(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 601 476**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **86 10209**

(51) Int Cl⁴ : G 06 K 19/00; G 06 F 7/02.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 11 juillet 1986.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 2 du 15 janvier 1988.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *BULL CP8.* — FR.

(72) Inventeur(s) : Michel Hazard et Michel Hugon.

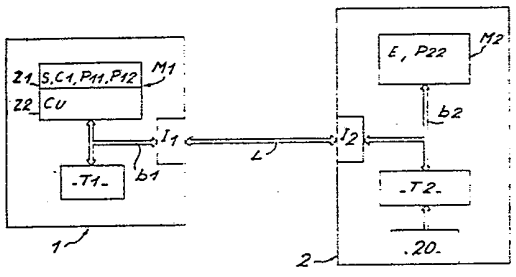
(73) Titulaire(s) :

(74) Mandataire(s) : M. Colombe.

(54) Procédé pour authentifier une donnée d'habilitation externe par un objet portatif tel qu'une carte à mémoire.

(57) La donnée d'habilitation C1 entrée dans un appareil 2 est chiffrée avec une information E prédéterminée pour donner un message M qui est transmis à un objet portatif 1. L'objet 1 déchiffre le message M en prenant en compte une donnée d'habilitation de référence C1 pour retrouver une information E' qui doit être cohérente avec l'information E.

L'invention s'applique notamment à la reconnaissance du code porteur du titulaire d'une carte de crédit.



FR 2 601 476 - A1

Procédé pour authentifier une donnée d'habilitation externe par un objet portatif tel qu'une carte à mémoire.

L'invention se rapporte à un procédé pour authentifier une donnée d'habilitation externe par un objet portatif tel qu'une carte à mémoire.

L'invention s'applique notamment à l'authentification d'un code confidentiel attribué au titulaire d'une carte à mémoire.

Dans la majorité des applications qui mettent en oeuvre une carte à mémoire, chaque titulaire d'une carte se voit attribuer un code confidentiel par un organisme habilité. Ce code propre au titulaire et qui personnalise sa carte est préenregistré dans la mémoire de la carte. L'organisme habilité enregistre également dans cette mémoire des informations ou paramètres qui définissent les limites d'utilisation de la carte, notamment les services qui peuvent être obtenus au moyen de cette carte.

Le titulaire accède à ces services par l'intermédiaire d'appareils auquel il accouple temporairement sa carte. Ces appareils n'entament généralement le processus de délivrance du service demandé qu'après des contrôles visant notamment à s'assurer que le porteur de la carte en est bien le titulaire et que la carte donne bien droit à la délivrance du service demandé. Bien que ces contrôles puissent varier d'un service à un autre, il en est un qui est toujours effectué sur le code confidentiel. Plus précisément, le porteur de la carte entre son code dans l'appareil, par l'intermédiaire d'un clavier par exemple, le code entré est ensuite transmis à la carte pour être comparé à celui préenregistré dans la mémoire. En cas d'égalité, le processus de délivrance continue, et en cas d'inégalité il y a automatiquement interruption du processus de délivrance du service demandé. Ce contrôle permet d'éviter l'utilisation de la carte par toute personne autre que son titulaire.

Cependant, un fraudeur en possession d'une carte volée a la possibilité de faire des essais en grand nombre jusqu'à trouver le bon code qui correspond à celui préenregistré dans la mémoire de la carte. Pour pallier une telle tentative de fraude, il est prévu dans la carte un compteur d'erreurs qui est incrémenté à chaque présentation d'un code erronné. Dès que ce compteur atteint un nombre prédéterminé, la carte est automatiquement rendue inutilisable ; Comme cela est décrit dans le brevet français n° 2 311 360.

Ce premier perfectionnement s'avère insuffisant si le fraudeur arrive à interdire ou inhiber la fonction de mémorisation de ce compteur en coupant l'alimentation de la carte à l'instant précis où le compteur doit être incrémenté. La détection de cet instant est possible par l'analyse des signaux échangés entre la carte et l'appareil. En effet, il suffit au fraudeur de repérer les signaux transmis par l'appareil qui correspondent à la tension d'écriture envoyée à la carte pour lui permettre d'écrire dans le compteur d'erreurs.

Un second perfectionnement décrit dans le brevet français n° 2 401 459 de la demanderesse permet d'éviter ce type de fraude en prévoyant un processus de traitement identique que le code présenté soit bon ou mauvais. En effet, sachant que le fraudeur peut repérer l'instant où l'appareil transmet la tension d'écriture à la carte et que cette tension n'est transmise que dans le cas où le code présenté à la carte est mauvais, le perfectionnement consiste à transmettre également une tension d'écriture à la carte même si le code présenté est bon. Ainsi, on réalise la symétrie des temps de traitement d'un code bon ou d'un code erroné de façon à ce qu'un fraudeur ne puisse tirer partie d'une différence entre ces temps de traitement.

Néanmoins, cette symétrie des temps de traitement est une contrainte pour le programmeur et, dans la pratique, il s'avère très difficile de pouvoir mettre en oeuvre cette contrainte.

Selon le procédé conforme à l'invention, la reconnaisance d'une donnée d'habilitation externe ne s'effectue pas par une simple comparaison entre cette donnée et la donnée d'habilitation de référence enregistrée dans la carte.

Le procédé conforme à l'invention permet d'obtenir des temps variables mis pour la reconnaissance d'une donnée d'habilitation, ce qui ne facilite pas la tâche d'un fraudeur qui observe les signaux échangés entre la carte et l'appareil.

L'invention propose donc un procédé pour authentifier une donnée d'habilitation par un objet portatif tel qu'une carte à mémoire comprenant des circuits de traitement, ladite carte étant accouplée à un appareil tel qu'un appareil de délivrance de services, caractérisé en ce qu'il consiste :

- au niveau de l'appareil, à élaborer un message chiffré par application d'une fonction de chiffrement d'un algorithme inversible mise en oeuvre par un programme enregistré dans une mémoire de l'appareil et exécuté par des circuits de traitement, ce programme prenant au moins en compte la donnée d'habilitation et une information prédéterminée (E), et à transmettre ce message à la carte,

- au niveau de la carte, à appliquer au message reçu la fonction de déchiffrement de l'algorithme par exécution d'un programme enregistré dans la mémoire de la carte et prenant en compte une donnée d'habilitation de référence

pour donner une information (E'), et à vérifier que cette information (E') est cohérente avec l'information (E).

Selon une autre caractéristique de l'invention, l'information (E) est calculée à partir d'au moins un résultat prédéterminé, un paramètre fixe ou variable propre à la carte et une clé secrète par application d'une fonction de chiffrement d'un algorithme inversible.

Selon une autre caractéristique de l'invention, on applique sur l'information (E') calculée par la carte, la fonction de déchiffrement de l'algorithme précité à partir du même paramètre fixe ou variable et de la même clé secrète pour obtenir un résultat qui doit être cohérent avec le résultat prédéterminé précité.

D'autres caractéristiques, avantages et détails du procédé conforme à l'invention vont être mis en évidence dans la description qui va suivre faite en référence aux dessins annexés dans lesquels :

- la figure 1 illustre le principe du procédé suivant un premier mode de réalisation,

- et la figure 2 illustre une variante de ce procédé.

Les figures montrent schématiquement les caractéristiques d'une carte à mémoire (1) et d'un appareil (2) tel qu'un appareil de délivrance de services, qui sont nécessaires à la mise en oeuvre du procédé conforme à l'invention.

La carte à mémoire (1) comprend essentiellement une mémoire (M1) et des circuits de traitement (T1) tels qu'un microprocesseur. Une telle carte est notamment décrite dans les brevets français N° 2 401 459 et 2 461 301 de la demanderesse.

Succintement, la mémoire (M1) comprend au moins deux zones de mémoire (Z1, Z2). La zone de mémoire (Z1) est inaccessible en écriture et en lecture depuis l'extérieur, alors que la zone de mémoire (Z2) n'est accessible qu'en lecture depuis l'extérieur. Par contre, ces zones (Z1, Z2) sont librement accessibles en lecture et en écriture par les circuits de traitement (T1).

La mémoire (M1) et les circuits de traitement (T1) échangent des informations par l'intermédiaire d'un bus (b1) qui véhicule des signaux de commande, d'adresse et de donnée. Le bus (b1) est relié à une interface d'entrée-sortie (I1).

L'appareil (2) se compose essentiellement d'une mémoire (M2), de circuits de traitement (T2) tels qu'un microprocesseur et d'un dispositif d'entrée (20) tel qu'un clavier par exemple. Les différents circuits de l'appareil (2) échangent des informations entre eux par l'intermédiaire d'un bus (b2) relié à une interface d'entrée-sortie (I2). Bien entendu, l'appareil comprend également tous les circuits nécessaires pour la délivrance du service pour lequel il a été conçu.

L'accouplement d'une carte (1) avec l'appareil (2) est réalisé par l'intermédiaire des deux interfaces (I1, I2) reliées entre elles par une liaison (L) électrique ou optique. A titre d'exemple, ces deux interfaces sont du type de celles décrites dans la demande de brevet français de la demanderesse publiée sous le N° 2 490 367, et l'interface (I2) de l'appareil (2) peut être avantageusement équipée du connecteur tel que décrit dans le brevet français de la demanderesse N° 2 445 560 pour accoupler de façon amovible la carte (1) à l'appareil (2). Enfin, le mode de dialogue ou de transmission des informations entre la carte (1) et l'appareil (2) peut

être avantageusement celui décrit dans le brevet français de la demanderesse N° 2 483 713.

Il va être décrit ci-après le principe du procédé conforme à l'invention suivant un premier mode de réalisataion décrit en référence à la figure (1).

Le procédé se décompose en deux phases. La première phase consiste à initialiser la carte et l'appareil, et la deuxième phase consiste dans la mise en oeuvre proprement dite du procédé pour la reconnaissance d'une donnée d'habilitation telle que le code confidentiel attribué au titulaire d'une carte à mémoire.

La phase d'initialisation consiste essentiellement à prédéterminer certaines informations et à les enregistrer soit dans la mémoire (M1) de la carte (1), soit dans la mémoire (M2) de l'appareil (2).

Un organisme habilité, c'est-à-dire l'organisme responsable d'un service qui peut être délivré par l'appareil (2) sur présentation d'une carte (1), contrôle cette phase d'initialisation avant de délivrer une carte.

Tout d'abord, l'organisme habilité prédétermine un résultat (Rk) et une clé secrète (S). Le résultat (Rk) est décomposé en plusieurs champs (Rk1, Rk2,..., Rkn) qui doivent satisfaire des conditions ou des relations prédéterminées.

A titre d'exemple, le résultat prédéterminé (Rk) est décomposé en trois champs (Rk1, Rk2, Rk3) tels que :

$$Rk1 = Rk2 = ad\ Cu$$

où (ad Cu) est l'adresse de mémoire d'un mot de la zone (Z2) de la mémoire (M1) de la carte (1), et (Cu) un

paramètre commun à toutes les cartes qui peuvent accéder au service délivré par l'appareil (2).

L'organisme habilité calcule alors une information (E) telle que :

$$E = f (Rk, S, Cu)$$

où (f) est la fonction directe d'un algorithme inversible (A1) par exemple tel que celui décrit dans la demande de brevet français publiée sous le n° 2 566 155. Ce calcul est exécuté sur toute machine connue en soi ayant une mémoire et des circuits de traitement appropriés ou de préférence par les circuits de traitement d'une carte semblable à la carte (1) pour mieux protéger la fonction (f) et la clé secrète (S).

La phase d'initialisation se termine par l'enregistrement de données dans la mémoire (M1) de la carte (1) et dans la mémoire (M2) de l'appareil (2).

On enregistre dans la zone de mémoire (Z1) de la mémoire (M1) de la carte (1), la clé secrète (S) précitée, un programme (P11) qui est la mise en oeuvre de la fonction inverse (f^{-1}) de l'algorithme (A1) précité, un programme (P12) qui est la mise en oeuvre de la fonction inverse (g-1) d'un second algorithme (A2) dont le rôle sera explicité plus loin, ainsi qu'un code confidentiel (C1) qui sera ensuite attribué au titulaire de la carte (1). La zone de mémoire (Z1) est ensuite verrouillée pour rendre ces informations inaccessibles de l'extérieur, mais accessibles en interne par les circuits de traitement (T1) de la carte (1).

On enregistre dans la zone (Z2) de la mémoire (M1) de la carte (1) le paramètre (Cu) précité, et la zone de mémoire (Z2) est ensuite verrouillée en écriture de l'extérieur.

On enregistre dans la mémoire (M2) de l'appareil (2) l'information (E) calculée précédemment, ainsi qu'un programme (P22) qui est la mise en oeuvre de la fonction directe (g) du second algorithme (A2) précité.

L'appareil (2) est en état de fonctionnement et l'organisme habilité délivre la carte (1) ainsi personnalisée à un titulaire en lui attribuant le code confidentiel (C1) que le titulaire doit garder secret. Bien entendu, la clé secrète (S) n'est pas dévoilée au titulaire de la carte et est seule connue de l'organisme habilité.

La phase de reconnaissance d'un code confidentiel ainsi attribué au porteur d'une carte s'effectue de la manière décrite ci-dessous.

Une fois la carte (1) accouplée à l'appareil (2), le porteur de la carte entre un code confidentiel (C1) au clavier (20) de l'appareil (2). Ce code (C1) est combiné ensuite avec l'information (E) préenregistrée dans la mémoire (M2) de l'appareil (2).

D'une façon générale, cette combinaison consiste à appliquer la fonction directe (g) mise en oeuvre par le programme (P22) du second algorithme inversible (A2) qui est par exemple du même type que l'algorithme (A1).

Les circuits de traitement (T2) exécutent ce programme (P22) qui prend en compte l'information (E) et le code confidentiel (C1) entré au clavier (20) pour donner un message chiffré (M) tel que :

$$M = g\ (E,\ C1)$$

Ce message (M) est ensuite transmis à la carte (1) par la ligne de transmission (L). Le code confidentiel (C1) entré

au clavier est noyé dans le message (M) et est donc bien protégé pendant sa transmission. La première opération effectuée par la carte (1) est de faire appliquer la fonction inverse (g^{-1}) du second algorithme (A2) sur le message d'entrée (M).

Plus précisément, les circuits de traitement (T1) de la carte (1) exécutent un programme (P12) qui est la mise en oeuvre de la fonction inverse (g^{-1}) et qui a été préenregistré dans la zone (Z1) de la mémoire (M1) de la carte (1) pendant la phase d'initialisation. Ce programme (P12) prend en compte le message (M) et le code confidentiel de référence (C1) préenregistré dans la mémoire (M1) par l'organisme habilité avant délivrance de la carte. L'exécution de ce programme donne une information (E') telle que :

$$E' = g^{-1} (M, C1).$$

Si le code (C1) entré au clavier 20 et le code (C1) de référence sont identiques, l'information (E') sera identique à l'information (E) précédente. La deuxième opération effectuée par la carte (1) est de faire appliquer la fonction inverse (f^{-1}) du premier algorithme (A1) sur l'information (E').

Plus précisément, les circuits de traitement (T1) exécutent le programme (P11) préenregistré dans la mémoire (M1) de la carte (1) pendant la phase d'initialisation. Ce programme (P11) prend en compte l'information (E'), la clé secrète (S) et le paramètre (Cu) préenregistrés dans la carte (1) pour aboutir à un résultat (R'k) tel que :

$$R'k = f^{-1} (E', S, Cu)$$

Une fois le résultat (R'k) calculé, la carte vérifie que ce résultat satisfait une relation prédéterminée pour

prouver que les deux codes (C1) sont identiques et que le porteur de la carte (1) présentée à l'appareil (2) est bien le titulaire de la carte (1).

Du fait de l'utilisation d'un algorithme inversible, le résultat (R'k) doit être identique au résultat prédéterminé (Rk) qui a permis de calculer l'information (E) d'origine, à condition bien entendu que les codes (C1) soient identiques.

Le résultat (R'k) doit satisfaire la même relation que celle satisfaite par le résultat (Rk) et telle que :

$$R'k = R'k1, R'k2, R'k3$$

$$\text{avec} \quad R'k1 = R'k2 = \text{ad Cu}$$

où (ad Cu) est l'adresse mémoire à laquelle est enregistré le paramètre (Cu) dans la zone (Z2) de la mémoire (M1) de la carte (1).

Ainsi, le porteur de la carte (1) ne sera pas reconnu comme son titulaire si le code (C1) entré au clavier (20) de l'appareil (1) n'est pas identique au code (C1) préenregistré dans la carte (1). En effet, si les deux codes sont différents, la carte (1) en combinant le message (M) reçu et le code (C1) ne retrouvera pas l'information (E) d'origine, et le résultat (R'k) calculé par la carte (1) ne pourra pas satisfaire la relation prédéterminée définie à partir de l'information d'origine (E).

Selon une caractéristique importante de l'invention, le temps de traitement par la carte (1) d'un message chiffré (M) est variable d'un code confidentiel (C1) à l'autre. Pour cela il suffit qu'au moins l'un des algorithmes (A1,

A2) prennent en compte un paramètre qui correspond à une partie du code confidentiel (C1) à traiter. Ce paramètre peut par exemple déterminer le nombre de fois que l'on doit parcourir une boucle de programme dans l'algorithme.

A titre d'exemple et selon un type particulier de réalisation de l'invention les fonctions (g) et (g^{-1}) sont identiques et sont chacune mise en oeuvre par une fonction OU EXCLUSIF.

Le principe de base de l'invention tel qu'illustré en référence à la figure 1, peut être amélioré par l'utilisation d'une information (E) variable pour que le message (M) communiqué à la carte ne soit jamais le même pour un même code confidentiel entré dans l'appareil.

Pour que ce message (M) soit variable, il suffit que le paramètre (Cu) soit variable pour une même carte (1). Dans cette variante illustrée à la figure 2, la zone (Z2) de la mémoire (M1) de la carte (1) est alors une zone de contrôle telle qu'à chaque utilisation de la carte (1) au moins un bit de cette zone est modifié. Le paramètre (Cu) est alors le mot mémoire de la zone (Z2) qui contient le dernier bit modifié lors de la précédente utilisation de la carte (1).

Le paramètre (Cu) étant variable et spécifique à chaque carte, l'appareil (2) doit calculer à chaque fois l'information (E) telle que :

$$E = f(Rk, S, Cu).$$

Pour effectuer ce calcul, la mémoire (M2) de l'appareil (2) doit contenir un programme (P11) correspondant à la fonction (f) de l'algorithme (A1) précité et la clé secrète (S). En outre, l'appareil définit à chaque fois un résultat (Rk) tel que :

$$Rk = Rk1, Rk2, Rk3$$

avec $$Rk1 = Rk2 = ad\ (Cu).$$

Bien entendu, la carte (1) communique à l'appareil (2) le paramètre (Cu) et son adresse (ad) pour permettre le calcul de l'information (E). L'information (E) est ensuite traitée comme dans le mode de réalisation précédent.

Comme les informations à caractère secret sont protégées dans la carte, il faut prendre des mesures de protection pour les informations à caractère secret enregistrées dans la mémoire (M2) de l'appareil (2). Une solution consiste à prendre des algorithmes (A1, A2) du type à clé publique. Une autre solution consiste à intégrer la mémoire (M2) et les circuits de traitement (T2) dans des plaquettes semi-conductrices (puces) séparées ou non et montées dans un boîtier (2'). Avantageusement ces boîtiers sont conçus conformément aux brevets français n° 2 401 459 et 2 461 301 de la demanderesse et montés dans un support portatif tel qu'une carte à mémoire normalisée identique à la carte (1).

Dans l'exemple précédent, le résultat (Rk) est tel que les champs (Rk1) et (Rk2) sont identiques et chacun est égal à l'adresse mémoire du paramètre (Cu).

Cette condition peut évidemment être toute autre et ne pas faire intervenir obligatoirement l'adresse du paramètre (Cu).

Les exemples décrits se rapportent à la reconnaissance du code confidentiel (PIN : Personal Identification Number), mais le procédé s'applique plus généralement à la reconnaissance d'une donnée d'habilitation externe à la carte (1) et qui doit être authentifiée par la carte pour

la poursuite du dialogue entre la carte (1) et l'appareil (2).

Revendications :

1. Procédé pour authentifier une donnée d'habilitation externe par un objet portatif tel qu'une carte à mémoire comprenant des circuits de traitement, ladite carte étant accouplée à un appareil tel qu'un appareil de délivrance de services, caractérisé en ce qu'il consiste :

- au niveau de l'appareil (2), à élaborer un message (M) par application d'une fonction de chiffrement d'un algorithme inversible (A2) mise en oeuvre par un programme (P22) enregistré dans une mémoire (M2) de l'appareil (2) et exécuté par des circuits de traitement (T2), ce programme prenant au moins en compte la donnée d'habilitation (C1) et une information (E) prédéterminée, et à transmettre ce message (M) à la carte (1),

- au niveau de la carte (1), à appliquer au message (M) la fonction de déchiffrement de l'algorithme (A2) par exécution d'un programme (P12) enregistré dans la mémoire (M1) de la carte (1) et prenant en compte une donnée d'habilitation de référence (C1) pour donner une information (E'), et à vérifier que cette information (E') est cohérente avec l'information (E).

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à prédéterminer l'information (E) à partir d'au moins un résultat (Rk), un paramètre (Cu) propre à la carte (1) et une clé secrète (S).

3. Procédé selon la revendication (2), caractérisé en ce qu'il consiste à calculer l'information (E) par application de la fonction de chiffrement d'un algorithme inversible (A1) tel que :

$$E = f(Rk, S, Cu)$$

4. Procédé selon la revendication 3, caractérisé en ce qu'il consiste pour vérifier la cohérence de l'information

(E') calculée par la carte (1), à appliquer sur cette information la fonction de chiffrement de l'algorithme (A1) pour obtenir un résultat (R'k) tel que :

$$R'k = f^{-1} (E', S, Cu)$$

et à vérifier que ce résultat (R'k) est cohérent avec le résultat (Rk).

5. Procédé selon l'une des revendication 2 à 4, caractérisé en ce qu'il consiste à donner au résultat (Rk) la forme :

$$Rk = Rk1, Rk2, Rk3$$

avec au moins Rk1 ou Rk2 ou Rk3 égal à l'adresse mémoire du paramètre (Cu).

6. Procédé selon l'une des revendications 2 à 5, caractérisé en ce qu'il consiste à prendre un paramètre (Cu) variable pour faire varier l'information (E) et le message (M).

7. Procédé selon la revendication 6, caractérisé en ce qu'il consiste à réserver une zone de mémoire (Z2) de la mémoire (M1) de la carte (1), à modifier l'état d'au moins un bit de cette zone après chaque utilisation de la carte (1), et à prendre comme paramètre (Cu) le mot mémoire de cette zone (Z2) qui contient le bit précédemment modifié.

8. Procédé selon l'une des revendications précédentes, caractérisé en ce que les algorithmes (A1, A2) sont des algorithmes à clé publique.

1,2

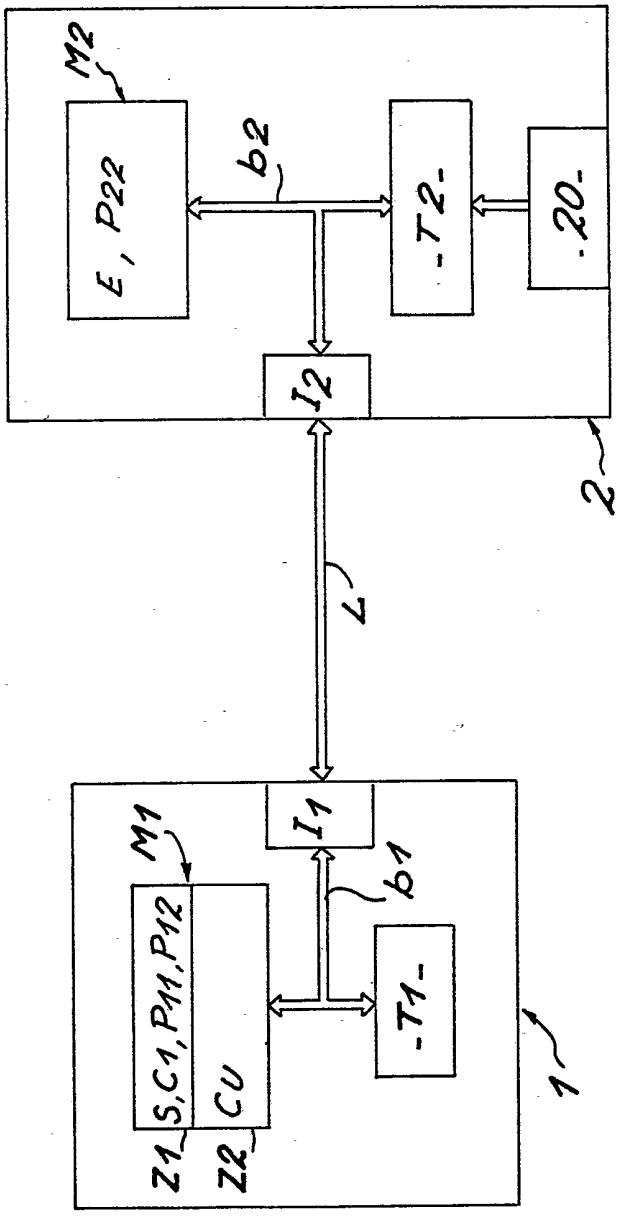


FIG. 1

FIG. 2