(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 409 725 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **90402060.9**

(51) Int. Cl.5: **E05G 1/00**, G07F 9/06

(22) Date de dépôt: **17.07.90**

(30) Priorité: **17.07.89 FR 8909579**

(43) Date de publication de la demande:
23.01.91 Bulletin 91/04

(84) Etats contractants désignés:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

(71) Demandeur: **AXYTEL**
24, Rue de la Redoute Z.I. ST Apollinaire
F-21019 Dijon Cédex(FR)

(72) Inventeur: **Devaux, Franklin**
1, rue de Dijon
F-21560 Couternon(FR)
Inventeur: **Genevois, Christophe**
14, rue Georges Lavier
F-21000 Dijon(FR)
Inventeur: **Geoffroy, Marc**
11, rue de la Combe
F-21450 Saint Julien(FR)

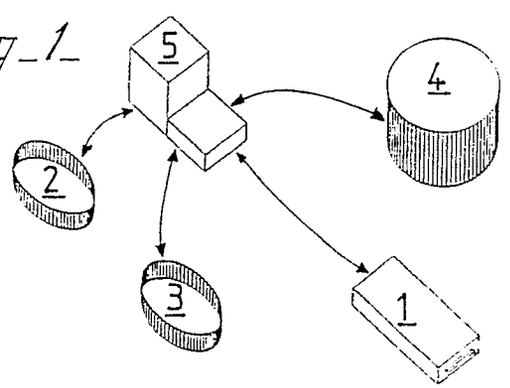
(74) Mandataire: **Bruder, Michel et al**
Cabinet Michel Bruder Conseil en Brevets
10, rue de la Pépinière
F-75008 Paris(FR)

(54) Système de protection de documents ou d'objets enfermés dans un contenant inviolable.

(57) L'invention concerne un système de protection de documents ou d'objets de valeur, et notamment de moyens de paiement tels que des billets de banque, des chèques, ou des cartes bancaires, enfermés dans au moins un contenant inviolable physiquement, appelé caissette (1), qui, en cas d'agression, provoque leur dégradation par des moyens appropriés, ce système étant caractérisé en ce que le cycle de fonctionnement d'une caissette (1) comporte un nombre restreint d'états logiques, appelés modes, la transition d'un premier mode à un second mode étant la conséquence d'un événement ponctuel, dont on vérifie la *licéité* par un moyen adéquat et autonome pouvant se mettre en relation avec la caissette (1), ladite transition s'accompagnant alors de la perte de mémoire, par la caissette (1), de son mode antérieur.

La présente invention est notamment destinée à la protection de documents ou d'objets de valeur, et notamment de moyens de paiement tels que des billets, des chèques ou des cartes bancaires, ou encore de médicaments dangereux (drogues) ou à forte valeur ajoutée. Cette protection est assurée aussi bien à l'intérieur d'une agence bancaire (ou d'une officine pharmaceutique, ou autre), que lors, du transport de cette agence vers une succursale.

Fig_1_



EP 0 409 725 A1

La présente invention concerne un système de protection de documents ou d'objets de valeur, et notamment de moyens de paiement tels que des billets de banque, des chèques, ou des cartes bancaires, enfermés dans un contenant inviolable physiquement, qui passe par ailleurs par une succession d'états logiques authentifiés en nombre restreint.

Des systèmes conventionnels de protection de documents ou d'objets de valeur tels que des moyens de paiement sont de nos jours bien connus et s'inspirent la plupart, dans une large mesure, du principe du coffre à parois renforcées, d'accès réservé aux seuls détenteurs d'une clef, à support matériel ou immatériel (tel un code), ce coffre se trouvant par ailleurs dans un environnement contrôlé et sécurisé par exemple au moyen de divers blindages.

Une alternative à ces dispositifs conventionnels souvent lourds et encombrants est proposée dans divers brevets français au nom du Demandeur. Dans le brevet FR-A-2 550 364, les documents ou objets de valeur à protéger, appelés fonds par la suite, sont enfermés dans une caissette, dont on contrôle l'état physique par l'intermédiaire de capteurs fournissant en permanence des signaux, qui doivent être conformes aux signaux résultant d'un processus obligatoire et inéluctable, sous peine de provoquer la destruction ou le marquage de la caissette et desdits fonds.

Le dispositif de dégradation utilisé à cet effet peut être, par exemple, celui décrit dans le brevet FR-A-2 574 845 au nom du Demandeur.

Dans le cas du transport d'objets de valeur, par exemple de médicaments dangereux (drogues, poisons) ou à forte valeur ajoutée, le dispositif de dégradation est sensiblement différent ; l'homme de l'art connait, à ce titre, les moyens connus et spécifiques à utiliser.

L'objet des brevets précités consiste à rendre inutilisables, ou à détruire, en cas d'agression, les fonds contenus dans une caissette et dont la valeur fiduciaire importante est très inférieure à leur valeur réelle (ce qui est le cas des billets, des cartes et des chèques ; la convoitise de ces fonds devient ainsi inefficace, ceux-ci étant détruits avant qu'on puisse les atteindre.

Les capteurs associés à ces systèmes et qui permettent notamment de détecter les agressions physiques sur la caissette peuvent être de structure très légère, contrairement aux blindages traditionnels ; un tel capteur d'intégrité de paroi est par exemple décrit dans le brevet français FR-A-2 615 987 au nom du Demandeur.

Un certain nombre d'inconvénients liés aux systèmes de protection proposés par ces brevets demeurent cependant sans remède, et mettent en jeu la fiabilité même d une protection que l'on veut parfaite, aussi bien lorsque la caissette contenant les fonds à protéger est mobile, que lorsqu'elle est immobile, et surtout lors des transactions nécessairement liées aux changements d états de la caissette, tels que par exemple son enlèvement, sa livraison, son ouverture ou sa fermeture.

En effet, conformément au brevet FR-A-2 550 364, la protection d'une caissette est intrinsèquement liée à la protection des autres caissettes que transporte le fourgon où elles ont été placées ; les caissettes sont en l'espèce protégées collectivement, grâce notamment à l'existence d'un dialogue secret et permanent, circulant entre elles, dont l'interruption non prévue provoque la dégradation des fonds à protéger. Un tel dispositif pose des problèmes de gestion de ce dialogue difficiles à résoudre, et la complexité ainsi mise en oeuvre conduit à des solutions coûteuses, lentes ou peu fiables.

Par ailleurs, il s'avère qu'une protection individuelle des caissettes est réalisable, et en l'occurrence préférable, puisqu'on bénéficie alors d'un système de protection souple, permettant par exemple d'éviter la destruction d'un grand ensemble de fonds contenus dans des caissettes différentes alors qu'une seule d'entre elles est en panne ou est agressée.

En outre, en cas de destruction d'une caissette et des fonds qui y sont contenus, les systèmes de protection décrits ne permettent pas de déterminer les personnes responsables de l'agression ayant causée cette destruction ; en effet, lors de sa destruction, il est souhaitable, et même nécessaire, que la caissette marque, ou détruise, non seulement les fonds, mais efface également toutes les informations ayant un caractère confidentiel et dont elle a besoin pour son correct fonctionnement : algorithmes de surveillance de ses états physiques, algorithmes de codage et de décodage des messages échangés avec l'extérieur, nature et contenu de ces messages tels que codes secrets, destinations et destinataires des fonds transportés.

La destruction de toutes ces informations rend impossible l'identification sûre du dernier manipulant d'une caissette détruite, qui peut aussi bien être un agresseur extérieur au système, qu'un agent chargé de la manutention ou du transport des caissettes voulant détourner les fonds à son profit, ou encore d'autres personnes autorisées à divers titres à les approcher, ou à les ouvrir "in fine".

Un autre inconvénient majeur du système décrit dans le brevet FR-A-2 550 364 réside, paradoxalement, dans l'inexorabilité stricte du processus gouvernant "l'histoire" d'une caissette pendant son transport. En effet, tout événement non prévu est considéré comme une agression par une caissette et conduit à sa destruction ; il n'y a donc

aucune possibilité de gradation dans la réponse fournie par la caissette à un événement imprévu. Par exemple, en cas d'embouteillage des voies de transport par lesquelles doit passer le fourgon transportant des caissettes, le retard dans leur livraison, induit par cet embouteillage, mène inexorablement à leur destruction, ce qui peut s'avérer être une coûteuse erreur économique et conduire un client, dont on transporte les fonds, à contester la fiabilité du système.

On ne peut pas, de manière immédiate, remédier à cet inconvénient car l'inexorabilité de certaines phases du processus de transport décrit dans ce brevet est impérative vis à vis de la sécurité.

On aura bien compris, par la lecture qui précède, que l'utilisation d'un unique centre de décision, la caissette, pour gérer la sécurité complète des fonds à protéger et la sécurité du transport lui-même, mène à des impasses incontournables.

La demande de brevet française 86-01 849 au nom du Demandeur constitue à ce titre un perfectionnement du brevet FR-A-2 550 364 ; les caissettes sont considérées comme étant dans un véhicule fixe, et servent alors de compartiments bancaires. Leur protection est toujours collective, avec les inconvénients précédemment soulevés, mais l'accès à la chambre forte où sont entreposées les caissettes est contrôlé de l'extérieur par un ordinateur pouvant entrer en relation avec un boîtier électronique, affecté à la surveillance de ladite chambre forte, et dialoguant également de manière secrète et permanente avec l'ensemble des caissettes. La communication de chacune de ces caissettes avec l'ordinateur extérieur devient possible ; ce dernier est alors capable de générer le processus inexorable réglant "l'histoire" d'une caissette et d'en contrôler l'initiation, qui s'effectue après diverses vérifications, dont celles de codes secrets détenus par les personnes ayant valablement accès aux caissettes (telles un banquier, ou un client).

Le système décrit dans ce dernier document possède encore des inconvénients notables, et il est en particulier possible de concevoir un ordinateur pirate, appelé clone par la suite, et remplissant les mêmes fonctions que l'ordinateur d'origine ; la sécurité des fonds enfermés dans les caissettes n'est donc pas totalement assurée, car il n'est prévu aucun moyen pour permettre aux caissettes de reconnaître sûrement l'ordinateur superviseur, et réciproquement.

On remarquera d'ailleurs, à la lecture de la demande de brevet précitée, que la source d'informations communiquant les données du processus aux divers éléments électroniques de l'ensemble n'est pas nécessairement unique, ce qui constitue un risque vis à vis de la confidentialité de ces données ; la redondance des informations, inexistante dans le brevet FR-A-2 550 364, devient ici trop importante.

L'invention vise à améliorer de manière décisive les différents systèmes connus, en proposant un système de protection de documents ou d'objets de valeur, et notamment de moyens de paiement tels que des billets de banque, des chèques, ou des cartes bancaires, enfermés dans au moins un contenant inviolable physiquement, appelé caissette, qui, en cas d'agression, provoque leur dégradation par des moyens appropriés, ce système étant caractérisé en ce que le cycle de fonctionnement d'une caissette comporte un nombre restreint d'états logiques, la transition d'un premier état logique à un second état logique étant la conséquence d'un événement ponctuel, dont on vérifie la *licéité* par un moyen adéquat et autonome pouvant se mettre en relation avec la caissette, ladite transition s'accompagnant alors de la perte de mémoire, par la caissette, de son état logique antérieur.

L'un des objectifs de la présente invention est ainsi de faire correspondre un état logique, appelé mode, à chaque situation dans laquelle peut se retrouver une caissette, ce mode étant délimité explicitement par deux bornes de nature purement conceptuelle, ce qui permet d'organiser avec rigueur et fiabilité le cycle de fonctionnement de ladite caissette ; les systèmes connus à ce jour ne connaissaient quant à eux que deux bornes implicites, soit "la transition entre caissette mobile et caissette fixe" et réciproquement.

La présente invention procure la souplesse nécessaire à une gestion plus intelligente de la protection fournie par les caissettes. Mais il est alors essentiel qu'à chaque étape du processus de protection, qu'à chaque transition entre deux états logiques, la caissette ne conserve aucune trace de son état logique antérieur ; on sait déjà que cette trace est inutile ; on comprend également que cette trace est dangereuse, puisqu'il est vital, pour la sécurité du système, que des messages confidentiels tels que des codes ne puissent pas être lus, s'ils ne sont pas détruits entièrement en cas d'agression. On comprendra enfin, grâce à ce qui suit, que cette trace ne peut pas exister.

En effet, cette absence de mémoire du mode précédent est fondamentale pour la sécurité du système, puisque deux modes extrêmes peuvent être reliés :

- soit directement grâce à un premier événement, prévu à cet effet, et qui provoque une transition entre ces deux modes,
- soit indirectement, par transitions préalables dans d'autres modes, dues à d'autres événements prévus et autorisés.

Si la caissette conservait la mémoire de son mode antérieur, c'est-à-dire si on acceptait qu'elle puisse s'en servir, il serait alors possible d'invalider une transition préalablement acceptée par la cais-

sette, entre un premier mode et un second mode ; un nouvel événement pourrait en effet provoquer une transition du premier mode vers un troisième mode, sans que, par ailleurs, il ait été prévu d'autoriser une transition du second mode vers ce troisième mode ; le système deviendrait par conséquent "ingérable".

En proposant d'organiser le fonctionnement d'une caissette en un cycle comportant un nombre limité d'états logiques, ou modes, cette caissette possédant par ailleurs pour seule mémoire son propre mode, la présente invention procure un moyen fiable et sur de définir divers cycles de fonctionnement, qui correspondent à de nombreux cas inaccessibles aux systèmes connus jusqu à aujourd'hui, pour lesquels une seule "histoire" peut exister entre la fermeture et l'ouverture d'une caissette.

Ce fonctionnement particulier d'une caissette, par transitions entre des états logiques existant en nombre limité, est à rapprocher du fonctionnement des machines connues par ailleurs sous le nom de "machines à modes limités".

La rigueur d'une telle organisation se traduit, pour le système de protection conforme à l'invention, par une intelligence supplémentaire rendant en quelque sorte "inviolable logiquement" les caissettes et le système dans son ensemble.

On peut à ce titre effectuer une véritable analogie entre le système de l'invention et les systèmes développés à l'heure actuelle en reconnaissance des formes, et notamment dans le domaine de l'intelligence artificielle ; "l'intelligence" de ces systèmes, c'est-à-dire leur capacité de déduction à partir d'informations quelquefois incomplètes, résulte, non pas d'informations explicitement formulées et stockées dans des mémoires par exemple électroniques, mais de l'organisation, de la forme, organisant la circulation et l'échange d'informations.

"L'information circulante" du système conforme à l'invention est la responsabilité attachée à la protection des fonds contenus dans une caissette ; la transmission effective et contrôlée de cette responsabilité est rendue possible par l'organisation en machine à modes limités de la caissette et constitue l'apport principal de ce système.

On aboutit de cette façon à un partage de la responsabilité qui est transférée, dans un sens ou dans l'autre sens, entre, d'une part, les utilisateurs des caissettes, d'autre part, un moyen pouvant se mettre en relation avec elles, et enfin, les caissettes.

Une caissette n'est totalement responsable des fonds qui y sont enfermés que durant son transport (par les moyens connus dont on a parlé).

Il est à noter enfin que la responsabilité n'est pas transférée à chaque transition d'un mode à un autre mode, mais seulement lorsque cela est nécessaire pour la sécurité du système.

D'autres caractéristiques et avantages du système selon l'invention ressortiront mieux de la description qui va suivre d'une réalisation particulière non limitative donnée à titre d'illustration de ce système, en référence au dessin annexé sur lequel :

- la figure 1 est un schéma synoptique de l'organisation en réseau du système selon l'invention.
- la figure 2 est un diagramme de représentation du concept de transitivité des authentifications.
- la figure 3 est un ordinogramme logique des transitions possibles et prévues entre les modes de fonctionnement du système, suivant une variante particulière de l'invention.

Conformément à la figure 1, le système suivant l'invention est utilisé pour la protection de fonds qui ont été placés dans une caissette 1 par le responsable d une agence bancaire, appelé par la suite expéditeur 2. La caissette 1 doit être transportée par un convoyeur 3 vers, par exemple, une succursale de cette agence bancaire.

Dans une des variantes préférées de l'invention, le moyen pouvant se mettre en relation avec les caissettes pour réaliser le transfert de la responsabilité est constitué par un ordinateur unique 4.

Cet ordinateur 4 possède un rôle de superviseur et gère la sécurité logique des caissettes 1, c'est-à-dire vérifie la *licéité* des transitions de certains modes de fonctionnement de celles-ci vers certains autres modes.

Lors de ces transitions particulières, il se produit une extension, ou un rétrécissement, du système de protection selon l'invention, et on peut citer trois cas très explicites :

a) lors d'un transport, la protection des fonds ne peut être assurée que par la caissette 1 les contenant : le système comprend alors uniquement la caissette 1.

b) à la fin d'un transport, au moment de la livraison, seule une source d'informations extérieure à la caissette 1 peut provoquer l'interruption du mode dans lequel elle a été placée au début de son transport, et qui constitue sa seule mémoire : le système doit alors être étendu à la source d'informations extérieure - c'est-à-dire l'ordinateur 4 - qui doit, préalablement à cette extension, être reconnu(e) comme un partenaire fiable et sûr par la caissette.

c) après la livraison, la protection des fonds enfermés dans la caissette 1 est encore totale, car son ouverture nécessite l'extension du système à une deuxième source d'informations extérieure - l'utilisateur de ces fonds (au sens large : destinataire, expéditeur 2, convoyeur 3) - qui doit, à son tour, être reconnue comme un

partenaire fiable et sûr par la caissette 1 et l'ordinateur 4.

Il existe ainsi trois types de modes pour une caissette 1 - en fait pour le système dans son ensemble, mais seule la caissette 1 participe à l'ensemble de la protection puisque c'est elle qui, en fin de compte, permet de supprimer la convoitise des tiers - selon qu'elle est considérée comme étant mobile et fermée, conformément au cas a), selon qu'elle est immobile et fermée, conformément au cas b), et enfin selon qu'elle est immobile et ouverte, conformément au cas c).

Les transitions entre ces trois types de modes décident du transfert de la responsabilité attachée à la protection des fonds, qu'ils soient ou non enfermés dans une caissette 1 (avant leur expédition, ces fonds sont librement placés par l'expéditeur 2 dans la caissette 1, et jusqu,à la confirmation de leur prise en charge par le système, cet expéditeur 2 en est responsable).

La mobilité de la caissette 1 est, par conséquent, un attribut purement logique du système, qui va au-delà de sa mobilité physique véritable, mais bien entendu la recouvre sans paradoxe. Cet avantage considérable du système est l'une des conséquences les plus inattendues de l'organisation en machine à modes limités de la partie physiquement mobile de celui-ci : la caissette 1.

On peut comparer, à ce titre, le système selon l'invention à un réseau informatique où un "jeton", symbolisant la détention du pouvoir de décision, peut être échangé entre les bornes du réseau ; la borne détentrice du "jeton" peut choisir, en outre, de transférer celui-ci, ce transfert s'accompagnant donc de la perte ou du partage du pouvoir. Le "jeton" transféré dans le système de l'invention est constitué, on l'aura compris, par la responsabilité attachée à la protection des fonds enfermés, ou non, dans une caissette 1.

Par ailleurs, un avantage inattendu de l'utilisation, suivant l'invention, d'un unique ordinateur 4 supervisant le système, est de limiter la redondance des informations nécessaires à la gestion sûre de celui-ci, c'est-à-dire leur transfert éventuel. Si un deuxième ordinateur devait exister - on pourrait par exemple placer un ordinateur au lieu de départ d'une caissette, et un autre ordinateur à son lieu d'arrivée, ce qui est le oas notamment du système décrit dans la demande de brevet française 86-01 849 - il serait impératif d'intégrer ce second ordinateur d une façon fiable au système :caissette/premier ordinateur: pour qu'il devienne un système :caissette/premier ordinateur/deuxième ordinateur: ; l'intégra-tion fiable du destinataire des fonds enfermés dans la caissette 1 deviendrait alors possible, par l'intermédiaire de ce second ordinateur. Or, l'étape d'intégration du second ordinateur n'est pas nécessaire car elle ne procure ni simplification (au contraire), ni sécurité complémentaire, le destinataire des fonds pouvant être intégré directement par le premier ordinateur.

On doit enfin remarquer que les caissettes 1 sont totalement indépendantes les unes des autres et que chaque système :caissette/ordinateur/utilisateur: doit être considéré comme un réseau particulier, même si l'ordinateur 4 superviseur peut être le même pour toutes les caissettes 1. Il est ainsi bon de rappeler qu'il n'existe aucun dialogue circulant en permanence entre les caissettes 1, ce qui constitue un avantage notable vis à vis du système décrit dans le brevet FR-A-2 550 364.

Il existe uniquement, suivant l'invention, une série de dialogues ponctuels. Pendant ces dialogues, les messages échangés ne doivent néanmoins pas mettre en jeu la sécurité du système ; c'est pourquoi les liaisons établies entre les parties font partie intégrante du système, leur défaillance éventuelle étant considérée comme une agression.

Ces liaisons peuvent posséder un support matériel, dont la nature est plus facilement protégeable, par exemple au moyen de blindages. On comprendra malgré tout par la suite qu'il peut être remédier avantageusement aux problèmes de confidentialité sans avoir recours à ces blindages physiques.

Suivant une caractéristique complémentaire de l'invention, et conformément à la figure 1, les quatre parties caissette 1, ordinateur 4, expéditeur 2, et convoyeur 3, peuvent être reliées à une borne unique, appelée station 5 par la suite, pour constituer un réseau en étoile dont ladite station 5 est le centre.

Il existe de cette façon une première station 5 au lieu de départ d'une caissette 1, et une autre station 5 à son lieu d'arrivée. Cette multiplicité de stations 5 n'entache cependant en rien la sécurité du système, car, selon une caractéristique très importante de l'invention, le "jeton", qui symbolise la responsabilité vis à vis de la protection des fonds, n'est jamais transmis auxdites stations 5, qui ne constituent par conséquent que des points de passage des informations confidentielles a priori vitales pour la sécurité du système.

L'utilisation d'un réseau en étoile procure nombre d'avantages bien connus.

En particulier, un message échangé entre deux parties intégrantes d'un réseau en étoile ne transite pas par les autres parties comme, par exemple, dans un anneau : on peut alors parler d'une confidentialité structurelle de ce type de réseau.

Par ailleurs, pour pouvoir dialoguer, chacune des parties du système possède une interface électronique qui doit gérer des échanges quelquefois complexes. L'utilisation d'une station 5, pouvant relier, conformément à l'invention, toutes les

parties entre elles, permet avantageusement, et de manière inattendue, de simplifier et d'alléger lesdites interfaces.

Par exemple, il n'est pas utile de transporter avec la caissette 1 des moyens de mise en communication évolués, nécessitant une électronique lourde. De même, la liaison d'un utilisateur (expéditeur 2, convoyeur 3) avec les autres parties du système doit rester simple.

La station 5 possède à cet effet toutes les interfaces électroniques lourdes, et il reste à la caissette 1 et à l'utilisateur à gérer uniquement un dialogue élémentaire de connexion avec ladite station 5.

Il est à noter que l'ordinateur 4 peut, quant à lui, gérer des échanges plus complexes, et qu'il est par ailleurs avantageux, suivant l'invention, d'en faire un centre serveur situé à distance de toutes les stations 5, de tous les utilisateurs, et de de toutes les caissettes 1, ce qui permet de le protéger efficacement, par la même occasion, d'éventuelles agressions, aussi bien logiques que physiques.

S'il est désormais acquis que le système suivant l'invention présente, en toutes ses caractéristiques, une structure fonctionnelle potentiellement confidentielle, cette confidentialité doit s'appuyer sur la certitude que les parties intégrantes du système, ou intégrées au système, sont celles qu'elles prétendent être.

Suivant alors une caractéristique complémentaire du système conforme à l'invention, les communications entre deux parties du système s'effectuent selon un protocole permettant à la partie recevant un message d'authentifier la partie qui est sensée l'avoir émis, cette authentification s'accompagnant éventuellement de l'envoi d'un message de bonne réception à ladite partie émettrice.

Selon l'invention, certaines authentifications sont effectuées dans les deux sens car il est nécessaire, par exemple, qu'une caissette 1 soit sûr que l'ordinateur 4 n'est pas un ordinateur clone, et que réciproquement, l'ordinateur 4 soit sûr que ladite caissette 1 n'est pas une caissette clone : on parle alors d'authentification mutuelle des parties. De même, une station 5, sur laquelle est connectée une caissette 1, est authentifiée, ce qui interdit l'existence de stations clones.

On notera que l'authentification du système par un utilisateur (expéditeur 2, convoyeur 3) de celuici est implicite ; en l'espèce, il ne sera procédé qu à une authentification simple de cet utilisateur, que ce soit par une caissette 1, l'ordinateur 4, et éventuellement, au passage, par la station 5 où est connectée ladite caissette 1 (cette station 5 ne possédera de toute façon aucun moyen d'intégrer l'utilisateur au système ; il s'agit uniquement d'une facilité et d'une sécurité supplémentaire visant à rejeter, dès le premier abord, un utilisateur illicite).

Grâce à la structure logique des caissettes 1 organisées en machines à modes limités, et à l'architecture physique et fonctionnelle des liaisons existant entre les diverses parties du système, cette authentification mutuelle des parties peut être gérée strictement, et procure une souplesse inattendue dans la gestion de la protection des fonds, enfermés, ou non, dans une caissette 1.

En effet, on peut pratiquement en toutes circonstances interrompre une phase de la protection des fonds, sans pour autant la remettre en cause ; ces interruptions, qui nécessitent l'intégration au système d'une partie fiable nouvelle (mise au courant de la "circonstance" conduisant, par exemple, à un détournement de transport), et donc la transition d'un type de mode vers un autre type de mode, imposent obligatoirement une authentification mutuelle des parties. Les retards de transport "normaux", les embouteillages, les pannes, peuvent enfin trouver une solution autre que la destruction pure et simple des fonds contenus dans une caissette 1.

Les moyens conventionnels de cette authentification sont nombreux, et de nature, pour la plupart, informatique.

On peut ainsi effectuer une analogie exacte des principes sécurisant le système conforme à l'invention avec les principes sécurisant une carte à mémoire ; notamment, on peut considérer la caissette 1, qui est inviolable physiquement et logiquement, comme étant une véritable carte à mémoire.

Les mesures à prendre pour la sécurité d'une caissette 1, et pour la sécurité des transactions auxquelles elle participe, sont alors bien connues, et visent à éliminer, d'une part, les menaces contre la confidentialité des messages échangés entre deux parties intégrantes du système, dont par exemple la caissette, et d'autre part, les menaces contre 1 intégrité de ces messages (altération volontaire ou non de leur contenu).

Une première mesure éliminant les menaces contre la confidentialité consiste à chiffrer les messages échangés, et on connait pour ce faire de nombreux procédés cryptographiques.

Suivant l'invention, il a été choisi d'utiliser l'algorithme de chiffrement de type symétrique connu sous le nom de DES (de l'anglais Data Encryption Standard), dont les caractéristiques sont normalisées, et que l'on peut consulter par exemple dans la publication référencée FIPS PUB 46 (Federal Information Processing Standards Publication 46 . Dans cet algorithme, un couple :caissette 1/ordinateur 4: (par exemple) possède une clef K ; cette clef K est placée dans une mémoire de la caissette 1 où elle est physiquement protégée, tandis que l'ordinateur 4 mémorise, suivant la va-

riante préférée de l'invention, les clefs K partagées avec toutes les caissettes 1.

Cette variante, peu économe en mémoire pour l'ordinateur 4, est préférable à celle conduisant à prendre une seule clef pour toutes les caissettes 1, car il pourrait advenir qu'une caissette 1 agressée ne détruise pas complètement la clef qui y est inscrite, permettant sa récupération, et le vol légal du contenu des autres caissettes 1 par constitution d'un clone -. Malgré le fait que l'algorithme DES est un algorithme public, seule la connaissance de la clef K permet de déchiffrer un message chiffré avec celle-ci ; il s,agit donc d'une authentification en soi du message, qui peut être considérée comme suffisante pour le fonctionnement du système. Cependant, un brouillage dudit message sur la ligne de communication n'est pas détecté : il s'avère donc préférable d'authentifier le message avant de le déchiffrer.

Une mesure visant à éliminer les menaces contre l'intégrité des messages consiste à signer ces messages ; une signature est envoyée en même temps que le message, et sa vérification par la partie destinataire sert à authentifier le message et son auteur.

Il convient de bien noter que cette signature n'a rien à voir avec le "jeton" symbolisant, suivant l'invention, le transfert de responsabilité attachée à la protection des fonds enfermés ou non dans une caissette 1 ; ce "jeton" est un message comme un autre, et il n'est pas forcément transmis au cours d'une authentification (par exemple il n'est jamais transmis à une station 5, qui pourtant doit être authentifiée par ses partenaires, directement ou indirectement). La signature est une preuve et la prise en compte des messages n'est possible qu'après vérification de cette preuve.

Suivant une caractéristique complémentaire de l'invention, cette signature, ou preuve, est calculée sur les paramètres de la transaction, c'est-à-dire le contenu des messages, suivant un algorithme semblable à l'algorithme DES de chiffrement, ce qui procure l'avantage notable de simplifier l'élaboration des messages échangés entre les parties du système. Les clefs de chiffrement et d'authentification sont différentes, ce qui augmente encore la sécurité cryptographique.

Par ailleurs, il devient avantageux d'intégrer dans un même circuit électronique, appelé "puce DES", l'algorithme de chiffrement et d'authentification des messages, et de pouvoir placer un tel circuit électronique à l'intérieur de chacune des caissettes 1. L'utilisation d'une "puce DES" permet notamment d'y mémoriser toutes les clefs et de procéder plus facilement à sa destruction en cas d'agression. En outre, un microprocesseur gère l'ensemble de l'électronique d'une caissette 1, et une implantation logicielle de l'algorithme DES dans ce microprocesseur tiendrait une place beaucoup trop importante en mémoire.

La "puce DES" procède donc à la fois au chiffrement du message et à la constitution de la signature sur ce message.

Il convient néanmoins de noter que le chiffrement n'est pas une opération obligatoire, car la connaissance par un tiers du contenu des messages, par exemple les instructions de changement de modes ou les paramètres d'un transport, ne met pas en cause la sécurité du système ; seule l'authentification fournie par la signature construite sur ces messages compte, et il ne serait donc pas possible de tromper l'électronique d'une caissette avec un faux message en clair non authentifié. Le chiffrement est une précaution visant pour l'essentiel à rassurer les utilisateurs sur les capacités de confidentialité du système.

Par ailleurs, certains codes secrets peuvent transiter entre deux parties du système ; le chiffrement devient alors nécessaire pour protéger ces codes.

Les stations 5 possèdent également une "puce DES", protégée physiquement, et contenant des clefs de chiffrement et d'authentification des messages qu elle transmet vers l'ordinateur 4 superviseur. On notera que ces clefs sont différentes des clefs utilisées par les caissettes 1. Un message à destination de l'ordinateur 4, provenant d'une caissette 1, est de cette façon doublement chiffré et authentifié : par la caissette 1 avec un premier couple de clefs, et par la station 5 avec un second couple de clefs.

Suivant la variante préférée l'invention, il a été choisi un algorithme de chiffrement symétrique, c est-à-dire un algorithme pour lequel la même clef est utilisée par les deux parties. Cet algorithme convient parfaitement pour les transactions qui sont établies entre une caissette 1, une station 5 et l'ordinateur 4 superviseur, puisqu'il peuvent être munis de circuits électroniques utilisés à cet effet sans aucun problème. Comme on l'a dit, la clef de chiffrement est différente de la clef servant à élaborer la signature, avec pratiquement le même algorithme. Cela signifie que pour authentifier toutes les autres parties, chaque partie du système doit partager avec ces autres un couple de clefs unique. En particulier, chaque caissette 1 doit pouvoir authentifier chacune des stations 5 auxquelles elle se connecte, chaque station 5 devant quant à elle authentifier chaque caissette 1 ; le nombre de clefs à mémoriser dans de telles conditions devient vite pléthorique et il a été choisi, suivant une variante préférentielle de l'invention, de procéder indirectement aux authentifications entre notamment les caissettes 1 et les stations 5.

Conformément à la figure 2, l'authentification indirecte est possible par transitivité, c'est-à-dire

que si deux parties A et B se sont authentifiés mutuellement, et si la partie A et une partie C se sont également authentifier mutuellement, alors les parties B et C s'authentifie mutuellement par l'intermédiaire de A, puisqu'il est un partenaire fiable de toutes les parties.

Suivant la variante préférentielle de l'invention, l'ordinateur 4 superviseur joue le rôle de la partie A, les caissettes 1, les stations 4, et les utilisateurs jouant le rôle des parties B ou C. Seul l'ordinateur 4 connait toutes les clefs. Les autres parties ne partagent, quant à elles, qu'une unique clef avec cet ordinateur 4.

Cet avantage considérable possède une contrepartie qui peut paraître lourde. En effet, chaque fois que deux parties du système dialoguent, il est nécessaire que ces parties établissent directement une connexion avec l'ordinateur 4 afin, tout d'abord, de s'authentifier mutuellement avec lui, puis de s'assurer que l'autre partie est déjà authentifiée.

L'ordinateur 4 devient néanmoins, dans ce cas, un intermédiaire obligatoire des transactions, et peut, de façon inattendue, en mémoriser l'historique. L'ordinateur 4 est par conséquent la mémoire insoupçonnable du système.

L'authentification des utilisateurs du système demeure, suivant l'invention, un cas particulier qu'il convient de noter.

Dans une première variante, chaque utilisateur possède un code secret lui permettant d'accéder au système. Ce code est connu de l'ordinateur 4 superviseur, qui le transmet, parfois, à une caissette 1 lorsque celle-ci se trouve dans un mode où sa connaissance lui est nécessaire. La station 5 reliant les parties peut éventuellement connaître également ce code, de manière à ne pas autoriser une connexion de l'utilisateur à l'ordinateur 5 sans une vérification préalable. Il est donc évident que ce code transite entre les parties. Cependant, pour ne pas permettre sa lecture aisée par un tiers, branché sur le réseau frauduleusement, ce code peut être chiffré lors de son transit par la station 5, notamment au moyen de l'algorithme préférentiellement utilisé dans l'invention.

Une autre procédure consiste à utiliser une fonction unilatérale f pour protéger ce code. Une fonction unilatérale $\bar{f}$ est une fonction dont il est très difficile de calculer l'inverse (la fonction puissance par exemple) . Si a est un code, seul $b = f(a)$ est connu de la station 5 ou de la caissette 1 ; la connaissance de b ne permettant pas de retrouver a , le code a est protégé. Si l'utilisateur rentre le code c , la station 4 ou la caissette 1 calculent $d = f(c)$ et comparent d et b ; si $d = b$, alors c est égal sûrement à a. Suivant l'invention, une fonction unilatérale particulièrement avantageuse à utiliser est $f = DES(x, a)$ où x est un message fixe et a le code secret : on utilise en effet une nouvelle fois la "puce DES".

Dans une autre variante de l'authentification d'un utilisateur du système, la procédure est conforme aux procédures d'authentification utilisées entre les autres parties. L'utilisateur dispose d'une carte à mémoire et d'un code fixe ; après reconnaissance interne du code, la carte génère un "jeton" qui est envoyé au système, ce "jeton" étant chiffré et signé par les mêmes algorithmes que ceux utilisés par ailleurs - on implémente à cet effet l'algorithme DES dans le microprocesseur de la carte -. La confidentialité et l'intégrité est parfaite, puisque l'information qui circule entre les parties est parfaitement aléatoire, et ne permet pas de remonter au code ou aux clefs de chiffrement et d'authentification. Pour s'introduire dans le système, il est alors nécessaire de posséder à la fois la carte et le code.

On décrira maintenant, conformément à la figure 3, l'organisation préférée du système conforme à l'invention, et notamment les différents états logiques, ou modes, pouvant caractériser une caissette 1. On décrira également les transitions entre ces modes, en suivant "l'histoire" d'une caissette 1 depuis le dépôt des fonds jusqu'à son ouverture par le destinataire, après sa livraison.

Sur la figure 3, les modes sont représentés par des ellipses contenant un code à deux lettres représentant chacun le nom d'un mode . Ces modes, définis par la suite, sont respectivement :

- le mode Départ représenté par le code DP,
- le mode Trottoir représenté par le code TR,
- le mode Socle représenté par le code SC,
- le mode Camion représenté par le code CM,
- le mode Depalarm représenté par le code DA,
- le mode Connect représenté par le code CO,
- le mode Servouv représenté par le code VO,
- le mode Selfouv représenté par le code SO,
- le mode Ouvert représenté par le code OV,
- le mode Caisse représenté par le code CA,
- le mode Coffre représenté par le code CF,
- le mode Verse représenté par le code VE,
- le mode Ferme représenté par le code FE,
- le mode Verrou représenté par le code VR,
- le mode Refus représenté par le code RF.

Sur la même figure, les autres blocs contenant le code CS représentent l'établissement d'une connexion entre la caissette 1 et l'ordinateur superviseur 4.

Considérons donc des fonds, composés de cartes bancaires, de billets de banque et de chèques, que l'agence centrale d'une banque désire expédier à sa succursale située à distance.

Les fonds se trouvent alors sous la responsabilité du chef de l'agence centrale. Localement se trouve une station 5 du réseau constituant le système de protection selon l'invention. A cette station

5, appelée station de départ, est connectée une caissette 1 (il peut s'y connecter plusieurs) ne contenant pas forcément de fonds. Dans cette situation, les trois modes possibles pour la caissette 1 sont le mode Ouvert, le mode Caisse, et le mode Coffre.

Dans le mode Ouvert, la caissette 1 est considérée comme étant ouverte, mais son ouverture physique, grâce à des moyens prévus à cet effet, n'est pas obligatoire ; on peut l'ouvrir et la fermer à la manière d'un simple tiroir, la protection de fonds placés à l'intérieur étant alors nulle. Ni la caissette 1, ni l'ordinateur 4, ni la station de départ n'en sont responsables.

Le mode Caisse est un mode "local", c'est-à-dire que la transition vers ce mode depuis le mode Ouvert est possible sans que l'ordinateur 4 intervienne. Dans ce mode, le chef d'agence confie à la caissette 1 des fonds. Après versement de ces fonds et fermeture, celle-ci ne peut être ouverte qu'au moyen d'une authentification du chef d'agence, c'est-à-dire par exemple au moyen d'un code secret $\bar{a}$ dont la caissette 1 et la station de départ ne connaissent que le transformé par une fonction unilatérale telle que la fonction DES($\bar{x}$, $\bar{a}$) - on notera que le message fixe $\bar{x}$ est différent pour la caissette 1 et pour la station -. La responsabilité de la protection des fonds est donc partagée, dans ce mode Caisse, entre le chef d'agence et la caissette 1 (rappelons que la station de départ, qui est la borne commune de transmission du réseau, n'est jamais responsable). Il est à noter que la transition du mode Ouvert au mode Caisse a étendu une première fois le système : on est passé du système :chef d'agence: au système :chef d'agence/caissette:.

Le mode Coffre est un mode "global", c'est-à-dire que la transition du mode Ouvert vers ce mode n'est possible qu'avec l'autorisation de l'ordinateur 4 superviseur situé à distance. Dans ce mode, le chef d'agence confie des fonds au système et transmet totalement la responsabilité de leur protection. Après avoir placé les fonds dans une caissette 1, et refermé celle-ci, il donne son code qui est authentifié par la station de départ, et indique au système qu'il désire utiliser la caissette 1 en mode Coffre. La station de départ établit une connexion avec l'ordinateur 4, conformément à un protocole d'authentification mutuelle. L'ordinateur 4 authentifie alors le chef d'agence. La caissette 1 dans laquelle celui-ci veut placer des fonds doit être en état et ne pas être un clone ; celle-ci doit donc s'authentifier mutuellement avec l'ordinateur 4 par l'intermédiaire de la station de départ, qui est un partenaire fiable de l'ordinateur 4, mais ne peut authentifier directement la caissette 1 pour des raisons exprimées plus haut. Toutes les authentifications étant directement ou implicitement effectuées, le système, par l'intermédiaire de l'ordinateur 4, accepte, d'une part, le transfert de responsabilité venant du chef d'agence, et d'autre part, tourne la caissette 1 dans le mode Coffre. Dans la transition du mode Ouvert au mode Coffre, on est passé du système :chef d'agence: au système :caissette/ordinateur:. Cette transition s'est effectuée progressivement, la responsabilité appartenant au chef d'agence jusqu'à l'accord final de l'ordinateur 4 - il y a eu des élargissements successifs puis un rétrécissement du système -.

La transition du mode Coffre au mode Ouvert s'effectue de manière identique, l'ordinateur 4 conservant la responsabilité de la protection des fonds jusqu à authentification complète de toutes les parties ; on passe dans ce cas du système :caissette/ordinateur: au système :caissette/ordinateur/sta-tion: puis au système :caissette/ordinateur/station/chef d'agence: et enfin au système :chef d'agence: avec transfert de la responsabilité dans le mode Ouvert.

Les transitions du mode Ouvert aux modes Caisse ou Coffre peuvent en outre dépendre d'une programmation horaire, transmise par l'ordinateur 4 à la caissette 1 lors de son arrivée à l'agence. Une telle programmation horaire peut être hebdomadaire et permet notamment d'interdire l'ouverture de la caissette 1 en dehors de certaines heures fixées à l'avance. Suivant une variante de l'invention non représentée, on peut regrouper les modes Caisse et Coffre en un seul mode, appelé par exemple mode Stockage, auquel on associe deux options d'ouverture - Caisse ou Coffre -, le choix entre ces options étant fait par programmation horaire transmise à un moment donné à la caissette 1 par l'ordinateur 4.

A partir du mode Caisse ou du mode Coffre, le chef d'agence peut demander à envoyer des fonds à la succursale. Il existe pour ce faire un mode Verse, analogue au mode Ouvert, mais qui ne peut pas être suivi du mode Caisse ou du mode Coffre. Le mode Verse impose que les fonds placés dans une caissette 1 soient transportés. Les transitions du mode Caisse ou du mode Coffre vers le mode Verse s'effectuent de la même façon que les transitions de ces modes vers le mode Ouvert, c'est-à-dire qu'elles sont initiées par l'authentification préalable du code du chef d'agence.

Après fermeture d'une caissette 1 se trouvant dans le mode Verse, celle-ci se tourne automatiquement dans le mode Fermé où il est impossible de l'ouvrir sans connexion à l'ordinateur 4. La transition du mode Verse au mode Fermé signifie que le système :caissette: a provisoirement accepté le transfert de responsabilité. Ce mode est cependant temporaire car une connexion est établie immédiatement, via la station de départ, avec l'ordinateur 4, afin d'obtenir son accord sur ce verse-

ment. En cas de refus (qui peut intervenir par exemple si la station d'arrivée n'existe pas ou plus, ou si la caissette 1 n'est plus en état), la caissette 1 se tourne dans le mode Refus puis dans le mode Ouvert et la procédure d'envoi des fonds est annulée. En cas d'accord de l'ordinateur 4, et après les authentifications mutuelles nécessaires, il y a transition du mode Fermé au mode Verrou, dans lequel le système :caissette/ordinateur: est responsable des fonds.

Dans le mode Verrou, la caissette 1 doit être nécessairement transportée à la station d'arrivée pour pouvoir être réouverte (sauf indication différente de l'ordinateur 4). Le système attend alors le convoyeur 3 de la caissette 1 qui est authentifié, à son arrivée, par vérification d'un code, dont le transformé par une fonction unilatérale est connue du système ; il est établi une connexion avec l'ordinateur 4 qui seul connait ce code et la fonction unilatérale correspondante (il n'est en effet pas nécessaire que la caissette 1 ou la station le connaisse). Il est à noter que le mode Verrou peut durer très longtemps : l'ordinateur 4, qui a reçu de la station. les paramètres du transport, ne les a pas encore transmis à la caissette 1. L'un de ces paramètres est notamment la durée prévue du transport - conformément au brevet français FR-2 550 364, des consignes temporelles limitent en effet la durée d'un trajet et conduisent à la destruction d'une caissette 1 en cas de dépassement -.

Après authentification du convoyeur 3, l'ordinateur 4 donne l'autorisation d'enlèvement de la caissette 1 qui se trouve alors dans le mode Départ. La transition du mode Verrou vers ce mode s'accompagne du transfert de la responsabilité du système :caissette/ordinateur: vers le système :caissette:, c'est-à-dire que la caissette 1 assure totalement la protection des fonds à transporter. C'est pourquoi les consignes temporelles de transport sont initiées dès la transition dans ce mode ; la caissette 1 est par conséquent considérée comme mobile, qu'elle soit ou non enlevée physiquement de son socle. En cas de dépassement du temps prévu de livraison, la caissette se considère comme étant agressée et dégrade son contenu par des moyens appropriés..

Après son enlèvement physique, la caissette 1 quitte le mode Départ pour le mode Trottoir. Celui-ci correspond au trajet à pied qu'effectue le convoyeur 3 en portant la caissette 1, entre la station de départ et un véhicule, ou une autre station (si la totalité du trajet s'effectue à pied). Ce mode est délimité temporellement par une durée prévue à cet effet, de manière à réduire les risques de détournement lors du trajet ; en cas de dépassement de la durée prévue du trajet, la caissette 1 dégrade son contenu.

Le transport de l'agence centrale de la banque à une succursale s'effectue généralement au moyen d'un véhicule. A l'intérieur de celui-ci, se trouve un ordinateur de bord, gérant une électronique permettant de contrôler les caissettes 1 à transporter. La connexion physique à cette électronique d'une caissette 1 en mode Trottoir provoque la transition de ce mode vers le mode Socle. Le réceptacle physique d'une caissette 1 est le même que celui situé dans une station, et c'est pourquoi la caissette 1 envoie un message d'identification vers l'électronique :

- si elle reconnait une station, elle demande immédiatement une connexion à l'ordinateur 4 superviseur : il y a transition vers le mode Connect.
- si elle reconnait l'électronique du bon véhicule, il y a transition vers le mode Camion.
- si elle ne reconnait ni l'un ni l'autre, il y a transition vers le mode Depalarm.

Dans le mode Depalarm, la caissette 1 se retrouve physiquement dans une situation imprévue et doit être déconnectée de son réceptacle ; sinon, après un temps déterminé (par exemple 30 secondes), le décompte de la durée du trajet à pied reprend. Néanmoins, la caissette 1 attend d'être déconnectée pour repasser logiquement du mode Depalarm au mode Trottoir : de cette façon, le mode Trottoir correspond toujours à la déconnexion physique de la caissette 1.

Le mode Camion correspond à la suite logique du transport. Dans ce mode, la caissette 1 ne peut être déconnectée sans en être prévenue ; elle dégrade en effet son contenu au delà d'un certain intervalle de temps (par exemple 10 secondes) si elle n'a pas été reconnectée. A l'arrivée du véhicule à la succursale, le convoyeur 3 s'authentifie de nouveau à la caissette 1 par l'intermédiaire de l'ordinateur de bord - le code du convoyeur 3 a été transmis provisoirement à la caissette 1 par l'ordinateur 4 superviseur au moment de la transition du mode Verrou au mode Départ -. Si la caissette 1 accepte le code du convoyeur 3, elle passe dans le mode Départ (d'où elle pourra passer dans le mode Socle et enfin dans le mode Connect).

Il est important de noter que l'organisation en modes rend réalisable une intervention en cas d'accident du véhicule initial. Il suffit alors d'envoyer vers le lieu de l'accident un véhicule possédant un code de reconnaissance connu de la caissette 1, de déconnecter légalement la caissette 1 du véhicume accidenté, avec le code du convoyeur 3, et de la reconnecter sur le nouveau véhicule -l'ordinateur 4 transfère à cet effet les numéros matricules de deux véhicules à la caissette 1 lors de la transition du mode Verrou au mode Départ -. On peut de cette manière passer plusieurs fois dans les modes Socle, Camion ou Départ lors d'un transport d'une station de départ à une station d'arrivée ; seules les consignes temporelles doi-

vent être respectées.

La transition du mode Socle vers le mode Connect a lieu si la caissette 1 reconnait qu'elle est connectée sur une station. Elle demande alors immédiatement à être connectée à l'ordinateur 4 superviseur, ce qui nécessite l'authentification mutuelle préalable de la station et de cet ordinateur 4 ; si cette authentification mutuelle est possible, on sait déjà que la station n'est pas un clone. L'ordinateur 4 et la caissette 1 s'authentifie ensuite mutuellement. Si la station sur laquelle est connectée la caissette 1 n'est pas la bonne, il se produit alors une transition du mode Connect au mode Depalarm. Si la station est la station d'arrivée prévue, le système :caissette: devient le système :caissette/ordi-nateur/station d'arrivée: et on passe du mode Connect au mode Selfouv ou au mode Servouv.

Le choix entre ces deux modes est effectué par l'ordinateur 4 superviseur au moment de l'authentification mutuelle caissette 1/ordinateur 4. Ces modes sont conceptuellement comparables au mode Caisse et au mode Coffre respectivement, mais aboutit toujours au mode Ouvert, déjà décrit, dans lequel la caissette 1 est considérée comme étant ouverte. Dans le mode Selfouv, seule la caissette 1 authentifie le code du chef de la succursale pour pouvoir être ouverte. Dans le mode Servouv, après authentification de ce code par la caissette 1, celle-ci demande à être connectée à l'ordinateur 4, qui à son tour procède aux authentifications requises.

Dans le mode Ouvert, la caissette 1 peut être vidée de ses fonds, la responsabilité de leur protection étant alors transférée au chef de la succursale.

La caissette 1 peut à nouveau servir soit comme caisse, soit comme coffre, soit pour un autre transport, conformément aux procédures décrites ci-dessus.

De nombreuses variantes de cette organisation préférée du système sont bien entendu envisageables sans sortir du cadre de l'invention, et peuvent combiner dans un ordre quelconque les trois types de modes possibles. La seule condition à respecter pour ce faire est le respect des procédures d'authentification, lors des extensions ou des restrictions du système, c'est-à-dire lors du transfert de la responsabilité attachée à la protection des fonds.

Il convient en outre de noter que l'utilisation d'algorithmes de chiffrement des messages échangés entre les parties du système nécessite des supports de liaison fiables à faible taux d'erreurs.

Ceci n'est pas nécessairement le cas, car l'infrastructure à mettre en place serait nécessairement lourde, notamment au niveau des agences et de leurs succursales, où se trouvent, intégrés aux stations 5, les moyens de télécommunications avec l'ordinateur 4 superviseur : modems couteux, liaisons spécialisées à faible taux d'erreurs, etc... Or ces agences ne disposent généralement que de lignes téléphoniques courantes à taux d'erreurs élevé (1 information binaire fausse en moyenne pour 10 000 transmises).

On met par conséquent en place un protocole pour la correction des erreurs de transmission entre une borne du système, ou station 5, et l'ordinateur 4 superviseur. Ce protocole fractionne le message à transmettre en blocs de quelques octets à quelques dizaines d'octets. Si un bloc est transmis avec des erreurs, seul ce bloc est retransmis, ce qui permet de ne pas avoir à répéter l'intégralité des messages très longs qui sont échangés (typiquement d'une longueur de 300 octets). L'intégrité d'un bloc est contrôlée au moyen d'une signature élaborée avec le contenu du bloc et avec son entête - cette entête comportant essentiellement l'information de longueur du bloc -. L'algorithme de calcul de cette signature non secrète est avantageusement celui servant au chiffrement et à l'authentification des messages ; on utilise de cette façon à nouveau la "puce DES", sans avoir à écrire et à stocker, notamment dans la station, un nouvel algorithme.

Après reconstitution du message fractionné à l'émission, et dans le cas où la partie émettrice est l'ordinateur 4 superviseur, la station 5 authentifie et déchiffre avec ses propres clefs ledit message (grâce à la "puce DES" placée dans la station). Puis elle transmet à la caissette 1, dont le matricule servant à l'identifier lui apparait maintenant en clair, la partie du message qui lui est destinée ; la caissette 1 authentifie et déchiffre ce message avec ses propres clefs, grâce à la "puce DES" prévue à cet effet. Elle en confirme alors la réception à l'ordinateur 4 et prépare à cet effet un message chiffré et authentifié avec ces mêmes clefs ; ce message est transmis à l'ordinateur 4 - complété par le matricule de la caissette 1 - chiffré et authentifié avec les clefs de la station 5. L'ordinateur 4 renvoie alors, selon le même protocole, un acquit à la caissette 1, qui peut éventuellement changer de mode, mais uniquement à la réception de cet acquit.

Le protocole de télécommunications décrit n'est bien entendu pas limité à la réalisation préférentielle décrite ci-dessus, et on peut par exemple employer les principes d'architecture fonctionnelle popularisés par le modèle d'interconnexion des systèmes ouverts (modèle en couches OSI), ou des dérivés directs de ce modèle.

La présente invention est notamment destinée à la protection de documents ou d'objets de valeur, et notamment de moyens de paiement tels que des billets, des chèques ou des cartes bancaires, ou encore de médicaments dangereux (drogues)

ou à forte valeur ajoutée. Cette protection est assurée aussi bien à l'intérieur d'une agence bancaire (ou d'une officine pharmaceutique, ou autre), que lors du transport de cette agence vers une succursale. La présente invention n'est limitée en outre ni par la taille, ni par le poids des objets ou des documents de valeur que l'on désire protéger, et il est à la portée de l'homme de l'art de procéder à toute modification visant à adapter l'invention à des objets ou des documents autres que ceux donnés ici à titre d'exemples non limitatifs.

Revendications

1 - Système de protection de documents ou d'objets de valeur, et notamment de moyens de paiement tels que des billets de banque, des chèques, ou des cartes bancaires, enfermés dans au moins un contenant inviolable physiquement, appelé caissette (1), qui, en cas d'agression, provoque leur dégradation par des moyens appropriés, ce système étant caractérisé en ce que le cycle de fonctionnement d'une caissette (1) comporte un nombre restreint d'états logiques, appelés modes, la transition d'un premier mode à un second mode étant la conséquence d'un événement ponctuel, dont on vérifie la *licéité* par un moyen adéquat et autonome pouvant se mettre en relation avec la caissette (1), ladite transition s'accompagnant alors de la perte de mémoire, par la caissette (1), de son mode antérieur.

2 - Système de protection selon la revendication 1, caractérisé en ce qu'une caissette (1) n'est totalement responsable des documents ou des objets de valeur qui y sont enfermés que durant son transport, qui est délimité, d'une part, par la transition d'un mode où la caissette (1) est considérée comme étant fixe à un mode où elle est considérée comme étant mobile, d'autre part, par la transition d'un mode où la caissette (1) est considérée comme étant mobile à un mode où elle est considérée comme étant fixe.

3 - Système de protection selon l'une quelconque des revendications précédentes, caractérisé en ce que le moyen pouvant se mettre en relation avec une caissette (1) pour contrôler la *licéité* des transitions entre certains modes de fonctionnement de ladite caissette (1), est constitué par un ordinateur (4) unique, pouvant être notamment un centre serveur situé à distance, dont on assure par ailleurs la protection logique et physique.

4 - Système de protection selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il peut comporter successivement, totalement, ou en partie seulement, les éléments d'un ensemble constitué par :

- un utilisateur des documents ou des objets de valeur, que se soit un expéditeur (2), un destinataire, ou un convoyeur (3),
- une caissette (1),
- le moyen pouvant se mettre en relation avec ladite caissette (1) pour contrôler la *licéité* des transitions entre certains modes de fonctionnement de celle-ci,

lesdits éléments pouvant être reliés entre eux par l'intermédiaire d'une borne unique, appelée station (5), de manière à constituer un réseau en étoile dont ladite station (5) est le centre, ce qui procure une confidentialité structurelle audit système.

5 - Système de protection selon la revendication 4, caractérisé en ce qu'une station (5) n'est jamais responsable de la sécurité d'une caissette (1) et/ou des documents ou des objets de valeur qui y sont placés, c'est-à-dire qu'elle ne contrôle jamais la *licéité* d'un événement pouvant provoquer une transition d un mode de fonctionnement d'une caissette (1) vers un autre mode.

6 - Système de protection selon l'une quelconque des revendications 4 ou 5, caractérisé en ce qu'une station (5) est équipée des moyens de communication adéquats servant à mettre en relation :

- une caissette (1) et le moyen pouvant se mettre en relation avec ladite caissette (1) pour contrôler la *licéité* des transitions entre certains modes de fonctionnement de celle-ci,
- une caissette (1) et un utilisateur des documents ou des objets de valeur contenus dans ladite caissette (1), que se soit un expéditeur (2), un destinataire, ou un convoyeur (3),
- un utilisateur des documents ou des objets de valeur contenus dans une caissette (1), que se soit un expéditeur (2), un destinataire, ou un convoyeur (3), et le moyen pouvant se mettre en relation avec ladite caissette (1) pour contrôler la *licéité* des transitions entre certains modes de fonctionnement de celle-ci,

7 - Système de protection selon l'une quelconque des revendications précédentes, caractérisé en ce que les communications entre deux des parties du système s'effectuent selon un protocole permettant à la partie recevant un message d'authentifier la partie qui est sensée l'avoir émis, cette authentification s'accompagnant éventuellement de l'envoi d'un message de bonne réception à ladite partie émettrice.

8 - Système de protection selon la revendication 7, caractérisé en ce que l'authentification de la partie émettrice d'un message consiste à authentifier le message lui-même, par vérification d'une signature informatique, calculée sur le contenu dudit message au moyen d un algorithme à clefs, ces clefs étant détenues uniquement par la partie émettrice du message et la partie devant le recevoir.

9 - Système de protection selon l'une quelconque

des revendications 7 ou 8, caractérisé en ce que l'intégration au système d'une partie nouvelle est précédée :
- de l'authentification de ladite partie nouvelle par l'une seulement des parties intégrantes du système,
- réciproquement, de l'authentification de ladite partie intégrante par ladite partie nouvelle,
cette authentification mutuelle desdites parties permettant alors à toutes les parties du système de s'authentifier mutuellement et implicitement, par transitivité, à ladite partie nouvelle.

10 - Système de protection selon la revendication 9, caractérisé en ce que l'authentification mutuelle d'une caissette (1) et d'une station (5) sur laquelle elle a été connectée est toujours implicite, et nécessite, d'une part, l'authentification mutuelle préalable de ladite station (5) au moyen pouvant se mettre en relation avec ladite caissette (1) pour contrôler la *licéité* des transitions entre certains modes de fonctionnement de celle-ci, d'autre part, l'authentification mutuelle préalable de ladite caissette (1) audit moyen, qui peut alors mémoriser avantageusement toutes les transactions entre les parties, cette configuration du système permettant par ailleurs de limiter, dans ladite station (5) et ladite caissette (1), le nombre de clefs d'authentification à mémoriser.

11 - Système de protection selon la revendication 7, caractérisé en ce que l'authentification d'un utilisateur des documents ou des objets de valeur contenus dans une caissette (1), que se soit un expéditeur (2), un destinataire, ou un convoyeur (3), s'effectue au moyen d'un code secret, dont seul le transformé, par une fonction unilatérale, est connu de la partie authentifiant cet utilisateur.

12 - Système de protection selon la revendication 7, caractérisé en ce que l'authentification d un utilisateur des documents ou des objets de valeur contenus dans une caissette (1), que se soit un expéditeur (2), un destinataire, ou un convoyeur (3), s'effectue au moyen d'un message chiffré et authentifié, qui est généré par une carte à mémoire dont l'utilisation par l'utilisateur nécessite la connaissance d'un code.

13 - Système de protection selon l'une quelconque des revendications précédentes, caractérisé en ce que les messages échangés entre deux parties du système sont chiffrés au moyen d'un algorithme de chiffrement à clefs, qui sont détenues uniquement par ces deux parties, ledit algorithme pouvant avantageusement être, par exemple, une variante de l'algorithme servant à élaborer une signature d'authentification dudit message.

Fig_1

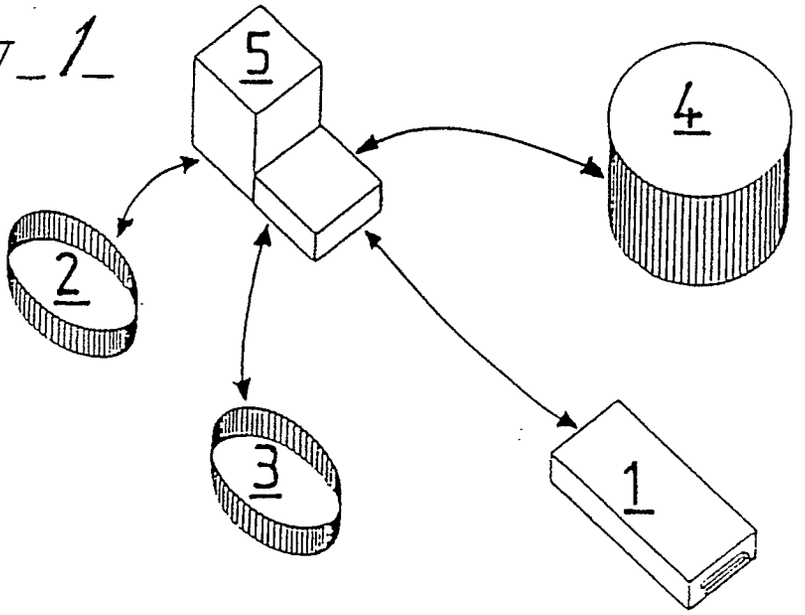
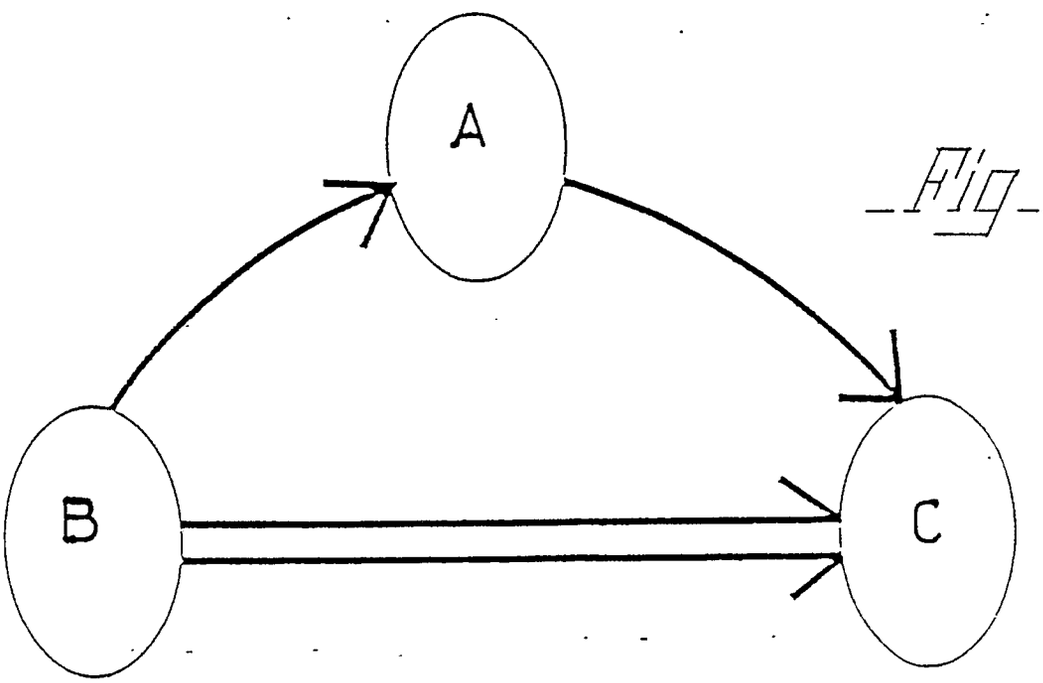


Fig_2



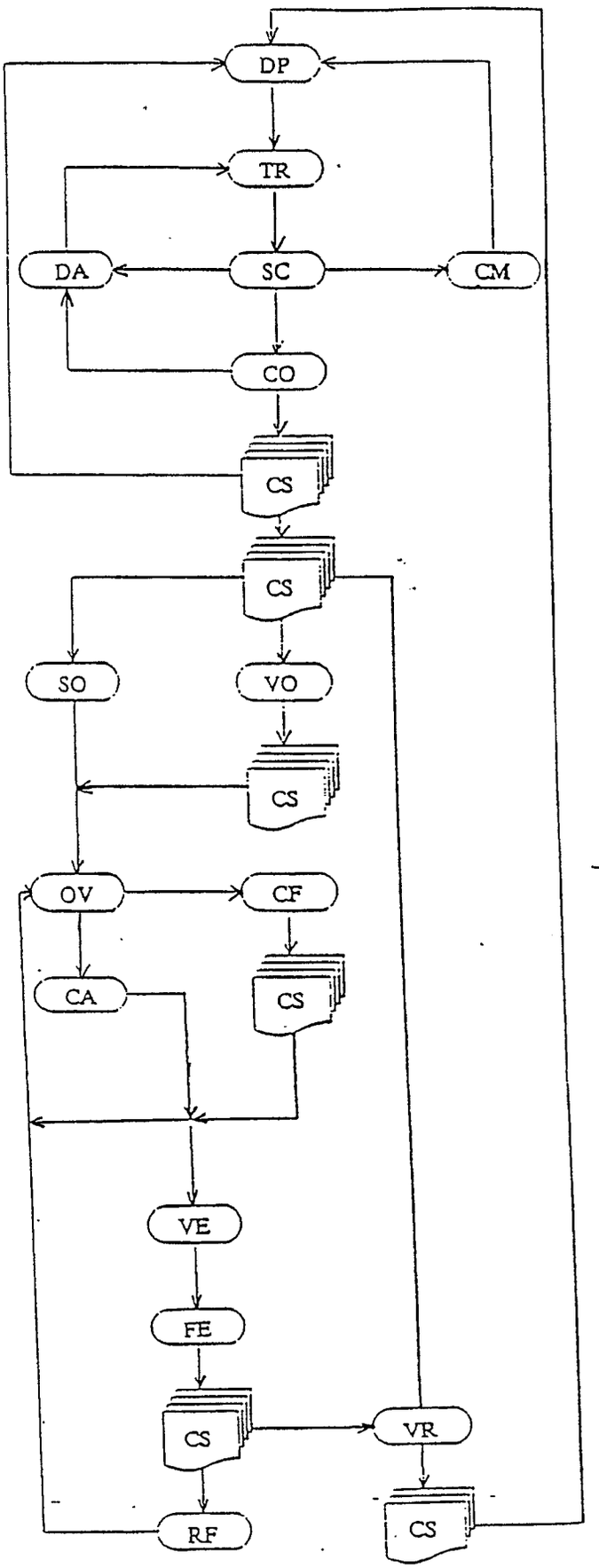


Fig 3

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande

EP 90 40 2060

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.5)
D,A	FR-A-2594169 (SOCIETE AXYTEL) * le document en entier * ---	1	E05G1/00 G07F9/06
A	EP-A-30413 (LUNDBLAD) * page 1, lignes 1 - 23 * * page 2, lignes 13 - 26 * * page 3, lignes 6 - 37 * * page 4, lignes 1 - 9 * * page 4, lignes 27 - 30 * * page 5, lignes 5 - 12 * * page 6, lignes 20 - 35; figures 1, 2 * ---	1-6	
A	EP-A-307375 (INTER INNOVATION AB) * colonne 1, ligne 49 - colonne 59; revendication 1 * -----	1-6	

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
E05G
G07F
G08B

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	22 OCTOBRE 1990	GUILLAUME G.E.P.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0402)