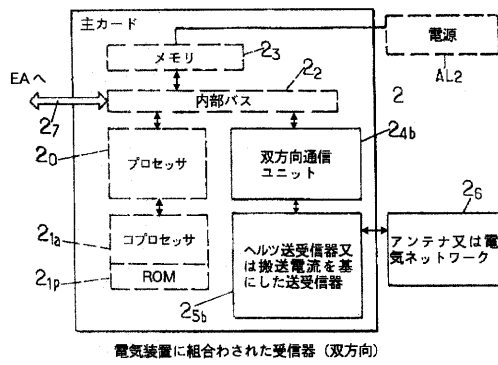
【図 6 b】



【図 7 a】



【図 7 b】



フロントページの続き

(74)代理人 100106297

弁理士 伊藤 克博

(72)発明者 マルタン、 フブリス

フランス国 エフー78180 モンテニ ル ブルトニュ ル ジェラール ド ネルヴァル
60

(72)発明者 フルリシュ、 ロベール

フランス国 エフー78380 ブジヴァル アンパース デュ オ ニュルジュ (番地なし)

(72)発明者 デルブクール、 イヴ

フランス国 エフー92330 ソー アレ ベルナドト 6

審査官 高野 誠治

(56)参考文献 国際公開第00/005820 (WO, A1)

特表平09-506500 (JP, A)

特開平09-312687 (JP, A)

登録実用新案第3007842 (JP, U)

英国特許出願公開第02229025 (GB, A)

国際公開第96/003728 (WO, A1)

(58)調査した分野(Int.Cl., DB名)

H02J 13/00

H04Q 9/00

H04Q 9/14