(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 820 848**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 01962**

(51) Int Cl[7] : **G 06 F 12/14,** G 06 K 19/073, H 04 L 9/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 13.02.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 16.08.02 Bulletin 02/33.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

(71) **Demandeur(s) :** *GEMPLUS Société anonyme* — FR.

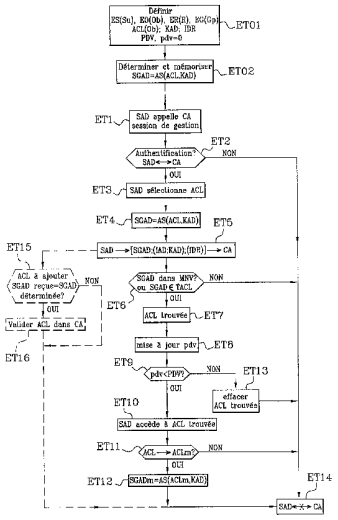
(72) **Inventeur(s) :** GIRARD PIERRE et GIRAUD JEAN LUC.

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

(74) **Mandataire(s) :**

(54) GESTION DYNAMIQUE DE LISTES DE DROITS D'ACCES DANS UN OBJET ELECTRONIQUE PORTABLE.

(57) Des listes de droits d'accès (ACL) telles que des listes de contrôle d'accès ou des capacités sont gérées dynamiquement dans un moyen de traitement de données tel que carte à puce (CA) depuis un serveur d'administrateur (SAD). Pour accéder à une liste de droits d'accès (ACL) depuis le serveur, la liste est signée (ET4) dans le serveur afin de transmettre (ET5) une signature (SGAD) à la carte. La carte compare (ET6) la signature reçue à des signatures déterminées en fonction de listes de droits d'accès contenues dans la carte et de clés respectivement associés à ces listes. L'accès du serveur n'est autorisé à une liste trouvée (ACL) qu'en correspondance avec une signature trouvée parmi les signatures déterminées dans la carte et identique à la signature reçue.



FR 2 820 848 - A1

2820848

Gestion dynamique de listes de droits d'accès dans un objet électronique portable

La présente invention concerne d'une manière générale la gestion de droits d'accès par des sujets constituant des utilisateurs ou modules de logiciels d'un moyen de traitement de données, à des objets tels que des applications implémentées dans le moyen de traitement de données. Plus particulièrement, l'invention a trait à l'administration des accès à des ressources dans un objet électronique portable, tel qu'une carte à puce dite également carte à microcontrôleur ou à circuit intégré, constituant le moyen de traitement de données, notamment lorsque la carte à puce est une carte multi-applicative.

A cause du nombre de plus en plus élevé des applications de plus en plus complexes introduites dans une carte à puce, la gestion des applications constituant les ressources principales de la carte à puce sont de plus en plus difficilement gérables. Les difficultés de gestion sont également dues aux nombreux partenaires intervenant dans l'attribution des accès aux applications et dont les intérêts divergent parfois. Ces partenaires peuvent être le fabricant de la carte à puce, le distributeur ou l'opérateur de la carte à puce, et les développeurs des applications dans la carte à puce.

Néanmoins, malgré cette complexité, l'accès aux ressources de la carte à puce doit être contrôlé et sécurisé.

Actuellement, l'accès à une ressource de traitement, telle qu'une application, est effectuée en transmettant depuis un terminal d'accueil de la carte à puce au moins une commande constituant une

unité de données de protocole applicatif APDU (Application Protocol Data Unit) qui contient des données ou une référence à des données présentes et à traiter dans la carte. Selon une autre variante, l'accès à une ressource dans la carte peut être effectué à un niveau supérieur en invoquant une méthode d'un objet présent dans la carte lorsque celle-ci contient des applications écrites en un langage de programmation de haut niveau orienté objet tel que le langage Java.

La coexistence et la coopération de plusieurs applications au sein d'une même carte à puce soulève de nombreux problèmes du point de vue de la sécurité. En particulier, chaque application possède ses propres données pour lesquelles le développeur de l'application définit des droits d'accès propres à l'application. Les conditions d'accès sont des moyens de liaison entre des accès externes qui peuvent être des utilisateurs de la carte ou bien des modules logiciels, comme des interfaces d'usager, et des accès internes à la carte tels que des applications, éventuellement par l'intermédiaire d'autres applications ou d'autres éléments logiciels d'application dans la carte.

Le contrôle des conditions d'accès repose sur l'identification des sujets Su, tels que les utilisateurs, qui sont des éléments "actifs" qui manipulent des informations contenues dans des objets Ob, tels que des applications, qui sont des éléments "passifs" contenant des données. Les conditions d'accès des sujets Su aux objets Ob sont régies par des règles de contrôle d'accès entre les sujets et les objets. Chaque règle comporte un droit d'accès, c'est-à-dire un lien entre un sujet et un objet sous

la forme d'une action qui peut être accomplie par le sujet sur l'objet.

Il est connu de représenter les conditions d'accès de sujets Su à des objets Ob par une matrice d'accès MA dont les colonnes correspondent à des sujets et dont les lignes correspondent à des objets, comme montré à la figure 1. Par exemple, la matrice MA est relative à trois sujets S1, S2 et S3, tels que trois utilisateurs, et à trois objets O1, O2 et O3, tels que des fichiers et des programmes. Chaque case de la matrice à l'intersection d'une ligne et d'une colonne contient des droits d'accès, c'est-à-dire des actions privilégiées qui peuvent être accomplies par le sujet respectif sur l'objet respectif.

Les droits d'accès peuvent être positifs pour autoriser une action prédéterminée d'un sujet sur un objet, ou peuvent être négatifs pour interdire une action prédéterminée d'un sujet sur un objet. Par exemple, le sujet S2 peut lire et exécuter l'objet O2 mais ne peut pas écrire dans cet objet, et le sujet S3 peut lire l'objet O1 mais ne peut pas enregistrer et écrire l'objet O1.

Comme il est connu, les règles de contrôle d'accès sont généralement traitées suivant deux approches.

La première approche consiste en des listes de contrôle d'accès ACL (Access Control List) correspondant aux lignes de la matrice d'accès MA et spécifiant chacune des droits d'accès de sujets à l'objet associé à la ligne. A titre d'exemple, dans une carte à puce multi-applicative du type WINDOWS (marque enregistrée), des listes de contrôle d'accès ACL définissent des accès d'utilisateurs à des fichiers inclus dans la carte.

A l'inverse, la deuxième approche consiste en des capacités correspondant aux colonnes de la matrice MA et spécifiant chacune les droits d'accès du sujet associé à la colonne sur les objets. Par exemple, le contrôle d'accès porte sur des méthodes d'applets pour cartes à puce multi-applicatives de type JavaCard dans lesquelles des programmes en langage Java ont été écrits. Les capacités sont sous la forme de pointeurs effectuant des appels pour accéder à des méthodes constituant des objets, dans des applets prédéterminés constituant des sujets.

Pour plus de simplicité, on se référera dans la suite à la gestion de listes de contrôle d'accès bien que l'invention se rapporte également à la gestion de capacités. Les listes de contrôle d'accès et les capacités sont à considérer comme des listes de droits d'accès entre au moins un sujet et au moins un objet.

Pour une carte à puce actuelle, la modification des listes de contrôle d'accès est réservée à une seule autorité d'administration de la carte. Après authentification de l'autorité d'administration par la carte, l'autorité commande des modifications des listes de contrôle d'accès, par exemple en ajoutant ou en supprimant des listes, en ajoutant ou supprimant des sujets dans une liste, ou en ajoutant ou supprimant des droits d'accès d'un sujet par rapport à un objet.

Cette unique autorité d'administration doit bien sûr respecter les exigences des différents partenaires intervenant dans l'élaboration et la gestion des différentes ressources applicatives dans la carte à puce.

La présente invention a pour objectif de rendre possible la gestion dynamique de listes de contrôle d'accès, ou de capacités, dans un objet électronique portable, de type carte à puce, afin d'affiner la gestion de ces listes ou capacités et ainsi de permettre une augmentation du nombre des administrateurs autorisés à intervenir de manière sécuritaire sur des modifications des listes de contrôle d'accès ou capacités.

Pour atteindre cet objectif, un procédé pour gérer des listes de droits d'accès entre des sujets et des objets, mémorisées dans un moyen de traitement de données depuis une entité d'administrateur externe, est caractérisé en ce qu'il comprend les étapes suivantes :

- initialement associer des clés d'entités d'administrateur à des listes de droits d'accès et fournir un algorithme de sécurisation dans le moyen de traitement de données, et

- pour accéder à une liste de droits d'accès depuis l'entité :

signer la liste de droits d'accès dans l'entité en appliquant des données déterminées de la liste et la clé à l'algorithme de sécurisation afin de produire une signature,

transmettre la signature depuis l'entité au moyen de traitement de données, et

comparer la signature reçue dans le moyen de traitement de données à des signatures déterminées en fonction des applications de données déterminées de listes de droits d'accès contenues dans le moyen de traitement de données et de clés respectivement associées à ces listes à l'algorithme de

sécurisation, et n'autoriser l'accès de l'entité à une liste de droits d'accès trouvée qu'en correspondance avec une signature trouvée parmi les signatures déterminées dans le moyen de traitement de données et identique à la signature reçue.

Ainsi selon l'invention, tout administrateur autorisé accède à une liste de droits d'accès constituant une liste de contrôle d'accès ou une capacité dans un moyen de traitement de données constitué par exemple par le microcontrôleur d'un objet électronique portable. Un droit d'accès autorise ou interdit un ou plusieurs sujets à accomplir une action sur un sujet, ou bien un sujet à accomplir une action sur un ou plusieurs objets. Cette liste de contrôle d'accès ou capacité est alors gérée dynamiquement par chaque administrateur, en l'obligeant préalablement à signer la liste de contrôle d'accès ou la capacité à laquelle il souhaite accéder, de manière à se faire reconnaître dans l'objet électronique par sa signature de la liste de contrôle d'accès ou de la capacité.

La gestion des listes de droits d'accès est ainsi décentralisée dans des entités d'administrateur externes au moyen de traitement de données.

Selon un autre caractéristique de l'invention, la durée d'application d'une liste de droits d'accès est limitée. Plus précisément, avant d'autoriser l'accès de l'entité à la liste de contrôle, un paramètre de durée de vie de la liste de droits d'accès trouvée est mis à jour afin d'effacer la liste de droits d'accès trouvée lorsque le paramètre de durée de vie mis à jour excède une limite maximale et afin d'autoriser l'accès à la liste de droits

d'accès trouvée à l'entité lorsque le paramètre de durée de vie mis à jour est inférieur à la limite maximale. La durée de vie limitée d'une liste de droits d'accès incite alors le ou les sujets concernés par cette liste devenue périmée maintenant effacée, à revenir vers le ou les administrateurs de cette liste pour leur demander à nouveau des droits d'accès.

L'invention concerne également un moyen de traitement de données notamment dans un objet électronique portable, mémorisant des listes de droits d'accès gérées depuis au moins une entité d'administrateur externe, mettant en oeuvre le procédé de l'invention. Il est caractérisé en ce qu'il comprend :

- un moyen pour mémoriser des clés d'entités d'administrateur en association à des listes de droits d'accès,
- un moyen pour implémenter un algorithme de sécurisation,
- un moyen pour déterminer des signatures en fonction des applications de données déterminées des listes de droits d'accès et de clés respectivement associées à ces listes à l'algorithme,
- un moyen pour comparer une signature reçue d'une liste de droits d'accès qui résulte, dans l'entité, de l'application de données déterminées de la liste et de la clé de l'entité à l'algorithme et qui est transmise par l'entité, auxdites signatures déterminées, et
- un moyen pour autoriser l'accès de l'entité à une liste de droits d'accès trouvée qu'en correspondance avec une signature trouvée parmi les

signatures déterminées et identique à la signature reçue.

Le moyen de traitement de données peut comprendre, en outre, un moyen pour mémoriser un paramètre de durée de vie et une limite maximale de durée pour chaque liste de droits d'accès, et un moyen pour mettre à jour le paramètre de durée de la liste trouvée afin d'effacer la liste de droits d'accès trouvée lorsque le paramètre de durée de vie mis à jour excède la limite maximale et afin d'autoriser l'accès à la liste de droits d'accès trouvée à l'entité lorsque le paramètre de durée de vie mis à jour est inférieur à la limite maximale.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un diagramme montrant une matrice de contrôle entre trois sujets et trois objets, déjà commentée selon la technique antérieure ;

- la figure 2 est un bloc-diagramme schématique d'un système de télécommunication entre un serveur d'administrateur et un objet électronique portable de type carte à puce pour la mise en oeuvre du procédé de gestion selon l'invention ; et

- la figure 3 est un algorithme d'étapes du procédé de gestion dynamique de listes de droits d'accès selon l'invention.

En référence à la figure 2, le moyen de traitement de données est un contrôleur, tel que le microcontrôleur d'une carte à puce CA qui contient

plusieurs applications constituant des objets auxquels des sujets, tels que des utilisateurs ou des unités ou moyens logiciels, peuvent accéder en fonction de droits d'accès.

De manière connue, le microcontrôleur de la carte à puce CA comporte un microprocesseur PR, une mémoire MO de type ROM, une mémoire non volatile MNV de type programmable et effaçable, comme une mémoire EEPROM, et une mémoire MA de type RAM recevant notamment des données d'un terminal d'accueil TE de la carte.

Dans la mémoire MO sont inclus notamment un système d'exploitation OS de la carte, des applications AP de communication, d'authentification et de service constituant des objets Ob, ainsi qu'un algorithme de sécurité AS utilisé pour reconnaître des signatures d'administrateur et un algorithme de gestion de listes de droits d'accès AG selon l'invention.

La mémoire MNV contient des données notamment liées au possesseur de la carte et au fournisseur de la carte, ainsi que des listes de contrôle d'accès ACL(Ob), ou bien des capacités.

Chaque liste de contrôle d'accès relative à un objet respectif Ob, à laquelle référence est faite ci-après en tant que liste de droits d'accès, contient, comme montré à la figure 1, une liste de sujets Su associés chacun à une liste de droits d'accès positifs autorisant et/ou négatifs interdisant l'accomplissement d'actions sur l'objet respectif Ob. La mémoire MNV contient ainsi un ensemble de sujet ES, un ensemble d'objet EO, c'est-à-dire un ensemble de référence à des applications, et un ensemble de règle d'accès ER. De préférence, la mémoire MNV contient également un ensemble de groupe

de sujet EG. Chaque groupe Gp réunit des sujets Su ayant chacun au moins un accès prédéterminé à un objet prédéterminé Ob ; ainsi un sujet dans un groupe Gp a tous les droits d'accès accordés à ce groupe, et un sujet peut appartenir à un ou plusieurs groupes. Une règle d'accès R à un objet Ob concerne une action, telle que par exemple lecture, écriture, exécution ou enregistrement, qui est autorisée ou interdite à un sujet Su ou à un groupe de sujet Gp sur un objet Ob. Par conséquent, une liste de contrôle d'accès ACL(Ob) est relative à des règles d'accès de sujets prédéterminés et/ou de groupes prédéterminés sur l'objet respectif Ob.

Selon l'invention, lors de la fabrication de la carte, ou avant la mise en service de la carte CA, c'est-à-dire avant la remise de celle-ci au propriétaire de la carte, des administrateurs des listes ACL contenues dans la carte sont définies à une étape initiale ET01. Chaque administrateur AD est défini par une clé d'administrateur respective KAD qui est associée à une ou plusieurs listes de contrôle d'accès ACL auxquelles l'administrateur AD a accès. Chaque liste de contrôle d'accès ACL est associée à une sous-liste d'administrateur constituée par les clés d'administrateur correspondantes KAD. Comme on le verra dans la suite, de préférence la liste de clés d'administrateur KAD est complétée par une liste de signature d'administrateur SGAD. Une signature est représentative de la liste de contrôle d'accès ACL signée par l'administrateur respectif selon l'algorithme de sécurité AS. Ainsi selon l'invention, les clés d'administrateur KAD et de préférence les signatures d'administrateur SGAD sont préalablement écrites dans la mémoire non volatile

MNV de la carte à puce CA en correspondance avec les listes de contrôle d'accès ACL.

Dans la figure 2 est également schématisée une entité d'administrateur externe à la carte CA sous la forme d'un serveur d'administrateur SAD relié à la carte à puce à travers un réseau de télécommunication RT et le terminal d'accueil TE. Le réseau de télécommunication RT désigne n'importe quel type de réseau de télécommunication, ou combinaison de réseaux, tel que réseau de radiotéléphonie, réseau téléphonique commuté, réseau numérique à intégration de service RNIS, réseau à haut débit de type ATM, réseau internet, réseau de transmission par paquets, etc.

Le serveur SAD est représentatif d'un administrateur ou bien de plusieurs administrateurs. D'autres administrateurs peuvent être situés au niveau d'autres serveurs distants (non représentés). L'administrateur AD est par exemple le distributeur de la carte à puce CA, ou un partenaire associé commercialement à ce distributeur, ou bien encore le développeur d'une ou plusieurs applications AP constituant des objets Ob implémentés dans la carte à puce CA. En variante, un administrateur possède lui-même une carte à puce qui est logée dans un lecteur additionnel du serveur SAD afin que le serveur SAD lise dans la carte à puce les références de l'administrateur, telles qu'un identificateur d'administrateur IAD et une clé d'administrateur KAD.

Comme montré schématiquement également à la figure 2, le terminal d'accueil TE est doté d'un clavier CL et d'un lecteur LE pour recevoir la carte à puce CA et se connecter à celle-ci par une liaison à contacts électriques LI selon cette réalisation. Le terminal d'accueil TE est par exemple un terminal de

mise en service de carte à puce, un terminal bancaire, ou un terminal point de vente, ou bien un terminal radiotéléphonique mobile dans lequel la carte à puce CA constitue un module d'identité d'abonné amovible SIM (Subscriber Identity Module) ou une carte à puce additionnelle lorsque le terminal mobile est doté d'un lecteur de carte additionnel.

Après l'étape initiale ET01, le procédé de gestion selon l'invention comprend de préférence une deuxième étape initiale ET02 au cours de laquelle des signatures d'administrateur SGAD sont déterminées. L'étape ET02 est également mise en oeuvre pour une liste ACL qui vient d'être modifiée ou introduite en mémoire MNV dans la carte CA. Chaque signature SGAD d'un administrateur SAD dépend de la clef KAD de l'administrateur et des données déterminées d'une liste de contrôle d'accès ACL à laquelle est associée la clé KAD. Les données déterminées de la liste de contrôle d'accès ACL dépendent essentiellement les caractéristiques de l'objet Ob et des sujets Su et/ou des groupes de sujet Gp ayant chacun au moins un droit d'accès à l'objet Ob, ainsi que le cas échéant des caractéristiques des droits d'accès. La liste ACL et la clé KAD sont appliquées à l'algorithme de sécurisation AS dont le résultat constitue la signature d'administrateur SGAD.

Le procédé de gestion montré à la figure 3 comprend principalement des étapes ET2 à ET14 déclenchées par une première étape ET1 au cours de laquelle le serveur d'administrateur SAD demande l'établissement d'un appel avec le terminal d'accueil TE contenant la carte à puce CA à travers le réseau de télécommunication RT, de manière à initier une

session de gestion de liste de contrôle d'accès avec la carte à puce CA.

Au début de cette session la carte CA tente d'authentifier le serveur d'administrateur SAD à l'étape ET2. L'authentification est classique et consiste essentiellement à transmettre un nombre aléatoire par la carte à puce CA au serveur SAD et à comparer dans la carte à puce CA les résultats de l'application de ce nombre aléatoire et d'une clé d'authentification pré-mémorisée dans la carte CA et le serveur SAD, effectuée à la fois dans la carte CA et le serveur SAD. Inversement, le serveur SAD authentifie la carte à puce CA. Selon une autre variante, l'authentification est mutuelle et comprend une authentification du serveur SAD par la carte CA et une authentification de la carte CA par le serveur SAD. Si l'authentification ou l'une des authentifications à l'étape ET2 donne des résultats différents dans le serveur SAD et la carte à puce CA, l'appel est rompu à une étape finale ET14.

En variante, le procédé de gestion ne comprend aucune authentification.

Lorsque l'authentification a réussi, le serveur d'administrateur SAD sélectionne une liste de contrôle d'accès ACL qu'il a en gestion localement dans une table de listes de contrôle d'accès, à l'étape suivante ET3, bien que l'administrateur ne peut gérer qu'une liste de contrôle d'accès ACL. Le serveur SAD signe ensuite la liste de contrôle d'accès sélectionnée ACL en appliquant les données déterminées de la liste ACL et la clé KAD du serveur d'administrateur SAD à l'algorithme de sécurité AS de manière à produire une signature d'administrateur SGAD à l'étape ET4.

En variante, au lieu de signer lui-même la liste de droits d'accès ACL et produire la signature d'administrateur SGAD, le serveur SAD reçoit cette signature SGAD transmise par une autre entité d'administrateur principal, tel qu'un serveur d'administrateur principal relié au réseau de télécommunication RT, après que le serveur d'administrateur principal ait authentifié le serveur SAD.

Puis la signature SGAD constituant la liste de contrôle d'accès sélectionnée ACL signée est transmise par le serveur SAD à la carte à puce CA à travers le réseau RT et le terminal TE sous la forme d'un message approprié à l'étape ET5. Ce message peut contenir d'autres données telles qu'un identificateur d'administrateur IAD qui désigne une table de listes de contrôle d'accès respective TACL dans la carte à puce CA. La table TACL contient des identificateurs de listes de contrôle d'accès auxquelles le serveur d'administrateur SAD a accès, et de préférence contient des signatures de ces listes de contrôle d'accès signées par le serveur d'administrateur SAD.

A l'étape suivante ET6, en réponse à la signature d'administrateur SGAD, le microprocesseur PR dans la carte à puce CA recherche une liste de contrôle d'accès qui est susceptible d'être signée par le serveur d'administrateur SAD. Cette recherche peut consister à déterminer toutes les signatures d'administrateur respectivement associées aux listes de contrôle d'accès que contient la carte à puce CA, puis à comparer les signatures déterminées avec la signature SGAD reçue par la carte CA.

Toutefois, comme cela a été indiqué à l'étape ET02, le processeur PR de la carte à puce CA a, de préférence, préalablement au moins à l'étape ET5,

déterminé les signatures SGAD correspondant à tous les administrateurs respectivement associés aux listes de contrôle d'accès ACL et les a écrites en mémoire EEPROM MNV. Le processeur PR ne compare alors la signature SGAD reçue à l'étape ET5 qu'avec les signatures préalablement déterminées et classées dans la table TACL. Si le processeur PR ne trouve aucune signature d'administrateur en mémoire MNV identique à la signature SGAD transmise par le serveur SAD, le processeur PR invite le terminal d'accueil TE à rompre la communication à l'étape ET14.

En variante, lorsque les identificateurs d'administrateur IAD sont prévus dans la mémoire MNV, le processeur PR ne compare la signature reçue SGAD qu'aux signatures contenues dans la table TACL désignée par l'identificateur reçu IAD et associée à la clé KAD, c'est-à-dire qu'aux signatures associées à des listes de contrôle d'accès auxquelles le serveur d'administrateur SAD a accès.

Ainsi après l'étape ET6, une liste de contrôle d'accès ACL correspondant à la signature d'administrateur reçue SGAD est trouvée afin de la traiter par le serveur SAD, comme indiqué à l'étape ET7. Bien que selon une variante simple, l'étape ET7 est suivie par une étape ET10 permettant l'accès du serveur d'administrateur SAD à la liste de contrôle d'accès ACL précédemment trouvée, l'invention prévoit des étapes intermédiaires ET8 et ET9 au cours desquelles un paramètre de durée de vie pdv de la liste de droits d'accès trouvée ACL est mis à jour et comparé à une limite maximale PDV.

Le paramètre pdv et la limite PDV sont écrits dans la mémoire MNV de la carte. La limite PDV exprime la durée de vie de la liste de contrôle

d'accès ACL trouvée à l'étape ET7 et est pré-mémorisée dans la mémoire MNV à l'étape initiale ET01, lors de la fabrication ou de la mise en service de la carte CA, ou lors d'une adjonction de la liste ACL, comme on le verra par la suite. A l'étape initiale ET01, le paramètre de durée de vie pdv est mis à zéro de manière à ce qu'il soit incrémenté chaque fois que l'étape ET8 est exécutée.

Le paramètre de durée de vie pdv peut être une durée cumulée de sessions d'utilisation de la carte à puce CA exprimée en heure et minute comme la limite PDV. Selon une deuxième variante, le paramètre pdv est une durée cumulée de temps absolu exprimée en date et heure, la limite PDV désignant alors une durée prédéterminée maximale ou une date de péremption de la liste déterminée ACL. La mise à jour de la durée peut être effectuée dans la carte CA en interrogeant un horodateur de confiance, par exemple inclus dans le terminal TE, ou dans le serveur d'administrateur SAD.

Selon d'autres variantes, le paramètre de durée de vie pdv est un nombre de sessions d'utilisation de la carte à puce CA, ou un nombre de sessions mettant en oeuvre la liste de droits d'accès trouvée ACL, la limite ACL étant un nombre maximal de sessions.

Selon encore une autre variante, le paramètre de durée de vie pdv est un nombre de commandes APDU reçues par la carte à puce CA, la limite PDV étant alors un nombre maximal de commandes.

Selon encore une autre variante, le paramètre de durée de vie est une valeur de synchronisation changée périodiquement dans les serveurs d'administrateur et transmise à la carte par tout serveur d'administrateur SAD dans chaque message qui contient la signature SGAD de la liste de droits

d'accès recherchée ACL, à l'étape ET5, la limite PDV étant au nombre maximal.

L'étape ET8 incrémente ainsi le paramètre de durée de vie selon sa nature, l'incrément étant notamment une durée ou une différence de date, ou une unité, ou un nombre de commandes.

Si à l'étape ET9 le paramètre de durée de vie pdv excède la limite PDV, le processeur PR efface la liste de contrôle d'accès ACL qui a été trouvée à l'étape ET7 et toutes les données associées à la liste ACL à l'étape ET13, et rompt la communication avec le serveur SAD à l'étape ET14. En variante, l'étape ET13 n'efface que partiellement la liste trouvée, par exemple en n'y effaçant que les droits d'accès positifs ou négatifs.

Si la durée de vie n'est pas encore atteinte à l'étape ET9, le serveur d'administrateur SAD est autorisé à accéder effectivement à la liste de contrôle d'accès ACL trouvée, à l'étape ET10. Le serveur SAD procède alors à une modification de la liste de contrôle d'accès trouvée ACL. Cette modification consiste par exemple à effacer totalement la liste de contrôle d'accès ACL dans la mémoire MNV, ou à modifier l'une des données dans la liste trouvée ACL, en particulier à supprimer ou à ajouter un sujet Su dans la liste de contrôle d'accès trouvée avec des droits d'accès correspondants R, ou bien à supprimer ou ajouter au moins un droit d'accès R relatif à un sujet Su inclus dans la liste trouvée. La modification peut également consister en l'adjonction d'une nouvelle clé d'administrateur à associer à la liste trouvée et incluse dans le message transmis à l'étape ET5.

Si à l'étape ET11, la liste de contrôle d'accès trouvée ACL n'a pas été modifiée ou a été effacée, le

procédé passe directement à la rupture de la communication à l'étape ET14. En revanche, si la liste de contrôle d'accès trouvée ACL a été modifiée par le serveur SAD, cette liste modifiée étant désignée par ACLm, le processeur PR détermine, à l'étape ET12, de nouvelles signatures d'administrateur SGADm résultant de l'application des données déterminées de la liste de contrôle d'accès modifiée ACLm et respectivement des clés d'administrateur KAD associées à la liste, à l'algorithme de sécurisation AS. Les signatures SGADm remplacent les signatures précédentes SGAD afin que lors d'une prochaine session de gestion de liste, le serveur d'administrateur SAD puisse accéder à la liste de contrôle ACLm ainsi modifiée dans la mémoire MNV de la carte CA.

Puis le procédé de gestion se termine par la rupture de la communication entre le serveur SAD et la carte CA à l'étape ET14.

Lorsqu'une liste de contrôle d'accès établie dans le serveur d'administrateur SAD est à ajouter dans la mémoire MNV de la carte à puce CA, les étapes ET1 à ET5 sont exécutées, le message transmis à l'étape ET5 contenant en outre la liste ACL à ajouter avec les clés d'administrateur KAD associées à la liste. Puis, à la place des étapes ET6 à ET13, le processeur PR détermine et mémorise les signatures SGAD de la liste reçue dans les tables de liste respectives TACL dans la carte CA. Pour chaque administrateur associé à la liste, la signature respective SGAD résulte de l'application des données déterminées de la liste et de la clé respective KAD reçues à l'algorithme de sécurisation AS. Le processeur PR compare les signatures déterminées à la

signature reçue, comme montré à une étape ET15 en traits pointillés à la figure 3. L'enregistrement de la liste reçue et des clés et signatures d'administrateur associées dans la mémoire MNV est validé à une étape ET16 lorsque l'une des signatures déterminées est identique à la signature reçue. Sinon, l'étape ET14 rompt la communication entre le serveur SAD et la carte CA.

Suivant une variante de la réalisation décrite ci-dessus, le serveur SAD est une entité déléguée par un autre serveur d'administrateur qui lui a transmis une information de droit de délégation IDR. Une information de droit de délégation IDR a été préalablement mémorisée dans la mémoire MNV de la carte à puce CA à l'étape initiale ET01, et est transmise dans le message contenant la signature d'administrateur SGAD à l'étape ET5. A l'étape ET6, la carte à puce CA autorise l'accès à la liste de contrôle d'accès ACL lorsqu'à la fois la signature SGAD est reconnue dans la table TACL associée à la clé KAD du serveur SAD et l'information de droit de délégation IDR est détectée en association avec la liste ACL reconnue dans la table TACL de la carte. Sinon la communication est rompue à l'étape ET14.

Bien que l'invention a été décrite en relation avec une carte à puce contenant des liste de contrôle d'accès associées respectivement à des signatures, la carte à puce peut contenir également des listes de contrôle d'accès non signées. Ainsi un serveur d'administrateur SAD peut décider d'effacer toutes les listes de contrôle d'accès chargées dans la carte à puce CA et associées à la clé KAD du serveur SAD,

en transmettant les signatures correspondantes à l'étape ET4.

Comme déjà dit, tout ce qui a été décrit ci-dessus pour des listes de contrôle d'accès dans la carte à puce CA, ou dans tout autre objet électronique portable tel qu'assistant ou organisateur électronique personnel, porte-monnaie électronique, jeton ou calculette, est applicable à une liste de droits d'accès faisant correspondre plusieurs sujets à un objet, comme une capacité.

2820848

REVENDICATIONS

1 - Procédé pour gérer des listes de droits d'accès (ACL) entre des sujets et des objets, mémorisées dans un moyen de traitement de données (CA) depuis une entité d'administrateur externe (SAD), caractérisé en ce qu'il comprend les étapes suivantes :

- initialement associer (ET01 ; ET15) des clés (KAD) d'entités d'administrateur (SAD) à des listes de droits d'accès (ACL) et fournir un algorithme de sécurisation (AS) dans le moyen de traitement de données (CA), et

- pour accéder à une liste de droits d'accès (ACL) depuis l'entité (SAD) :

signer (ET4) la liste de droits d'accès (ACL) dans l'entité en appliquant des données déterminées de la liste et la clé à l'algorithme de sécurisation (AS) afin de produire une signature (SGAD),

transmettre (ET5) la signature (SGAD) depuis l'entité au moyen de traitement de données, et

comparer (ET6) la signature (SGAD) reçue dans le moyen de traitement de données à des signatures déterminées en fonction des applications de données déterminées de listes de droits d'accès contenues dans le moyen de traitement de données et de clés respectivement associées à ces listes à l'algorithme (AS), et n'autoriser (ET10) l'accès de l'entité (SAD) à une liste de droits d'accès trouvée (ACL) qu'en correspondance avec une signature trouvée parmi les signatures déterminées dans le moyen de traitement de données et identique à la signature reçue.

2 - Procédé conforme à la revendication 1, selon lequel l'association des clés (KAD) aux listes de

droits d'accès (ACL) est préalablement effectuée (ET01) dans le moyen de traitement (CA) lors de la fabrication ou avant la mise en service du moyen de traitement de données (CA) (ET01).

3 - Procédé conforme à la revendication 1 ou 2, selon lequel l'association de clés (KAD) à une liste de droits d'accès (ACL) à ajouter dans le moyen de traitement de données (CA) est effectuée par transmission (ET5) de la liste avec les clés depuis l'entité (SAD) vers le moyen de traitement de données (CA), et détermination (ET15) de signatures (SGAD) de la liste reçue dans le moyen de traitement de données en appliquant les données déterminées de la liste reçue et des clés reçues à l'algorithme (AS), et validation (ET16) de l'enregistrement de la liste reçue dans le moyen de traitement de données lorsque l'une des signatures déterminées est identique à la signature reçue.

4 - Procédé conforme à l'une quelconque des revendications 1 à 3, selon lequel l'étape de signer (ET4) est remplacée par la réception dans l'entité (SAD), de ladite signature (SGAD) transmise par une autre entité.

5 - Procédé conforme à l'une quelconque des revendications 1 à 4, selon lequel une information de délégation (IDR) est transmise avec la signature (SGAD), et l'accès de l'entité (SAD) à la liste trouvée (ACL) n'est autorisé lorsqu'en outre, l'information de délégation est détectée en association avec la liste trouvée dans le moyen de traitement de données (CA).

6 - Procédé conforme à l'une quelconque des revendications 1 à 5, selon lequel les signatures à comparer à la signature reçue (SGAD) sont déterminées dans le moyen de traitement de données (CA) préalablement (ET02) à l'étape de transmettre (ET5).

7 - Procédé conforme à l'une quelconque des revendications 1 à 6, comprenant, avant d'autoriser l'accès de l'entité (ET10) à la liste de contrôle, une mise à jour (ET8) d'un paramètre de durée de vie (pdv) de la liste de droits d'accès trouvée afin d'effacer (ET13) la liste de droits d'accès trouvée (ACL) lorsque le paramètre de durée de vie mis à jour excède une limite maximale (PDV) et afin d'autoriser l'accès à la liste de droits d'accès trouvée à l'entité (SAD) lorsque le paramètre de durée de vie mis à jour est inférieur à la limite maximale.

8 - Procédé conforme à la revendication 7, selon lequel le paramètre de durée de vie (pdv) est une durée cumulée de sessions d'utilisation du moyen de traitement de données (CA) ou une durée cumulée de temps absolu.

9 - Procédé conforme à la revendication 7, selon lequel le paramètre de durée de vie (pdv) est un nombre de sessions d'utilisation du moyen de traitement de données (CA) , ou un nombre de sessions mettant en oeuvre la liste de droits d'accès trouvée (ACL).

10 - Procédé conforme à la revendication 7, selon lequel le paramètre de durée de vie (pdv) est un nombre de commandes reçues par le moyen de traitement de données (CA).

11 - Procédé conforme à la revendication 7, selon lequel le paramètre de durée de vie (pdv) est une valeur de synchronisation changée périodiquement dans des entités d'administrateur externes (SAD) et transmise (ET5) avec la signature (SGAD) de la liste de droits d'accès.

12 - Procédé conforme à l'une quelconque des revendications 1 à 11, selon lequel les signatures (SGADm) de la liste d'accès (ACLm) associées aux clés de cette liste sont de nouveau déterminées (ET12) dans le moyen de traitement de données (CA) si la liste de droit d'accès trouvée (ACL) a été modifiée par l'entité (SAD).

13 - Procédé conforme à l'une quelconque des revendications 1 à 12, selon lequel les données déterminées de la liste (ACL) qui sont appliquées à l'algorithme de sécurisation (AS) dépendent de caractéristiques d'au moins un sujet et/ou d'au moins un groupe de sujet et/ou d'au moins un objet et/ou d'au moins un droit d'accès d'un sujet à un objet relatif à la liste.

14 - Moyen de traitement de données (CA) mémorisant des listes de droits d'accès (ACL) gérées depuis au moins une entité d'administrateur externe (SAD), pour la mise en oeuvre du procédé conforme à l'une quelconque des revendications 1 à 13, caractérisé en ce qu'il comprend :

- un moyen (MNV) pour mémoriser des clés (KAD) d'entités d'administrateur (SAD) en association à des listes de droits d'accès (ACL),

- un moyen (MO) pour implémenter un algorithme de sécurisation (AS),

- un moyen (PR, MO) pour déterminer des signatures en fonction des applications de données déterminées des listes de droits d'accès et de clés respectivement associées à ces listes à l'algorithme (AS),

- un moyen (PR) pour comparer une signature reçue (SGAD) d'une liste de droits d'accès (ACL) qui résulte, dans l'entité, de l'application de données déterminées de la liste (ACL) et de la clé (KAD) de l'entité à l'algorithme (AS) et qui est transmise par l'entité, auxdites signatures déterminées, et

- un moyen (PR) pour autoriser l'accès de l'entité (SAD) à une liste de droits d'accès trouvée (ACL) qu'en correspondance avec une signature trouvée parmi les signatures déterminées et identique à la signature reçue.

15 - Moyen de traitement de données conforme à la revendication 14, comprenant un moyen (MNV) pour mémoriser un paramètre de durée de vie (pdv) et une limite maximale de durée (PDV) pour chaque liste de droits d'accès, et un moyen (PR) pour mettre à jour le paramètre de durée de la liste trouvée (ACL) afin d'effacer la liste de droits d'accès trouvée (ACL) lorsque le paramètre de durée de vie mis à jour excède la limite maximale (PDV) et afin d'autoriser l'accès à la liste de droits d'accès trouvée à l'entité (SAD) lorsque le paramètre de durée de vie mis à jour est inférieur à la limite maximale.

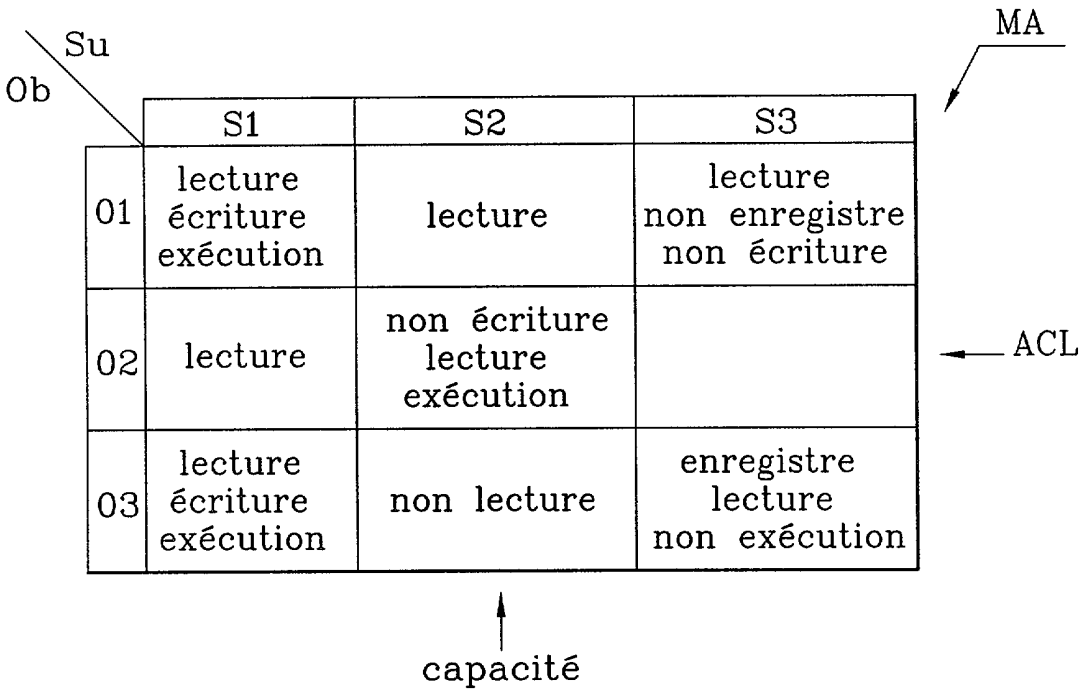

Su
Ob
MA
S1
S2
S3
01
lecture écriture exécution
lecture
lecture non enregistre non écriture
02
lecture
non écriture lecture exécution
ACL
03
lecture écriture exécution
non lecture
enregistre lecture non exécution
capacité

Fig. 1

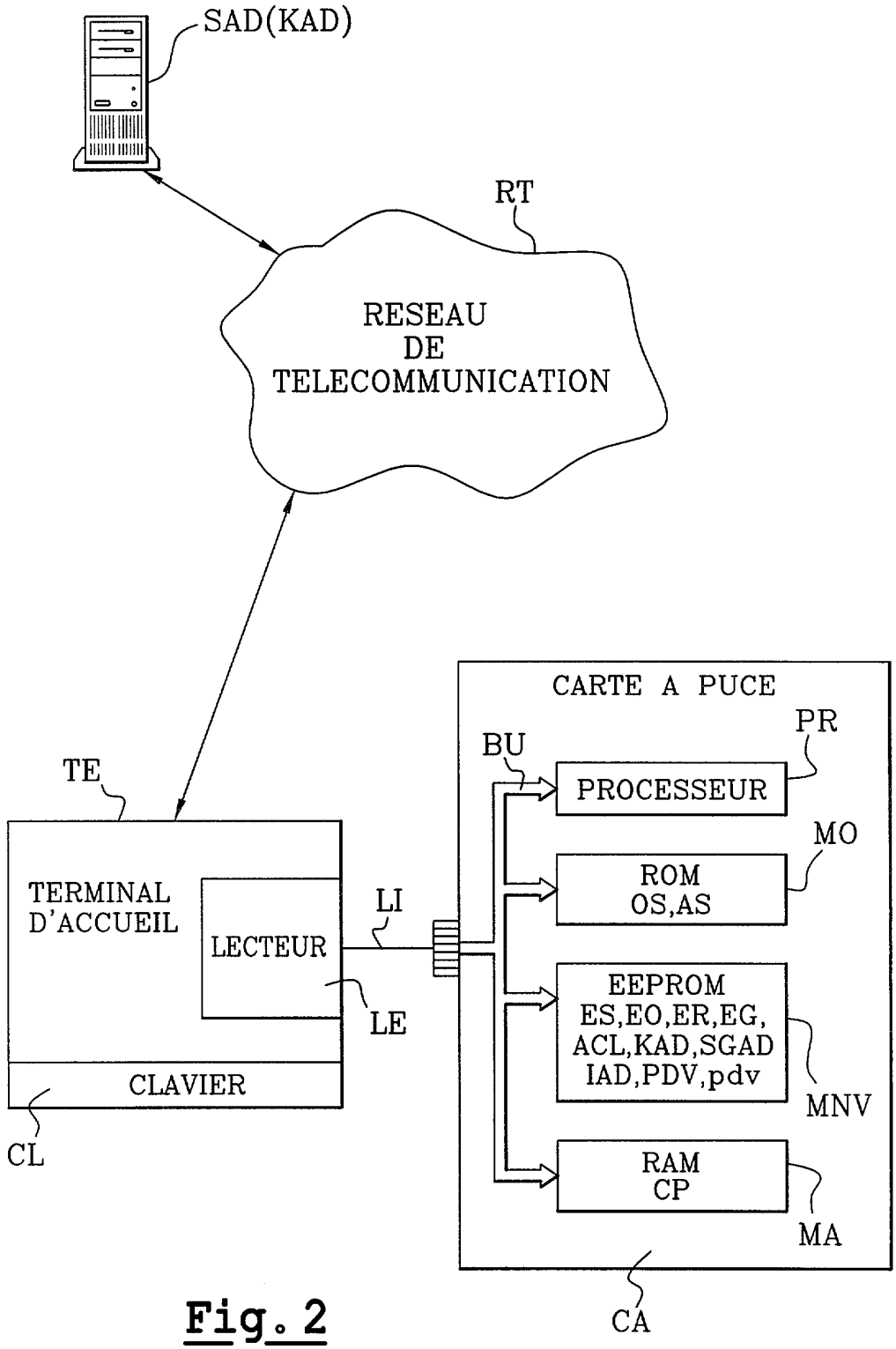
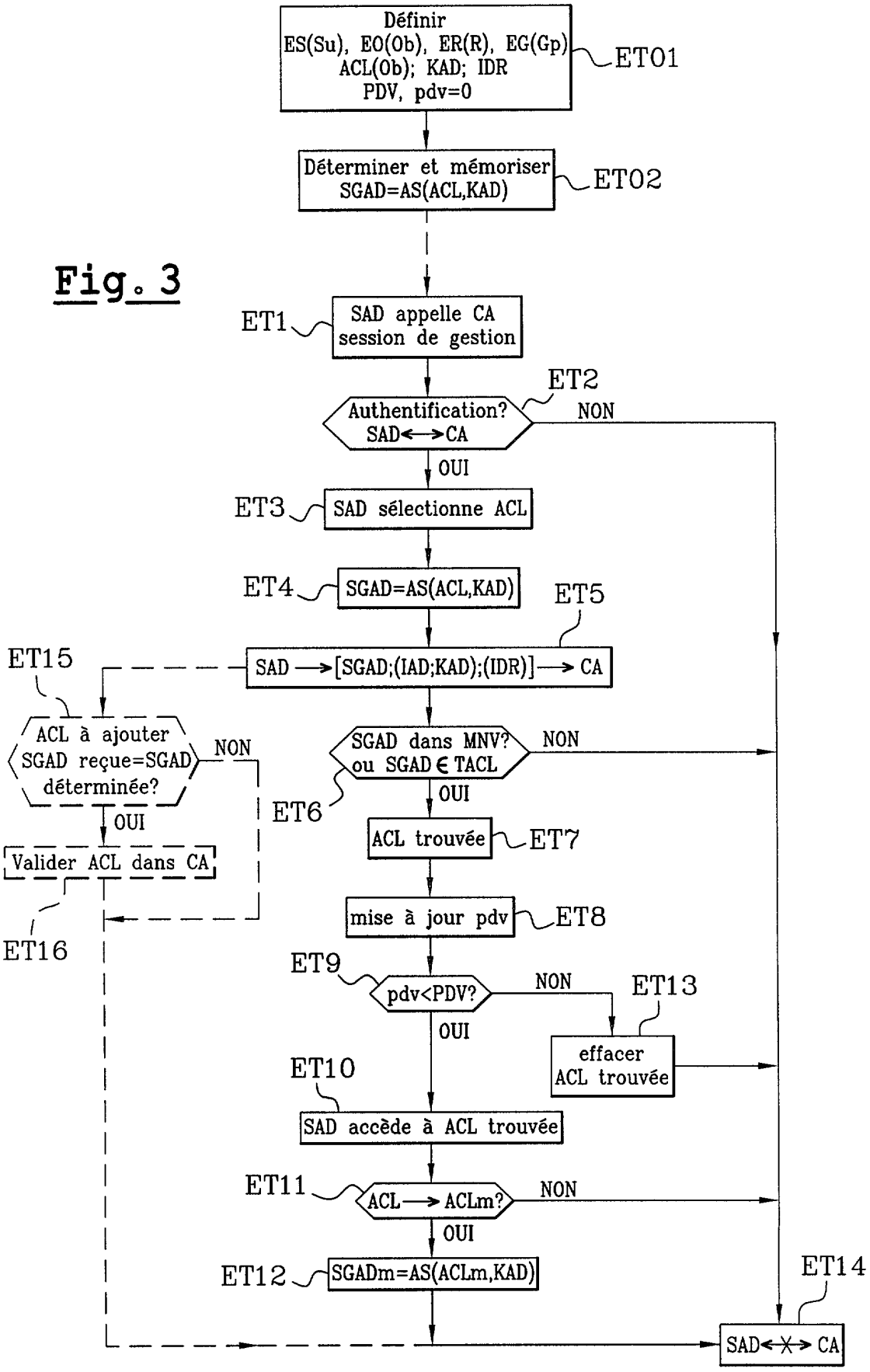

SAD(KAD)
RT
RESEAU
DE
TELECOMMUNICATION
CARTE A PUCE
PR
BU
PROCESSEUR
MO
ROM
OS,AS
TE
TERMINAL
D'ACCUEIL
LECTEUR
LI
LE
EEPROM
ES,EO,ER,EG,
ACL,KAD,SGAD
IAD,PDV,pdv
MNV
CLAVIER
CL
RAM
CP
MA
CA

Fig. 2

Fig. 3


Définir
ES(Su), EO(Ob), ER(R), EG(Gp)
ACL(Ob); KAD; IDR
PDV, pdv=0
ET01
Déterminer et mémoriser
SGAD=AS(ACL,KAD)
ET02
ET1
SAD appelle CA
session de gestion
ET2
Authentification?
SAD←→CA
NON
OUI
ET3
SAD sélectionne ACL
ET4
SGAD=AS(ACL,KAD)
ET5
SAD → [SGAD;(IAD;KAD);(IDR)] → CA
ET15
ACL à ajouter
SGAD reçue=SGAD
déterminée?
NON
OUI
Valider ACL dans CA
ET16
SGAD dans MNV?
ou SGAD ∈ TACL
NON
OUI
ET6
ACL trouvée
ET7
mise à jour pdv
ET8
ET9
pdv<PDV?
NON
OUI
ET13
effacer
ACL trouvée
ET10
SAD accède à ACL trouvée
ET11
ACL → ACLm?
NON
OUI
ET12
SGADm=AS(ACLm,KAD)
ET14
SAD←X→ CA

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2820848

N° d'enregistrement national

FA 598982
FR 0101962

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 5 224 163 A (GASSER MORRIE ET AL) 29 juin 1993 (1993-06-29) * colonne 12, ligne 43 - colonne 22, ligne 18 *	1-3,5,6, 13,14	G06F12/14 G06K19/073 H04L9/32
A	EP 0 813 132 A (IBM) 17 décembre 1997 (1997-12-17) * abrégé * * page 2, ligne 58 - page 5, ligne 23 * * figures 1,2 *	1-3,6, 13,14	
A	US 5 701 458 A (KELLS TIMOTHY ROGER ET AL) 23 décembre 1997 (1997-12-23)		
A	FR 2 791 159 A (BULL CP8) 22 septembre 2000 (2000-09-22)		
A	WO 99 65207 A (MICROSOFT CORP) 16 décembre 1999 (1999-12-16)		
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			G06F H04L

Date d'achèvement de la recherche	Examinateur
18 décembre 2001	Jacobs, P

CATÉGORIE DES DOCUMENTS CITÉS

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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0101962 FA 598982

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 18-12-2001
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5224163	A	29-06-1993	AUCUN		
EP 0813132	A	17-12-1997	US	5825877 A	20-10-1998
			EP	0813132 A2	17-12-1997
			JP	10083310 A	31-03-1998
			KR	267872 B1	16-10-2000
US 5701458	A	23-12-1997	AUCUN		
FR 2791159	A	22-09-2000	FR	2791159 A1	22-09-2000
			AU	3298200 A	04-10-2000
			CN	1300494 T	20-06-2001
			EP	1076972 A1	21-02-2001
			WO	0056030 A1	21-09-2000
WO 9965207	A	16-12-1999	US	6308273 B1	23-10-2001
			EP	1095493 A1	02-05-2001
			WO	9965207 A1	16-12-1999

EPO FORM P0465