

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
1 mai 2003 (01.05.2003)

PCT

(10) Numéro de publication internationale
WO 03/036974 A2

(51) Classification internationale des brevets⁷ : H04N 7/16

(21) Numéro de la demande internationale :
PCT/FR02/03673

(22) Date de dépôt international :
25 octobre 2002 (25.10.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/13878 26 octobre 2001 (26.10.2001) FR

(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES [FR/FR]; 34, Place Raoul Dautry,
F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : DAUVOIS,
Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris
(FR).

(74) Mandataire : DU BOISBAUDRY, Dominique; Brevaux,
3, rue du Docteur Lancereaux, F-75008 Paris (FR).

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, 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, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée
dès réception de ce rapport

En ce qui concerne les codes à deux lettres et autres abrévia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.

(54) Title: METHOD FOR VERIFYING TELEVISION RECEIVER SETS WITH ACCESS CONTROL AND CORRESPOND-
ING RECEIVER SET

(54) Titre : PROCEDE DE VERIFICATION DE RECEPTEURS DE TELEVISION A CONTROLE D'ACCES ET RECEPTEUR
CORRESPONDANT

(57) Abstract: The invention concerns a method for verifying television receiver sets with access control and a corresponding receiver set. The invention is characterized in that a broadcaster performs parametered calculations, for example through the sub-
scriptions and the characteristics of the receiver sets. The results of said calculations are transmitted to the receiver set which store
them. In order to verify a receiver, the broadcaster transmits thereto the parameter(s) used, the receiver performs the calculation
and compares the result it obtains with that which it has stored. In case of non-conformity, the receiver set modifies its operating
conditions. The invention is applicable to television with access control.

(57) Abrégé : Procédé de vérification de récepteurs de télévision à contrôle d'accès et récepteur correspondant. Selon l'invention,
un diffuseur effectue des calculs paramétrés, par exemple par les abonnements et les caractéristiques des récepteurs. Les résultats de
ces calculs sont transmis aux récepteurs, qui les stockent. Pour vérifier un récepteur, le diffuseur lui transmet le ou les paramètres
utilisés, le récepteur effectue le calcul et compare le résultat qu'il obtient avec celui qu'il stocke. En cas de désaccord, le récepteur
modifie son fonctionnement. Application en télévision à contrôle d'accès.



WO 03/036974 A2

**PROCEDE DE VERIFICATION DE RECEPTEURS DE TELEVISION
A CONTROLE D'ACCES ET RECEPTEUR CORRESPONDANT**

DESCRIPTION

5

Domaine technique

La présente invention a pour objet un procédé de vérification de récepteurs de télévision à contrôle d'accès et un récepteur apte à être vérifié
10 par ce procédé.

Etat de la technique

Dans la télévision à contrôle d'accès, les données à transmettre sont d'abord embrouillées par un
15 algorithme de chiffrement et les données embrouillées sont ensuite diffusées avec des messages de contrôle d'accès. Les récepteurs des abonnés ayant souscrit l'abonnement approprié sont chargés par des informations constituant un droit d'accès leur
20 permettant de retrouver, dans les messages de contrôle d'accès, la clé nécessaire au désembrouillage des données transmises.

A titre d'exemple, le document FR-A-
2 448 825 décrit un système utilisant des clés
25 d'abonnement C_i changeant de manière aléatoire à des intervalles relativement longs de l'ordre du mois, et une clé de service K changeant elle aussi de manière aléatoire mais à des intervalles courts de l'ordre de quelques minutes. Les données sont embrouillées à
30 l'aide de la clé de service K . Les messages de contrôle d'accès M_i sont obtenus à partir des clés d'abonnement C_i et de la clé de service K par un algorithme

paramétré par les clés d'abonnement Ci. Dans le poste récepteur d'un abonné, la carte à puce qu'il contient a été chargée par les clés correspondant aux abonnements souscrits par l'abonné. Le terminal associé à la carte
5 contient un circuit de restitution de la clé de service K, qui reçoit les messages Mi et qui dispose de la clé d'abonnement Ci contenue dans la carte. Ce circuit restitue la clé de service. Des moyens de désembrouillage retrouvent alors les données en clair.

10 Bien que donnant satisfaction à maints égards, une telle technique présente l'inconvénient d'être sujet à des fraudes. En effet, un récepteur pourrait être modifié par un fraudeur habile pour qu'il puisse recevoir un programme alors même que l'abonné
15 n'a pas acquitté l'abonnement correspondant. Eviter de telles fraudes (ou les réduire), nécessiterait d'effectuer périodiquement des vérifications chez les abonnés pour contrôler l'intégrité de leur récepteur. Ce n'est guère envisageable pour des raisons
20 commerciales évidentes.

La présente invention a justement pour but de résoudre ce problème.

Exposé de l'invention

25 Selon l'invention, la vérification d'un récepteur est commandée par l'organisme diffuseur et s'effectue par le récepteur lui-même. Si la vérification montre que le récepteur a conservé son intégrité, il continue à fonctionner normalement. Dans
30 le cas contraire, le fonctionnement est modifié, d'une

manière ou d'une autre, par exemple par arrêt partiel ou total.

Selon l'invention, on s'y prend comme suit :

A) - Le diffuseur effectue des calculs
5 paramétrés par un ou plusieurs paramètres déterminés ;

- le diffuseur transmet ensuite à chaque récepteur les résultats des calculs qui le concernent, chaque récepteur stockant ces différents résultats ;

B) - pour vérifier un récepteur particulier,
10 le diffuseur transmet à ce récepteur le ou paramètres déterminés ;

- le récepteur effectue alors le calcul et compare le résultat qu'il obtient avec le résultat correspondant qu'il a stocké ; en cas de désaccord, il
15 modifie son fonctionnement de manière appropriée, par exemple en cessant de fonctionner.

Lorsque le récepteur comprend un terminal et une carte à puce, c'est de préférence la carte qui stocke les résultats de calcul transmis par le
20 diffuseur et c'est le terminal qui effectue le calcul en question.

Dans une première variante, le terminal transmet le résultat de son calcul à la carte ; celle-ci compare ce résultat avec celui qu'elle stocke et, en
25 cas de différence, elle modifie le fonctionnement du récepteur, par exemple en refusant de continuer à coopérer avec le terminal.

Dans une seconde variante, le terminal lit dans la carte celui des résultats qui correspond au
30 calcul qu'il a effectué et compare ce résultat avec celui qu'il a lui-même obtenu ; en cas de différence,

il modifie le fonctionnement du récepteur, par exemple en refusant de continuer à coopérer avec la carte.

Les paramètres utilisés peuvent être constitués par un premier paramètre correspondant à l'un des abonnements et par un second paramètre constitué par l'une des caractéristiques des récepteurs, par exemple le numéro de série de leur carte à puce (qui est unique).

Les algorithmes de calcul mis en œuvre peuvent être d'un type quelconque : il peut s'agir d'algorithmes de chiffrement symétriques ou asymétriques, de type RSA, de type HASH, de type DES ou de tout autre type.

L'algorithme de calcul mis en œuvre en liaison avec un abonnement n'est pas nécessairement le même que celui qui est mis en œuvre avec les autres. Cet algorithme peut être introduit dans le terminal à la fabrication ou chargé par le diffuseur au moment de la vérification.

La présente invention a également pour objet un récepteur de télévision apte à être contrôlé selon le procédé qui vient d'être défini. Ce récepteur comprend un terminal et une carte à puce contenant des droits d'accès et il est caractérisé en ce que :

- la carte contient en outre différents résultats de calcul,
- le terminal comprend des moyens aptes à effectuer un calcul déterminé en utilisant un ou plusieurs paramètres déterminés,

- le récepteur comprend des moyens pour comparer le résultat du calcul effectué par le terminal avec le résultat correspondant contenu dans la carte,

- le récepteur comprend des moyens pour
5 modifier son fonctionnement de manière appropriée en cas de différence entre les deux résultats.

Dans une première variante, les moyens pour comparer les résultats sont situés dans la carte, celle-ci étant apte à modifier le fonctionnement du
10 récepteur.

Dans une seconde variante, les moyens pour comparer les résultats sont situés dans le terminal, celui-ci étant apte à modifier le fonctionnement du récepteur.

15 L'un des paramètres peut correspondre à l'un des abonnements et un autre paramètre peut être l'une des caractéristiques du récepteur et par exemple le numéro de série de la carte.

20 Brève description des dessins

Les figures 1 à 3 illustrent chacune, de façon schématique, un récepteur apte à réaliser le procédé de l'invention.

25 Exposé détaillé de modes de réalisation particuliers

On suppose, à titre d'exemple non limitatif, que l'algorithme de calcul est un algorithme de chiffrement à clé symétrique portant sur le numéro de série de la carte à puce. De tels algorithmes sont déjà
30 utilisés dans le contrôle d'accès, notamment pour retrouver la clé de service (cf. l'introduction). On

note $A_{C_i}(NSj)$ l'algorithme utilisant la clé C_i , où l'indice i se rapporte aux n différents abonnements du système (i va de 1 à n), et NSj représente le numéro de série du $j^{\text{ième}}$ récepteur, l'indice j identifiant le
5 récepteur (j va de 1 à p). Le résultat de ce calcul est noté $R_{i,j}$. On suppose que chaque récepteur est muni des n clés d'abonnement C_i .

Le diffuseur calcule, à un moment ou à un autre, les np résultats $R_{i,j}$, i allant de 1 à n et j de
10 1 à p . A un récepteur de rang q déterminé ($j=q$) correspond seulement n résultats $R_{i,q}$ correspondant aux n clés d'abonnement C_i (i de 1 à n).

Pour effectuer la vérification du récepteur de rang q , le diffuseur choisit l'une des clé
15 d'abonnement parmi les n soit C_k , et ordonne au récepteur d'effectuer le calcul en prenant comme paramètre la clé C_k . Ce calcul avait donné le résultat $R_{k,q}$ lorsque le diffuseur l'avait effectué. Celui-ci calcule donc $A_{C_k}(NSq)$ et compare le résultat avec celui
20 qu'il a déjà reçu du diffuseur et qu'il a stocké. S'il y a égalité entre les résultats, le récepteur continue son fonctionnement normal. Si les résultats sont discordants, ou si le récepteur ne peut même pas effectuer le calcul demandé, il y a eu manipulation
25 frauduleuse du récepteur et le fonctionnement peut être interrompu.

Le tableau I résume ces opérations.

Ce tableau ne précise pas quels moyens du récepteur effectuent la comparaison des résultats. Dans
30 le tableau II, il est supposé que c'est la carte qui se charge de cette tâche. Dans ce cas, les résultats

inscrits dans la carte ne sont pas lisibles par le terminal. Le tableau III correspond au cas où c'est le terminal qui se charge de la comparaison. Dans les deux tableaux II et III l'indice q , repérant le récepteur, a été omis pour simplifier les notations.

Tableau I

DIFFUSEUR	RECEPTEUR $j=q$
• Calcule tous les $R_{ij} = A_{C_i} (NS_j)$ (i de 1 à n) (j de 1 à p) • Transmet au récepteur q C_i (i de 1 à n) $R_{i,q}$ • Ordonne au récepteur q le calcul en stipulant $i=k$ soit $A_{C_k} R_{k,q} = (NS_q)$	• Stocke C_i (i de 1 à n) • Stocke $R_{i,q}$ • Calcule $R'_{k,q} = A_{C_k} (NS_q)$ • Compare $R'_{k,q}$ et $R_{k,q}$

10

Tableau II

CARTE A PUCE	TERMINAL
• Stocke C_i et R_i (i de 1 à n) • Compare R'_i et R_i	• Reçoit l'ordre de calcul avec un C_i déterminé • Lit dans la carte C_i et NS • Calcule $R'_i = A_{C_i} (NS)$ • Transmet R'_i à la carte

Tableau III

CARTE A PUCE	TERMINAL
• Stocke C_i et R_i	• Reçoit l'ordre de calcul avec C_i déterminé • Lit dans la carte C_i et NS • Calcule $R'_i = A_{C_i}(NS)$ • Lit R_i dans la carte • Compare R'_i et R_i

A titre d'exemple simple, on peut supposer qu'à chaque récepteur correspond un abonnement. Le diffuseur calcule les n résultats R_i . Au récepteur de rang q correspond un résultat R_q correspondant à la clé d'abonnement C_q et à l'algorithme AC_q .

Pour effectuer la vérification de ce récepteur, le diffuseur ordonne à celui-ci d'effectuer le calcul en prenant comme paramètre cette clé C_q . Ce calcul avait donné le résultat R_q lorsque le diffuseur l'avait effectué. Le récepteur calcule donc $AC_q(NS_q)$ et compare le résultat obtenu avec celui R_q qu'il tient du diffuseur.

On observera que, dans l'invention, le terminal et la carte à puce sont des produits dynamiques, en ce sens que leurs contenus peuvent varier : à tout moment ils peuvent recevoir de nouveaux droits d'accès et de nouveaux résultats de calcul.

L'algorithme de calcul peut faire appel à d'autres clés que les clés d'abonnement proprement dites, et par exemple à des clés diversifiées obtenues

à partir d'une clé de base combinée à l'identifiant de chaque carte à puce. Dans ce cas, chaque récepteur effectue un calcul avec une clé qui lui est propre. De même, l'algorithme peut être changé ou modifié
5 dynamiquement

Chacun des modes de réalisation de récepteur correspondant aux tableaux 1 à 3 est illustré sur chacune des figures 1 à 3 respectivement.

Sur la figure 1 le récepteur de télévision 1
10 apte à être vérifié par le procédé selon l'un des modes de réalisation de l'invention comprend un terminal 2 et une carte à puce 3 contenant des droits d'accès relatifs à des abonnements. la carte contient en outre différents résultats de calculs.

15 Le terminal 2 comprend des moyens 4 aptes à effectuer l'un quelconque des calculs prévus par le procédé en utilisant un ou des paramètres prédéterminés.

Le récepteur 1 comprend des moyens 5 pour
20 comparer le résultat du calcul effectué par le terminal 2 avec le résultat correspondant contenu dans la carte 3.

Le récepteur comprend des moyens 6 pour
25 modifier son fonctionnement de manière appropriée en cas de différence entre les deux résultats.

Dans le mode de réalisation de la figure 2, les moyens 5 pour comparer le résultat du calcul effectué par le terminal 2 avec le résultat correspondant contenu dans la carte 3, sont situés dans
30 la carte 3, celle-ci étant apte à modifier le fonctionnement du récepteur.

Dans le mode de réalisation de la figure 3, les moyens 5 pour comparer le résultat du calcul effectué par le terminal 2 avec le résultat correspondant contenu dans la carte 3, sont situés dans 5 le terminal 2, celui-ci étant apte à modifier le fonctionnement du récepteur.

REVENDICATIONS

1. Procédé de vérification de récepteurs pour système de télévision à contrôle d'accès, dans lequel un diffuseur transmet à des abonnés ayant souscrit des abonnements les droits d'accès correspondants, les récepteurs stockant ces droits d'accès,

ce procédé étant caractérisé en ce que :

- 10 A) le diffuseur effectue des calculs paramétrés par un ou plusieurs paramètres,
- le diffuseur transmet ensuite à chaque récepteur les résultats des calculs qui le concernent,
 - chaque récepteur stocke ces résultats,
- 15 B) pour vérifier un récepteur particulier :
- le diffuseur transmet à ce récepteur le ou les paramètres déterminés,
 - le récepteur effectue le calcul et compare le résultat qu'il obtient avec le résultat correspondant qu'il a précédemment stocké,
- 20 - en cas de différence, le récepteur modifie son fonctionnement de manière appropriée.

2. Procédé selon la revendication 1, dans lequel, chaque récepteur comprenant un terminal et une carte à puce, c'est la carte qui stocke les droits d'accès et les résultats que lui transmet le diffuseur et c'est le terminal qui effectue le calcul demandé par le diffuseur.

3. Procédé selon la revendication 2, dans lequel :

- le terminal transmet le résultat de son calcul à la carte,

5 - la carte compare le résultat transmis par le terminal et le résultat correspondant qu'elle a reçu du diffuseur,

- en cas de différence la carte modifie le fonctionnement du récepteur.

10

4. Procédé selon la revendication 2, dans lequel :

- le terminal lit dans la carte le résultat correspondant au calcul qu'il effectue,

15 - le terminal compare le résultat de son calcul avec le résultat lu dans la carte,

- en cas de différence le terminal modifie le fonctionnement du récepteur.

20 5. Procédé selon la revendication 1, dans lequel le diffuseur effectue des calculs paramétrés par un premier paramètre correspondant à l'un des abonnements et par un second paramètre constitué par l'une des caractéristiques des récepteurs.

25

6. Procédé selon la revendication 5, dans lequel les calculs effectués par le diffuseur et les récepteurs sont définis par un algorithme de chiffrement dont la clé de chiffrement dépend des clés d'abonnement, ce chiffrement portant sur un nombre qui

30

dépend de l'une des caractéristiques de chaque récepteur.

7. Procédé selon la revendication 6, dans lequel la clé de chiffrement est une clé d'abonnement.

8. Procédé selon la revendication 6, dans lequel la caractéristique chiffrée est le numéro de série de la carte à puce utilisée dans le récepteur.

10

9. Récepteur de télévision apte à être vérifié par le procédé selon l'une quelconque des revendications 1 à 8, ce récepteur comprenant un terminal et une carte à puce contenant des droits d'accès relatifs à des abonnements, ce récepteur étant caractérisé en ce que :

- la carte contient en outre différents résultats de calculs,
- le terminal comprend des moyens aptes à effectuer l'un quelconque de ces calculs en utilisant un ou des paramètres prédéterminés,
- le récepteur comprend des moyens pour comparer le résultat du calcul effectué par le terminal avec le résultat correspondant contenu dans la carte,
- le récepteur comprend des moyens pour modifier son fonctionnement de manière appropriée en cas de différence entre les deux résultats.

10. Récepteur selon la revendication 9, dans lequel les moyens pour comparer les résultats sont

situés dans la carte, celle-ci étant apte à modifier le fonctionnement du récepteur.

11. Récepteur selon la revendication 9, dans
5 lequel les moyens pour comparer les résultats sont situés dans le terminal, celui-ci étant apte à modifier le fonctionnement du récepteur.

12. Récepteur selon la revendication 9, dans
10 lequel le terminal utilise un premier paramètre constitué par l'un des droits d'accès contenus dans la carte et un second paramètre constitué par l'une des caractéristiques du récepteur.

13. Récepteur selon la revendication 12,
15 dans lequel le second paramètre utilisé pour effectuer le calcul est le numéro de série unique de la carte.

1 / 2

FIG. 1

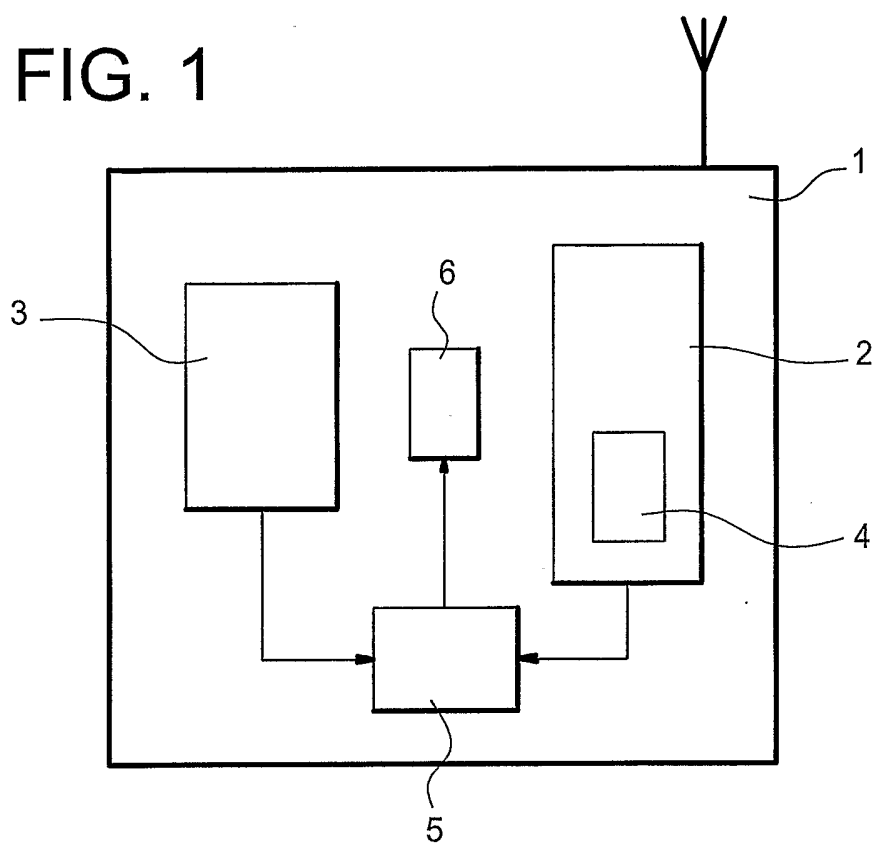
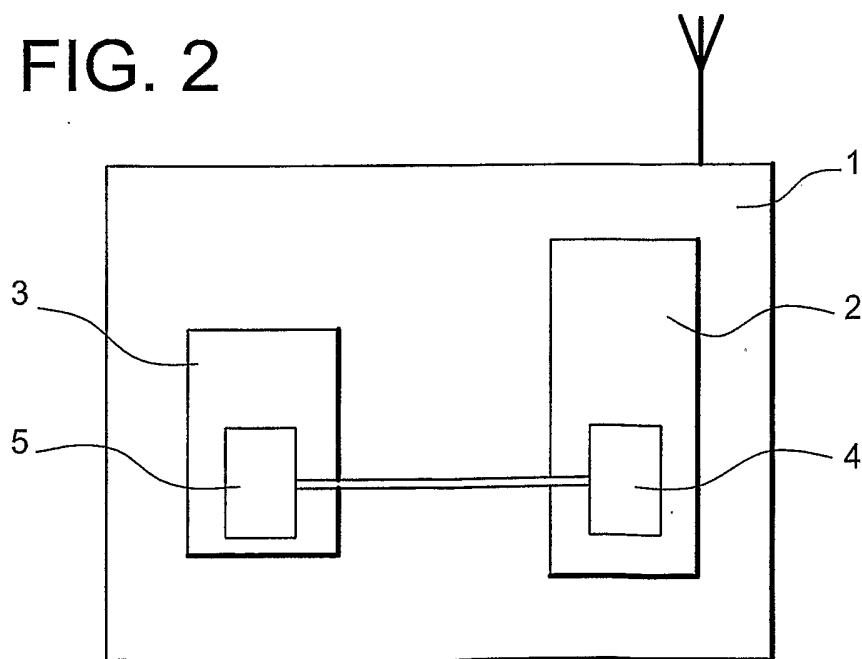


FIG. 2



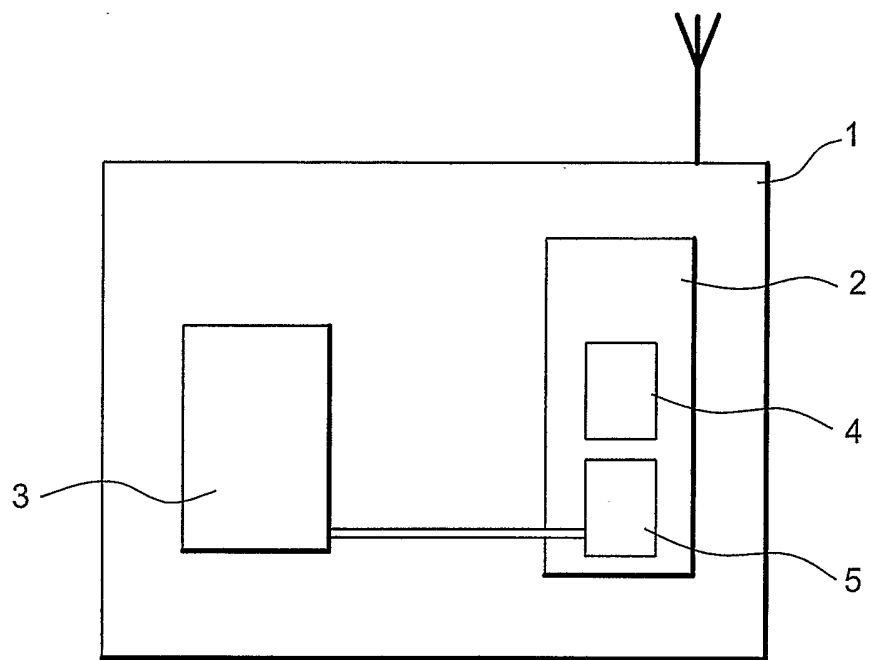


FIG. 3