(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 831 297**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **02 13148**

(51) Int Cl[7] : **G 06 F 17/60,** H 04 L 9/30

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 22.10.02.

(30) **Priorité :** 22.10.01 DE 10151278.

(43) **Date de mise à la disposition du public de la demande :** 25.04.03 Bulletin 03/17.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

(71) **Demandeur(s) :** *ROBERT BOSCH GMBH Gesellschaft mit beschränkter Haftung* — DE.

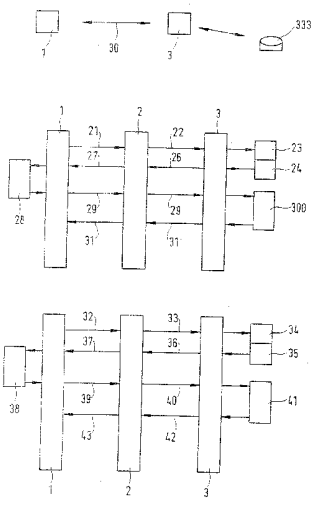
(72) **Inventeur(s) :** DRAEGER GERD et SKWAREK VOLKER.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET HERRBURGER.

(54) PROCEDE DE PRESTATION DE SERVICE PAR UN PRESTATAIRE DE SERVICE ET INSTALLATION POUR LA MISE EN OEUVRE DU PROCEDE.

(57) Procédé et installation pour fournir les services d'un prestataire de service (2) à un utilisateur (1) après requête envoyée au prestataire (2). L'utilisateur reçoit alors une offre de service. En cas d'accord avec l'offre, l'utilisateur (1) code au moins un élément de l'information qui contenait l'offre de service. La libération du service est faite par le prestataire de service (2) après que ce dernier ait reçu d'une comptabilité des services (3) une confirmation établie par cette comptabilité après contrôle de l'élément codé.



FR 2 831 297 - A1

Etat de la technique

On connaît déjà des services de télématique offerts à l'utilisateur contre paiement. En particulier dans un modèle de taxation dépendant de l'accès il est nécessaire que les unités soumises à taxation ainsi que le nombre d'accès, la nature du service et aussi la durée de l'accès soient saisis de manière protégée contre les manipulations et soient attribués sans équivoque à l'utilisateur correct.

Il existe actuellement différents procédés de comptabilité :

- l'utilisateur signe un contrat avec le prestateur de service de télématique. A chaque accès à un service, l'utilisateur s'identifie vis-à-vis du prestataire. Cela permet de saisir précisément les taxes et de les attribuer. Mais l'utilisateur doit conclure à un contrat individuel avec le prestataire de service,
- le prestataire de service présente, comme pour un numéro de service soumis à taxe, une modalité de décompte avec un prestataire sur mobile qui permet l'accès à ces services. Pour ne pas limiter toutefois le groupe d'utilisateur, il faut prévoir une convention entre le prestataire de service et tous les fournisseurs de services mobiles,
- il existe des entreprises spécialisées pour le décompte des activités de commerce sur les mobiles. Lorsqu'un utilisateur interroge un service de télématique, le prestataire de service lance une interrogation auprès de l'entreprise de comptabilité transmettant par exemple les taxes concernées et le numéro du mobile de l'utilisateur. Puis du côté de l'entreprise de comptabilité il y a une authentification qui se fait de manière séparée de l'utilisateur pour libérer la somme concernée. Cette libération est ensuite confirmée auprès du prestataire de service.

Avantages de l'invention

La présente invention concerne à cet effet un procédé de fourniture de service par un prestataire de service comprenant les étapes suivantes :

- un utilisateur reçoit une clé privée d'une comptabilité des services,
- l'utilisateur envoie une requête au prestataire de service pour recevoir un service du prestataire,
- en retour à sa requête, l'utilisateur reçoit une offre de service du prestataire de service,
- en cas d'accord de l'utilisateur avec l'offre de service, l'utilisateur code au moins un élément de l'information contenu dans l'offre de service

avec sa clé privée et envoie l'information en retour au prestataire de service qui la transmet à la comptabilité des services,

- la libération du service pour l'utilisateur est faite par le prestataire de service après qu'il ait reçu de la comptabilité des services une confirmation établie par la comptabilité des services à partir du contrôle de l'élément codé.

Selon d'autres caractéristiques du procédé :

- pour une requête du prestataire de service, il y a émission d'une caractéristique publique de l'utilisateur ;
- le prestataire de service transmet une caractéristique univoque de la caractéristique de service demandée et la caractéristique publique de l'utilisateur à la comptabilité des services ;
- la comptabilité des services génère une clé à partir de la caractéristique publique transmise de l'utilisateur, clé que l'utilisateur peut décoder avec sa clé privée qu'il a reçue au préalable de la comptabilité des services ;
- la comptabilité des services code un numéro de transaction qui désigne de manière univoque l'opération de décompte ;
- la comptabilité des services code non seulement le numéro de transaction codé mais également la caractéristique de service ;
- le prestataire de service envoie l'information codée que lui a renvoyé la comptabilité des services avec l'identification de la caractéristique de service demandée, par exemple le prix, et envoie l'ensemble à l'utilisateur comme offre de service ;
- l'offre de service est envoyée à l'utilisateur en même temps qu'une demande de confirmation de service ;
- l'utilisateur, pour contrôler l'offre de service, décode l'information avec sa clé privée et en cas d'accord avec l'offre de service, il renvoie au moins un élément de l'information, notamment le numéro de transaction, après codage avec sa clé privée au prestataire de service ;
- la comptabilité des services analyse la confirmation de service reçue de manière codée par l'utilisateur et par l'intermédiaire du prestataire de service et après contrôle du prestataire de service, notamment après comptabilisation du compte d'utilisateur, envoie une confirmation pour libérer le service par le prestataire de service.

Le procédé selon l'invention ou l'installation pour sa mise en œuvre permet de fournir les services d'un prestataire de service à un utilisateur de service et de comptabiliser les services par une comptabilité

des services indépendamment du prestataire de service ou du prestataire de service de mobile, sans avoir à établir un autre canal de communication du côté de l'utilisateur du service. Dans le procédé décrit ci-dessus, il faut, au contraire, un autre canal de communication entre celui qui fait le décompte du service et l'utilisateur du service, ce qui nécessite la mise en œuvre de moyens importants à la fois du point de vue technique et logistique.

Dans le procédé selon l'invention, on a une confirmation d'une prestation de service payante, par exemple pour le commerce (e) et/ou le commerce (m) par l'utilisateur du service par rapport à celui qui fait le décompte du service. Dans ce cas, le canal utilisé pour la prestation de service peut également s'utiliser avec une protection contre les manipulations frauduleuses, pour confirmer le paiement au comptable du service.

L'avantage du procédé de l'invention est notamment que l'utilisateur peut demander tous les services payants utilisant ce procédé, dès qu'il est enregistré auprès d'une comptabilité (comptabilité des services). De tels postes de comptable peuvent être par exemple des instituts de crédit (carte Visa, Paybox) ou aussi des banques et des caisses d'épargne. Il n'y a pas lieu de conclure des contrats d'utilisation individuels avec les prestataires de service si bien que tous les services concernés peuvent être utilisés immédiatement et indépendamment du fournisseur de communication.

L'utilisateur communique selon le procédé de l'invention pour les services pris en compte et le décompte uniquement par un canal de communication avec le prestataire de service. Le décompte des services n'apparaît pas publiquement.

La sécurité contre les manipulations frauduleuses est garantie car l'utilisateur renvoie un élément de l'information dans lequel était contenue l'offre de service de façon codée avec son code privé vers le prestataire de service qui assure ensuite le décompte. Le prestataire de service ne libère le service souhaité que si la comptabilité des services lui a fourni une confirmation établie par le prestataire de service du fait du contrôle de l'élément codé. Le paquet de données de l'information codée pourrait dans ce cas n'être codé que par l'utilisateur autorisé avec son code privé.

Pour cela, l'installation selon l'invention comporte :

- des moyens pour activer une clé privée reçue d'une comptabilité des services,
- une unité d'émission pour émettre une requête à destination d'un prestataire de service pour prendre en compte les services,
- une unité de réception pour recevoir une offre de service d'un prestataire de service,
- des moyens pour décoder une information codée contenant l'offre de service ainsi que des moyens pour exploiter l'information décodée,
- des moyens pour générer une nouvelle information avec codage d'au moins un élément d'information décodé avec la clé privée, et
- des moyens pour recevoir les services d'un prestataire de service après libération par le prestataire de service sur contrôle de l'élément codé.

Dessins

La présente invention sera décrite ci-après de manière plus détaillée à l'aide d'exemples de réalisation représentés dans les dessins annexés dans lesquels :

- la figure 1 montre un procédé d'annonce dans un calculateur de service,
- la figure 2 montre le déroulement des opérations pour une requête de service,
- la figure 3 montre le déroulement des opérations lors de la mise en œuvre d'un service d'un prestataire de service,
- la figure 4 montre un schéma par blocs d'une installation pour la mise en œuvre d'un service d'un prestataire de service.

Description des exemples de réalisation

Pour les services payants comme par exemple les services de télématique, il faut une convention entre l'utilisateur 1 et la comptabilité des services 3, par exemple un institut de crédit ou une banque. Pour cela, un utilisateur 1 informe selon la figure 1, la comptabilité des services 3 selon la phase 30 en indiquant un numéro d'utilisateur convenu servant de caractéristique officielle. La comptabilité des services 3 gère un compte client 333 avec l'attribution : numéro d'utilisateur, code d'utilisateur, auprès de la comptabilité des services 3 et, en option, les limites du crédit. Le procédé est protégé si la clé reste secrète. La clé privée (secrète) est communiquée à l'utilisateur 1 par la comptabilité des services 3 pour l'utilisation du compte client. L'utilisateur 1 autorise la comptabilité des services 3 pour mettre à sa charge sur son compte client 33 si l'utilisateur est authentifié de manière appropriée pour une telle opération.

L'opération d'authentification peut se dérouler de la manière suivante selon l'invention comme le montre la figure 2 :

1. l'utilisateur 1 sélectionne un service et demande la fourniture d'une caractéristique officielle (numéro d'utilisateur) au point 21,
2. le prestataire de service 2 indique une caractéristique non équivoque du service comme de préférence le prix et la caractéristique officielle de l'utilisateur 1, informations transmises à la comptabilité des services 3 (22). Si le prix n'a pas été transmis comme caractéristique de service non équivoque, le prix est transmis séparément par le calculateur de service,
3. le calculateur de service 3 peut générer une clé 23 à partir de la caractéristique officielle, clé que l'utilisateur 1 recevra ultérieurement du fait des connaissances reçues par sa clé privée,
4. avec cette clé, la comptabilité des services 3 code un numéro de transaction TAN (24) qui doit être sans équivoque du point de vue de l'utilisateur 1 et de l'opération de décompte. Au choix, on peut également coder la caractéristique de service, unique, au point 2. Le numéro TAN est de préférence valable seulement dans un intervalle de temps donné,
5. l'information codée est renvoyée au prestataire de service 2 (26) pour être mise ainsi d'une manière non équivoque en relation avec l'utilisateur 1 envoyant la requête,
6. le prestataire de service 2 accroche la caractéristique de service non équivoque selon le point 2 comme par exemple le prix à l'information. Cette information est transmise (27) à l'utilisateur 1 par le canal d'interrogation comme offre de service. La transmission se fait de préférence en liaison avec la requête de confirmation de service.
7. L'utilisateur 1 reçoit l'information et grâce à sa clé privée il est en mesure de décoder (28) l'information TAN et le cas échéant la caractéristique de service, sans équivoque, codée par le calculateur de service 3. Du fait du code privé, on peut s'assurer que seul l'utilisateur 1 peut décoder le paquet. Inversement, l'interrogation peut également être faite par l'utilisateur 1 de sorte qu'il ne peut y avoir de mauvais calcul. La caractéristique de service peut être comparée alors par l'utilisateur 1 ou à un terminal avec la caractéristique de service fournie par le prestataire de service pour déterminer s'il s'agit de la même caractéristique et ainsi de la même prestation. Pour cette raison, la solution la

plus sûre consiste à utiliser le prix comme caractéristique de service non équivoque.

8. L'utilisateur 1 réagit de manière correspondante à la requête de conformation. Dans le cas d'une confirmation négative, on effectue l'opération. Dans le cas d'une confirmation positive (accord de l'utilisateur) l'utilisateur 1 code un élément de l'information contenant l'offre de service, spécialement le code TAN des points 6 et 7 pour les remettre sur sa clé privée. La caractéristique selon laquelle le prestataire de service a envoyé au point 6 l'information est codée de même. Cela garantit que le prestataire de service 2 a offert à l'utilisateur la même caractéristique de service univoque, comme celle qu'il a donné à la comptabilité des services 3 pour faire le compte de la mission et que seul l'utilisateur de cette caractéristique a codé dans le paquet renvoyé. Le paquet de données doit avoir un aspect différent que celui envoyé au point 5. Le paquet confirmé est renvoyé (29) par le prestataire de service 2 à la comptabilité des services 3 avec la caractéristique officielle. En option, l'utilisateur selon le procédé cryptographique connu de manière générale, ajoute des compléments à cette information même si pour deux interrogations identiques, les réponses étaient aléatoires.
9. La comptabilité des services 3 reçoit et analyse le paquet (300).
   - Comme il correspond à une autre structure, le prestataire de service 2 ne peut pas simplement le copier et le renvoyer.
   - Comme le numéro TAN existe en liaison avec la caractéristique de service et la caractéristique officielle au point 4, du fait de la sélection systématiquement non retenue du numéro TAN, il n'y a pas d'opération antérieure que le prestataire de service pourrait copier.
   - Comme au point 4 on a envoyé également une caractéristique de service non équivoque codée, qui a pu être contrôlée en même temps que l'information non codée de l'utilisateur 1 ou le cas échéant la caractéristique de service rajoutée, de l'utilisateur 1, avec le prestataire de service 2, cela permet de garantir que le prestataire de service 2 fait le décompte vis-à-vis de l'utilisateur 14 de la même caractéristique de service que par rapport à la comptabilité des services 3.
   - Comme cette information pourrait être interprétée, l'utilisateur 1 doit la coder et la décoder avec une clé valable. En conséquence, il doit s'agir de l'utilisateur ayant une caractéristique indiquée de manière publique.

Ces contrôles confirment à la comptabilité des services 3 que l'utilisateur 1 connaît la caractéristique de service objet du décompte comme par exemple le prix, qu'il s'agit de l'utilisateur 1 et que cet utilisateur 1 a la priorité.

Si l'étape précédente s'est déroulée de manière positive la comptabilité des services 3 confirme au prestataire de service 2 que le compte de l'utilisateur sera débité (31). Maintenant le prestataire de service 2 fournira à l'utilisateur de service, le service de manière habituelle (c'est-à-dire qu'il libérera le service).

Un exemple de réalisation sera décrit ci-après à l'aide de la figure 3.

L'utilisateur 1 se signale avec une caractéristique d'utilisateur qui lui est propre, par exemple le numéro de son terminal (Nu 007) auprès de la comptabilité des services 3, par exemple les services de cartes Visa et reçoit une clé privée que l'utilisateur 1 est seul à connaître. Sans autres signalisations, l'utilisateur 1 souhaiterait utiliser le service payant d'un prestataire de service 2, par exemple d'un service de navigation non embarqué avec transmission téléphonique. Ce prestataire de service 2 est en mesure de décompter le service auprès de la comptabilité des services 3.

L'utilisateur 1 démarre par une requête de trajet 32 et envoie une caractéristique d'utilisateur (Nu 007) d'une manière non codée. Celle-ci est transmise par le prestataire de service 2 avec une caractéristique de service univoque (DM 3,99) à la comptabilité des services 3 (33). Celle-ci génère un numéro aléatoire de transaction (TAN 1234) (34) et la conserve en mémoire en liaison avec la caractéristique de service (DM 3,99) et la caractéristique d'utilisateur (Nu 007). Du fait de cette caractéristique d'utilisateur (Nu 007), la comptabilité des services 3 génère une clé ou une information que l'utilisateur 1 peut de nouveau décoder (35) avec sa clé privée. Avec la clé générée ou avec l'information générée, on code le numéro de transaction (TAN 1234) et en option la caractéristique de service arrive de manière non codée. Le prestataire de service 2 reçoit ce paquet de données pour sa transmission (36). Le prestataire de service 2 accroche la caractéristique de service (DM 3,99) de manière non codée au paquet de données reçu de la comptabilité des services 3.

La comptabilité des services 3 fournit alors l'offre de service (37), par exemple une liste de destinations avec chaque fois en dehors de l'élément codé pour l'utilisateur 1, la caractéristique de service univoque

(DM 3,99). La caractéristique de service (DM 3,99) est indiquée à l'utilisateur 1 qui la confirme. En même temps, il confirme par exemple une destination dans la liste des destinations. Par la confirmation, le numéro TAN (TAN 1234) qui a été décodé dans l'étape précédente, est de nouveau codé (38) avec la clé privée en même temps que la caractéristique de service (DM 3,99). Le paquet de données ainsi formé pourrait être généré seulement par l'utilisateur 1 car

- lui seul peut décoder le numéro TAN (TAN 1234) et recoder avec la caractéristique de service (DM 3,99) pour en former un paquet commun et
- ce paquet ne peut concerner que cette commande car les numéros TAN (TAN 1234) sont mis en relation par les services de la carte Visa, de manière spécifique à la commande, aléatoirement avec le numéro d'utilisateur et la caractéristique de service. Dans ces conditions il ne peut pas s'agir de la copie d'une ancienne requête et de sa confirmation.

Ce paquet est renvoyé au prestataire de service 2 (39) qui le transmet à la comptabilité des services 3 (40). La comptabilité des services 3 est alors en mesure de décoder le paquet de données et les numéros d'utilisateur (Nu 007, TAN 1234) et la caractéristique de service (DM 3,99) de cette combinaison pour en contrôler la véracité (41).

Si l'information est vraie, le montant dû est débité du compte d'utilisateur ; le montant correspondant est porté au crédit du compte du prestataire de service 2 et le solde de l'opération est indiqué au prestataire de service 2 (42). Puis le service est libéré, c'est-à-dire que le trajet demandé est fourni à l'utilisateur 43.

La figure 4 montre un schéma par blocs d'une installation du côté de l'utilisateur pour la prise en compte d'un service d'un prestataire. Pour l'émission des requêtes de service et des confirmations il est prévu une unité d'émission 12. L'unité de réception 11 permet à l'utilisateur 1 de recevoir les offres de service et les services libérés. La clé privée est introduite par exemple à l'aide de l'installation d'entrée 13 chaque fois par l'utilisateur 1. Pour décoder les informations reçues, il est prévu une installation de décodage 14. Celle-ci est commandée de manière appropriée par l'installation d'entrée de clé 13 pour permettre un décodage. Après exploitation de l'information décodée par l'installation d'exploitation 15, le générateur 16 peut combiner de nouvelles informations ou des éléments d'informations reçues à la clé privée, codé de façon

commandée par l'installation d'entrée 13 pour envoyer des confirmations authentifiées au prestataire de service 2. Les services libérés sont reçus de préférence par l'intermédiaire du mêle canal de communication par le prestataire de service 2 et dans l'unité 17. Cette unité 17 peut être équipée d'un afficheur 18, par exemple un moyen de visualisation des services revendiqués tels que les trajets ou autres graphiques et/ou moyens d'affichage d'informations de texte. Pour reproduire l'information de trajet qui se trouve déjà chez l'utilisateur 1, par exemple des données cartographiques sur l'afficheur 18, il est prévu une mémoire 19. Comme support de mémoire on peut utiliser par exemple une carte CD.

REVENDICATIONS

1°) Procédé de fourniture de service par un prestataire de service comprenant les étapes suivantes :

- un utilisateur (1) reçoit une clé privée d'une comptabilité des services (3),
- l'utilisateur (1) envoie une requête au prestataire de service (2) pour recevoir un service du prestataire (2),
- en retour à sa requête, l'utilisateur (1) reçoit une offre de service du prestataire de service (2),
- en cas d'accord de l'utilisateur (1) avec l'offre de service, l'utilisateur (1) code au moins un élément de l'information contenu dans l'offre de service avec sa clé privée et envoie l'information en retour au prestataire de service (2) qui la transmet à la comptabilité des services (3),
- la libération du service pour l'utilisateur (1) est faite par le prestataire de service (2) après qu'il (2) ait reçu de la comptabilité des services (3) une confirmation établie par la comptabilité des services (3) à partir du contrôle de l'élément codé.

2°) Procédé selon la revendication 1,
caractérisé en ce que
pour une requête du prestataire de service (2), il y a émission d'une caractéristique publique de l'utilisateur (1).

3°) Procédé selon l'une quelconque des revendications 1 ou 2,
caractérisé en ce que
le prestataire de service (2) transmet une caractéristique univoque de la caractéristique de service demandée et la caractéristique publique de l'utilisateur (1) à la comptabilité des services (3).

4°) Procédé selon la revendication 1,
caractérisé en ce que
la comptabilité des services (2) génère une clé à partir de la caractéristique publique transmise de l'utilisateur (1), clé que l'utilisateur (1) peut décoder avec sa clé privée qu'il a reçue au préalable de la comptabilité des services (3).

5°) Procédé selon la revendication 4,
caractérisé en ce que

la comptabilité des services (3) code un numéro de transaction (TAN) qui désigne de manière univoque l'opération de décompte.

6°) Procédé selon la revendication 5,
caractérisé en ce que
la comptabilité des services (3) code non seulement le numéro de transaction codé mais également la caractéristique de service.

7°) Procédé selon l'une quelconque des revendications 5 ou 6,
caractérisé en ce que
le prestataire de service (2) envoie l'information codée que lui a renvoyé la comptabilité des services (3) avec l'identification de la caractéristique de service demandée, par exemple le prix, et envoie l'ensemble à l'utilisateur (1) comme offre de service.

8°) Procédé selon la revendication 7,
caractérisé en ce que
l'offre de service est envoyée à l'utilisateur (1) en même temps qu'une demande de confirmation de service.

9°) Procédé selon la revendication 1,
caractérisé en ce que
l'utilisateur (1), pour contrôler l'offre de service, décode l'information avec sa clé privée et en cas d'accord avec l'offre de service, il renvoie au moins un élément de l'information, notamment le numéro de transaction, après codage avec sa clé privée au prestataire de service (2).

10°) Procédé selon la revendication 1,
caractérisé en ce que
la comptabilité des services (3) analyse la confirmation de service reçue de manière codée par l'utilisateur (1) et par l'intermédiaire du prestataire de service (2) et après contrôle du prestataire de service (2), notamment après comptabilisation du compte d'utilisateur, envoie une confirmation pour libérer le service par le prestataire de service (2).

11°) Application du procédé selon l'une quelconque des revendications 1 à 10 pour fournir des services de télématique dont le décompte se fait indé-

pendamment du prestataire de service (2), notamment sans établir de canal de communication séparé.

12°) Installation pour recevoir des services d'un prestataire de service (2), caractérisée par

- des moyens (13) pour activer une clé privée reçue d'une comptabilité des services (3),
- une unité d'émission (12) pour émettre une requête à destination d'un prestataire de service (2) pour prendre en compte les services,
- une unité de réception (11) pour recevoir une offre de service d'un prestataire de service (2),
- des moyens (13, 14) pour décoder une information codée contenant l'offre de service ainsi que des moyens (15) pour exploiter l'information décodée,
- des moyens (16) pour générer une nouvelle information avec codage d'au moins un élément d'information décodé avec la clé privée, et
- des moyens (17) pour recevoir les services d'un prestataire de service (2) après libération par le prestataire de service (2) sur contrôle de l'élément codé.

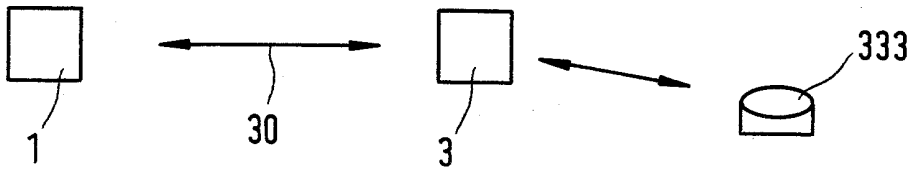


Fig.1

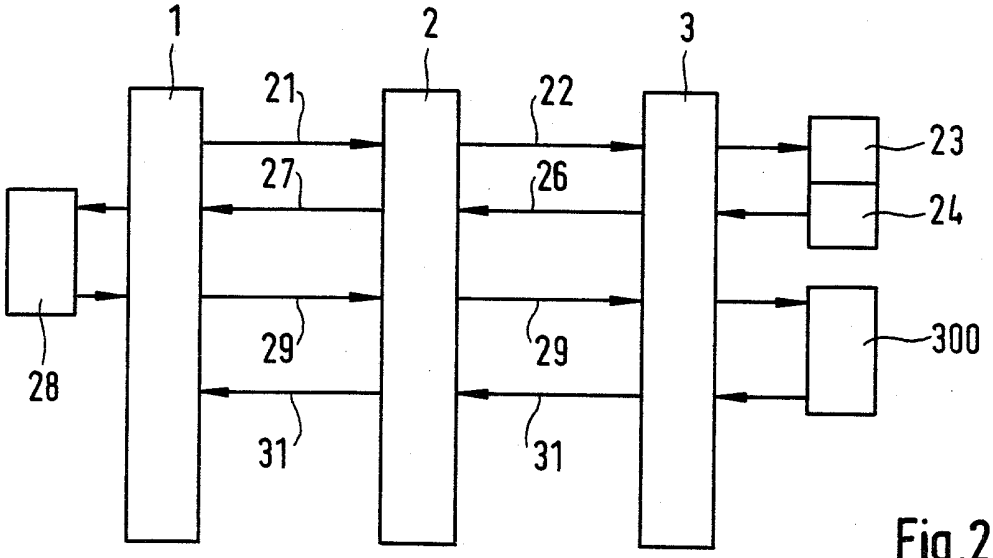


Fig.2

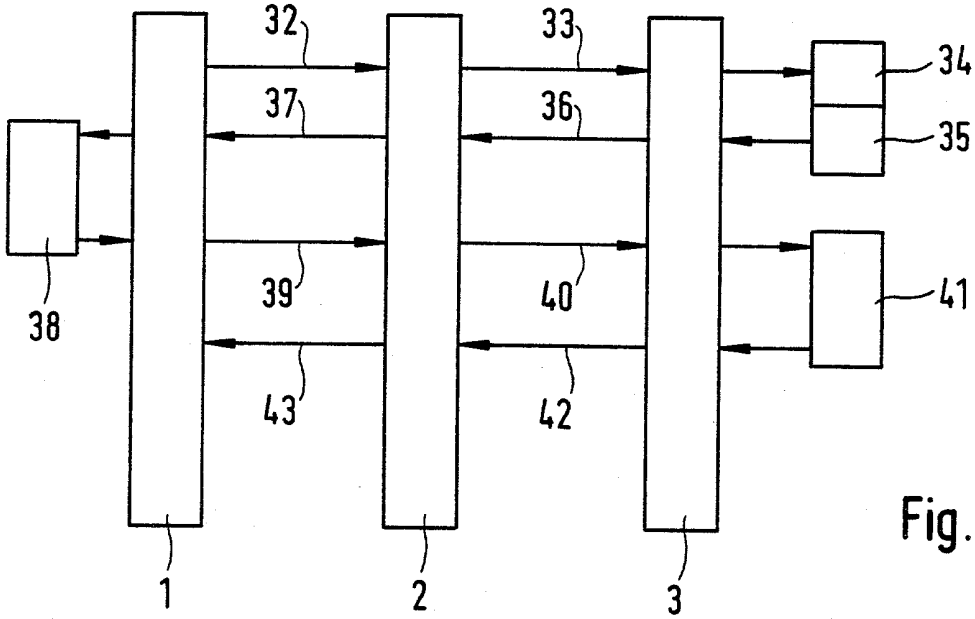


Fig.3

Fig. 4