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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
13 novembre 2008 (13.11.2008)

(10) Numéro de publication internationale
WO 2008/135692 A1

(51) Classification internationale des brevets :
G06F 21/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2008/050538

(22) Date de dépôt international : 27 mars 2008 (27.03.2008)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0754184 30 mars 2007 (30.03.2007) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GERMAIN, Florence** [FR/FR]; L'Eglise, F-38420 Saint Jean Le Vieux (FR). **ANNIC, Etienne** [FR/FR]; 59 avenue du Maréchal Leclerc, F-78120 Rambouillet (FR). **LOBRY, Olivier** [FR/FR]; 11 rue de Rungis, F-75013 Paris (FR).

(74) Mandataire : **FRANCE TELECOM/FTR & D/PIV/BREVETS**; MUSTAKI Daniel, 38-40 rue du Général Leclerc, F-92794 Issy Moulineaux Cédex 9 (FR).

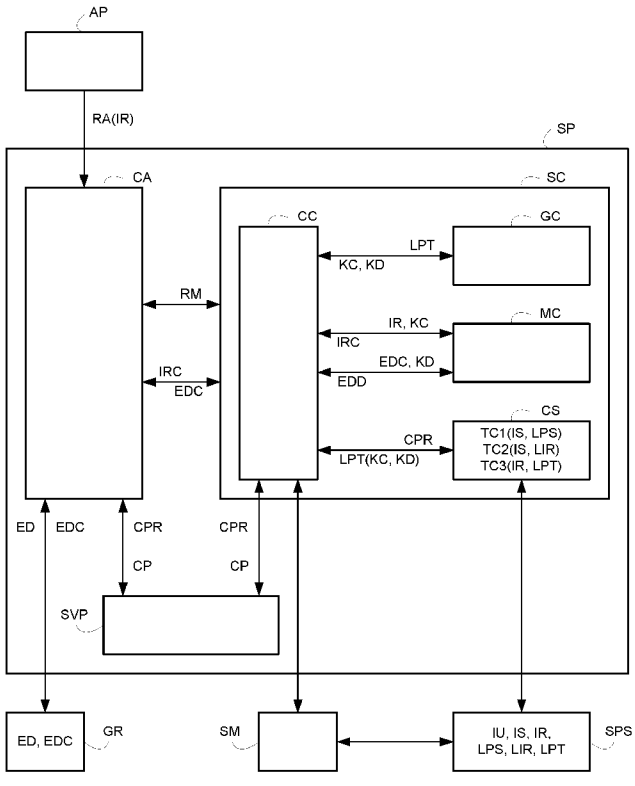
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK,

[Suite sur la page suivante]

(54) **Title:** ACCESS MANAGEMENT TO RESOURCES OF AN EXPLOITATION SYSTEM

(54) **Titre :** GESTION D'ACCES A DES RESSOURCES D'UN SYSTEME D'EXPLOITATION

FIG. 1



(57) Abstract: According to the invention, in order to manage the access to a terminal resource required by an execution unit (AP) of an application software run on said terminal, the execution unit (AP) being dedicated to a digital service and having outputted a system access (RA) including a resource identifier (IR) to a terminal exploitation system: said request (RA) is intercepted; the execution unit (AP) at the origin of the request is identified; at least one context parameter (CPR) concerning said identified execution unit (AP) is determined; the context parameter (CPR) is associated with the request (RA); the service is identified based on the context parameter (CPR); and identifiers of the resources associated with said identified service are determined. If the resource identifier (IR) contained in the request (RA) is one of the identifiers of the resources associated with the identified service, processing parameters (LPT) associated with this resource identifier (IR) are determined, and descriptive elements (ED) of the resource are processed based on said determined processing parameters (LPT) in order to make the resource accessible for the execution unit (AP).

(57) Abrégé : Pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution (AP) d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution (AP) étant dédiée à un service numérique et ayant émis une requête d'accès système (RA) incluant un identificateur de ressource (IR) à destination d'un système d'exploitation du terminal : ladite requête (RA) est interceptée; l'unité d'exécution (AP) à l'origine de ladite requête est identifiée;

[Suite sur la page suivante]

WO 2008/135692 A1

LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

au moins un paramètre de contexte (CPR) relatif à ladite unité d'exécution identifiée (AP) est déterminé; ledit paramètre de contexte (CPR) est associé à la requête (RA); ledit service est identifié en fonction du paramètre de contexte (CPR), et des identificateurs des ressources associées audit service identifié sont déterminés. Si ledit identificateur de ressource (IR) inclus dans la requête (RA) est l'un desdits identificateurs des ressources associées au service identifié, des paramètres de traitement (LPT) associés à cet identificateur de ressource (IR) sont déterminés, et des éléments descriptifs (ED) de la ressource sont traités en fonction desdits paramètres de traitement déterminés (LPT), afin de rendre la ressource accessible à l'unité d'exécution (AP).

Gestion d'accès à des ressources d'un système d'exploitation

La présente invention concerne une gestion d'accès à des ressources d'un système d'exploitation d'un terminal par une application dédiée à un service numérique.

Un service numérique est offert par un fournisseur de service à un utilisateur pour que ce dernier accède à un ensemble de données dans le strict respect des règles d'un modèle économique. A un couple données-modèle économique définissant un service est associée une liste d'ayants-droit, c'est-à-dire de personnes physiques ou morales qui ont acquis une licence d'usage et qui sont autorisées de ce fait à consommer ledit service et les données associées dans le cadre du modèle économique du service.

Un modèle économique définit un contrat commercial pour la consommation d'un service numérique, caractérisé par exemple par une tarification du service et des règles d'usage du service. Suite à l'inexécution d'une règle stipulée par le contrat, l'usage du service est réputé illicite.

Les règles d'usage imposées par un modèle économique sur des données sont typiquement mises en œuvre sous la forme d'une séquence d'instructions, appelée processus de gestion de droits numériques DRM ("Digital Rights Management" en anglais), exécutée à la demande d'un utilisateur ayant acquis une licence d'utilisation des données dans le cadre du modèle économique prévu pour ces données.

L'accès aux données d'un service numérique est réservé à des applications spécifiques, prévues au titre du modèle économique dudit service numérique.

Une "application" est classiquement définie comme une unité d'exécution d'un programme exécutable par un terminal. Un même programme peut être exécuté plusieurs fois de manière à ce que différentes applications requises par l'exécution du programme soient respectivement dédiées à des services numériques différents. Par exemple, un lecteur de média peut être exécuté une première fois pour lire une seule fois un fichier vidéo selon une visualisation à la demande, et une deuxième fois pour lire un autre fichier vidéo au moyen d'une licence accordant un nombre prédéterminé de visualisations de cet autre fichier vidéo.

Une application est dite "dédiée à un service numérique" associé à un couple données-modèle économique lorsque son exécution est destinée à être lancée sur les données dudit service numérique.

L'exécution d'une application dans un terminal requiert l'accès à des ressources du système d'exploitation du terminal, appelées plus simplement ressources système. Une ressource système désigne un élément matériel ou logiciel d'un terminal, accessible par le système d'exploitation. A titre d'exemples non limitatifs, une ressource système peut être un périphérique tel qu'un clavier, un écran, un haut-parleur, ou bien une batterie, une mémoire, un processeur, une interface réseau, ou bien encore un logiciel, un gestionnaire de fichier.

Dans un système d'exploitation, les ressources système sont représentées de différentes manières et ont chacune leur propre mode d'accès. De manière générale, on considère que le système d'exploitation

contient des éléments descriptifs pour chaque ressource système, ces derniers fournissant des instructions ou des indications interprétables par une application pour accéder à la ressource système. Des éléments descriptifs ont souvent la forme d'un fichier de données, tel qu'un "pseudo-fichier" dans les systèmes d'exploitation Unix pour l'accès à certaines ressources système telles que le clavier. Un élément descriptif peut être tout simplement un pointeur vers une mémoire, par exemple pour désigner une plage d'adresses d'une mémoire à dédier à une certaine ressource telle qu'une mémoire graphique.

Un système d'exploitation offre en particulier des fonctions de base d'un terminal informatique, comme la gestion de la mémoire, l'accès aux différents périphériques ou la gestion de l'exécution des processus sur le processeur. Les systèmes d'exploitation actuels mettent en œuvre une politique "centrée utilisateur" pour la gestion des droits d'accès aux ressources système : à un utilisateur donné sont attribués des droits lui donnant accès à plus ou moins de ressources du système d'exploitation.

Certains systèmes d'exploitation sont mono-utilisateur, c'est-à-dire qu'un seul utilisateur peut utiliser un terminal informatique à un moment donné. D'autres systèmes d'exploitation sont multi-utilisateur, c'est-à-dire que plusieurs utilisateurs peuvent utiliser un même terminal informatique simultanément. Dans ce dernier cas, un profil d'utilisateur confère à chaque utilisateur des droits d'accès à certaines ressources système. Un seul utilisateur, souvent appelé "administrateur", a accès à la totalité des ressources système tandis que les

autres utilisateurs n'ont accès qu'à un nombre limité de ressources.

Ces systèmes d'exploitation à profils permettent de mutualiser sur un même terminal informatique le travail de plusieurs utilisateurs tout en contrôlant les risques d'éventuelles ingérences pouvant être provoquées, intentionnellement ou non, par l'un des utilisateurs sur les données des autres utilisateurs. Comme pour les systèmes mono-utilisateur, les systèmes d'exploitation à profils mettent en œuvre une politique "centrée utilisateur" pour la gestion des droits d'accès aux ressources système.

Jusqu'à présent, les systèmes d'exploitation ont été conçus pour sécuriser les données et les accès à des ressources système en fonction de l'utilisateur. Cette approche a trouvé sa limite avec l'avènement d'internet qui a mis en évidence l'incapacité des systèmes d'exploitation à garantir la sécurité des échanges avec d'autres terminaux accessibles via un réseau. Ainsi, avec le développement des échanges de données par réseau, un système d'exploitation "centré utilisateur" ne peut pas gérer à la fois un utilisateur attitré et des utilisateurs de terminaux du réseau. Une telle gestion nécessiterait un re-développement complet des systèmes d'exploitation existants. Mais pour des raisons économiques, les développeurs de systèmes d'exploitation se sont limités à des adaptations légères.

En conséquence, il est très courant sur internet qu'un terminal soit "infecté" par un logiciel téléchargé à l'initiative d'un autre équipement du réseau et exécuté sur ledit terminal pour le compte et à l'insu de l'utilisateur. La politique de gestion des droits "centrée utilisateur" ne convient donc pas

aux usages présents et futurs d'un terminal informatique accédant à au moins un réseau de communication.

Par ailleurs, dans les systèmes d'exploitation "centrés utilisateur", un service exécuté pour le compte d'un utilisateur hérite des droits de l'utilisateur. Par exemple, un service exécuté pour le compte d'un utilisateur de type administrateur a tous les droits, même le droit de détruire le système d'exploitation lui-même.

Un système d'exploitation "centré utilisateur" traite tous les services exécutés par un même utilisateur avec les mêmes droits. Par exemple, un service de navigation sur internet et un service sécurisé de paiement par carte bancaire peuvent être exécutés tous deux pour le compte d'un utilisateur donné sur un terminal disposant d'un accès "sans contact" à un réseau bancaire et d'un accès sans fil à internet. L'usage du service de paiement par carte impose le recours exclusif au réseau bancaire, et exclut a priori l'accès à internet. Le système d'exploitation "centré utilisateur" ne contrôle pas le type d'accès utilisé par le service de paiement. Il est alors possible d'utiliser l'accès à internet pour le service de paiement et ainsi de divulguer des données confidentielles sans interdiction par le système d'exploitation. De même, un quelconque service sur internet peut interférer avec le service de paiement pour mettre des données bancaires confidentielles à disposition sur le réseau internet ou bien pratiquer des opérations bancaires illégales. En effet, pour le système d'exploitation, cette pratique est normale puisqu'elle est conforme aux droits de l'utilisateur. Or pour le fournisseur du

service de paiement, cette pratique peut engendrer des catastrophes économiques.

Dans un autre exemple, un service malveillant est téléchargé dans un terminal informatique depuis un réseau. Lors de l'exécution du service sur le terminal, le service hérite des droits de l'utilisateur, et donc notamment des droits d'accès aux données de l'utilisateur. Rien n'empêche alors le service de collecter les données de l'utilisateur et de les transmettre sur le réseau à l'insu de l'utilisateur. De même, pour le système d'exploitation, cette pratique apparaît comme tout à fait normale puisqu'elle est conforme aux droits de l'utilisateur.

Des services de commerce électronique recourant au paiement en ligne et/ou à la consultation de comptes, sont mis en œuvre sur un terminal aux risques et périls de l'utilisateur. Bien que certains services utilisent des outils performants, tels que le protocole de transfert hypertexte sécurisé HTTPS ("HyperText Transfer Protocol Secured" en anglais), pour protéger leurs échanges, il suffit à un service malveillant exécuté sur le terminal de copier des informations provenant de l'écran, du clavier ou voire directement de la mémoire du terminal pour détourner ces services de commerce et rendre ainsi possible des malversations, sans que l'utilisateur n'ait conscience du piratage.

On remarque d'après les exemples précédents que les systèmes d'exploitation "centrés utilisateur" délèguent la responsabilité du bon fonctionnement du terminal aux services eux-mêmes. Si le service est correctement conçu, aucune action malveillante n'aura lieu et le terminal fonctionnera correctement. Par contre, si le service est mal conçu ou malveillant,

le service endommagera les données du terminal et/ou créera des dysfonctionnements à hauteur de ce qu'autorisent les droits de l'utilisateur. Or pour le système d'exploitation, toutes ces actions ont eu lieu conformément aux droits de l'utilisateur.

De ce qui précède, il résulte que les systèmes d'exploitation "centrés utilisateur" s'appuient, pour leur politique de sécurité, sur l'utilisateur. Si ce dernier utilise deux services, par exemple la navigation sur internet et un service de carte bancaire, les services ont accès aux droits de l'utilisateur et peuvent interférer de façon maligne sans que le système d'exploitation ne décèle un dysfonctionnement. Aucun mécanisme au niveau du système d'exploitation ne contrôle l'accès individuel d'un service aux ressources système.

Il existe donc un besoin de définir et garantir une restriction d'accès aux ressources système pour chaque service exécuté sur un système d'exploitation, et plus particulièrement d'autoriser chaque service à accéder aux seules ressources système auxquelles le service a droit.

Pour remédier aux inconvénients évoqués ci-dessus, l'invention propose un procédé pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution étant dédiée à un service numérique et ayant émis une requête d'accès système incluant un identificateur de ressource à destination d'un système d'exploitation du terminal. Ledit procédé est remarquable en ce qu'il comprend les étapes de :

après interception de ladite requête, identifier l'unité d'exécution à l'origine de ladite requête,

déterminer au moins un paramètre de contexte relatif à ladite unité d'exécution identifiée, et associer à la requête ledit paramètre de contexte,

identifier ledit service en fonction du paramètre de contexte,

déterminer des identificateurs des ressources associées audit service identifié, et

si ledit identificateur de ressource inclus dans la requête est l'un desdits identificateurs des ressources associées au service identifié, déterminer des paramètres de traitement associés à cet identificateur de ressource, et traiter, en fonction desdits paramètres de traitement déterminés, des éléments descriptifs de la ressource, afin de rendre la ressource accessible à l'unité d'exécution.

L'invention autorise à chaque service exécuté sur un terminal informatique un accès "sur mesure" à tout ou partie des ressources du système d'exploitation. Les services n'ont donc pas accès aux ressources système qui leur sont interdites. En contrôlant l'accès aux éléments descriptifs d'une ressource système, l'invention assure un contrôle d'accès à la ressource système elle-même.

Avantageusement, chaque service dispose d'un "profil" qui lui est propre et qui comprend l'ensemble des ressources système auquel il a le droit d'accéder. Un "profil service" d'un système d'exploitation se comporte comme un système d'exploitation autonome. Vu du service, le système d'exploitation est perçu comme offrant exactement et uniquement les accès aux ressources système auxquelles le service a le droit d'accéder. La politique de gestion des droits selon l'invention est donc "centrée service" afin de protéger l'accès aux

ressources système en fonction du service et non plus en fonction de l'utilisateur.

Sur un même terminal informatique, un tel système d'exploitation "centré service" est capable de gérer l'exécution de plusieurs services simultanément, chaque service disposant individuellement de ses propres droits d'accès aux ressources système.

L'invention a l'avantage d'offrir une solution de confinement pour les services en protégeant chaque service contre ses propres dysfonctionnements ou les malveillances d'autres services. Par exemple selon l'invention, un service de paiement a un droit d'accès exclusif à une ressource "réseau sans contact". Le système d'exploitation protège le service d'interactions avec des services pernicieux qui tenteraient d'utiliser l'accès à la ressource "réseau sans contact" pour intercepter des données bancaires, alors qu'ils ne possèdent pas les droits d'accès à cette ressource. De la même façon, le système d'exploitation prémunit le service contre les conséquences d'un éventuel dysfonctionnement du service en interdisant à ce dernier l'accès au réseau internet et donc toute transmission des données bancaires à travers le réseau internet.

Avantageusement, des ressources peuvent être octroyées exclusivement à un service selon l'invention. Le service est exécuté sur un terminal de manière autonome et indépendante des autres services pouvant être exécutés sur le même terminal. Ce service est entièrement confiné par rapport aux autres services et il est totalement protégé de leurs comportements.

En corollaire, du fait que l'invention permet de contrôler l'accès des services aux ressources

système, on peut empêcher le piratage de ressources système sensibles, par exemple en refusant systématiquement toute recopie d'une séquence de touches composée sur un clavier pour le compte d'un service "officiel", c'est à dire un service légitimement enregistré sur le terminal, tel qu'un service bancaire. L'accès contrôlé à des ressources système selon l'invention garantit également le bon fonctionnement du terminal, par exemple en interdisant tout simplement aux services l'accès à des ressources système sensibles comme la ressource "batterie".

Par ailleurs, puisque chaque service est installé sur un terminal en étant restreint vis-à-vis de l'utilisation de ressources système sensibles, il est par exemple impossible à un service malveillant qui ne dispose pas des droits d'accès à ces ressources système de détourner les informations bancaires confidentielles d'un service de paiement même en cas de dysfonctionnement de ce dernier.

L'invention offre en outre une grande souplesse de gestion des droits en prévoyant la mise à jour dynamique des ressources système autorisées pour chaque service. La modification des droits d'un service sur le système d'exploitation conduit immédiatement à la prise en compte des nouveaux droits d'accès aux ressources système allouées ou retirées au service. En particulier, il n'est pas nécessaire de relancer le système d'exploitation pour que cette prise en compte soit effective. Comme expliqué en détail ci-dessous en relation avec les paramètres de traitement et des identificateurs de service, la même souplesse est conférée aux modalités de protection des ressources et aux modalités

d'identification et d'authentification des services, en prévoyant leur mise à jour dynamique.

Le contexte d'usage de l'invention est celui d'un terminal informatique susceptible d'exécuter au moins un service. L'interdiction à des services de s'installer sur le terminal sans autorisation, ou du moins en contrôlant l'accès aux ressources, réduit considérablement les risques de piratage du terminal suite à l'installation automatique d'un service, par exemple lors d'une navigation sur un site internet. Ainsi, l'invention permet aux terminaux d'accéder à des réseaux sans risque de piratage, consistant par exemple à installer un service à l'insu de l'utilisateur. Par conséquent, si des services malveillants n'ont plus la possibilité de détourner des données associées à un modèle économique, alors les modèles économiques ne peuvent plus être détournés de leurs objectifs commerciaux.

Selon d'autres caractéristiques de l'invention, les éléments descriptifs de la ressource peuvent ne pas être chiffrés et donc être interprétables par l'unité d'exécution sans recourir aux paramètres de traitement, ou bien les éléments descriptifs de la ressource peuvent être chiffrés et interprétables par l'unité d'exécution après un déchiffrement des éléments descriptifs chiffrés en fonction des paramètres de traitement.

Les paramètres de traitement sont spécifiques à une ressource système et permettent de déchiffrer les éléments descriptifs de la ressource lorsque ces derniers sont chiffrés. Dans tous les cas, les paramètres de traitement rendent accessibles en clair les éléments descriptifs à l'unité d'exécution pour que cette dernière accède à la ressource.

Selon une autre caractéristique de l'invention, des paramètres de service peuvent être associés au service, et le service est identifié si tous les paramètres de service associés au service et seulement audit service sont inclus dans un ensemble de paramètres de contexte relatifs à l'unité d'exécution identifiée et associés à la requête.

Les paramètres de service permettent d'identifier le service de manière unique et non ambiguë par rapport à d'autres services numériques. Cette identification exacte garantit en outre que l'unité d'exécution requérant une ressource du terminal est "officielle".

L'invention concerne également un système pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution étant dédiée à un service numérique et ayant émis une requête d'accès système incluant un identificateur de ressource à destination d'un système d'exploitation du terminal. Ledit système est remarquable en ce qu'il comprend :

un moyen pour intercepter ladite requête et pour identifier l'unité d'exécution à l'origine de ladite requête,

un moyen pour déterminer au moins un paramètre de contexte relatif à ladite unité d'exécution identifiée,

un moyen pour associer à la requête ledit paramètre de contexte,

un moyen pour identifier ledit service en fonction du paramètre de contexte,

un moyen pour déterminer des identificateurs des ressources associées audit service identifié,

un moyen pour déterminer des paramètres de traitement associés à cet identificateur de ressource si ledit identificateur de ressource inclus dans la requête est l'un desdits identificateurs des ressources associées au service identifié, et

un moyen pour traiter, en fonction desdits paramètres de traitement déterminés, des éléments descriptifs de la ressource, afin de rendre la ressource accessible à l'unité d'exécution.

Avantageusement, le système de protection selon l'invention intercepte systématiquement tout appel à une ressource du terminal par une unité d'exécution afin d'assurer une protection des accès à la ressource. Le système de protection garantit que l'accès à une ressource est obtenu dans le contexte du modèle économique associé au service, et par un ayant-droit utilisant une unité d'exécution autorisée à accéder à la ressource.

Par ailleurs, le système d'exploitation est rendu plus fiable par l'invention puisque, même si un utilisateur de type administrateur possédant tous les droits exécute un service, ce service ne possède que ses propres droits d'accès aux ressources. Un tel service ne peut donc pas endommager le fonctionnement du système d'exploitation et rendre indisponible le terminal. Une indisponibilité du terminal implique une perte de chiffre d'affaires pour le fournisseur du service puisque le client ne peut plus consommer de services pendant que le terminal ne fonctionne plus. Par exemple, si un service exécuté par un utilisateur de type administrateur a uniquement le droit d'utiliser la mémoire, l'écran et le clavier du

terminal, le service ne pourra pas accéder à la ressource système "batterie" afin d'éteindre le terminal par exemple.

La fiabilité accrue du terminal renforce l'image de marque et de sérieux du fournisseur de service, par conséquent renforce la confiance du client par rapport au fournisseur, et consolide donc indirectement la capacité commerciale du fournisseur.

Selon une autre caractéristique de l'invention, le moyen pour identifier le service peut contenir une première table mettant en correspondance des identificateurs de service et des listes de paramètres de service, une deuxième table mettant en correspondance les mêmes identificateurs de service et des listes d'identificateurs de ressource, et une troisième table mettant en correspondance des identificateurs de ressource et des listes de paramètres de traitement, ces tables de correspondance étant actualisées par au moins un moyen serveur en fonction des services numériques auxquels l'utilisateur du terminal est abonné.

Les tables de correspondance permettent une identification exacte du service numérique relatif à l'application exécutée dans le terminal, et sont actualisées par un moyen serveur externe au terminal pour prendre en compte tout changement éventuel relatif aux services numériques auxquels l'utilisateur du terminal est abonné. En particulier, les tables de correspondance remédient à l'inconvénient qu'aucune entité officielle dans l'état de la technique ne gère l'ensemble des services numériques existants, les services n'ayant pas de caractéristiques propres pour être distingués les uns des autres.

L'invention se rapporte également à un programme d'ordinateur apte à être mis en œuvre dans un système pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution étant dédiée à un service numérique et ayant émis une requête d'accès système incluant un identificateur de ressource à destination d'un système d'exploitation du terminal, ledit programme comprenant des instructions qui, lorsque le programme est exécuté dans ledit système, réalisent les étapes selon le procédé de l'invention.

L'invention se rapporte enfin à un support d'enregistrement lisible par un système pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution étant dédiée à un service numérique et ayant émis une requête d'accès système incluant un identificateur de ressource à destination d'un système d'exploitation du terminal, ledit support contenant un programme d'ordinateur comportant des instructions pour l'exécution des étapes selon le procédé de l'invention.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations de l'invention données à titre d'exemples non limitatifs, en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un bloc-diagramme schématique d'un système de protection selon l'invention pour gérer un accès aux ressources d'un terminal ; et

- la figure 2 est l'algorithme d'un procédé de gestion d'accès aux ressources d'un terminal selon l'invention mis en œuvre dans le système de protection.

En référence à la figure 1, le système de protection SP selon l'invention est inclus dans un terminal informatique capable de gérer des données numériques.

Le terminal informatique peut être de tout type et peut gérer tout type de données. Par exemple, le terminal est un ordinateur personnel, un terminal radio mobile, un terminal bancaire, un serveur applicatif ou encore une caméra de surveillance. Le terminal dispose d'au moins une ressource système et peut gérer au moins un service.

Le système de protection SP comprend un contrôleur d'accès CA, un système de chiffrement SC et au moins un serveur de paramètres SVP. Le système de chiffrement SC comprend un contrôleur de chiffrement CC, un générateur de clé GC, un module de chiffrement MC et un contrôleur de service CS. Le serveur de paramètres SVP communique directement avec le contrôleur d'accès CA et/ou le contrôleur de chiffrement CC. Les communications entre les différentes entités comprises dans le système de protection sont sécurisées, de manière à ce qu'aucun échange d'information ne puisse être intercepté pendant une communication entre deux de ces entités.

Le contrôleur d'accès CA contrôle l'accès à des ressources système qui sont gérées à travers le système d'exploitation du terminal par un

gestionnaire de ressources GR. Comme décrit précédemment, les ressources système sont représentées de différentes manières et ont chacune leur propre mode d'accès. Le gestionnaire de ressources GR contient des éléments descriptifs ED pour chaque ressource système qui sont interprétables par une application pour accéder à la ressource système. Par exemple, des éléments descriptifs sont réunis dans un fichier de données dans un gestionnaire de fichiers accessible seulement par le gestionnaire de ressources GR.

Le serveur de paramètres SVP gère notamment des informations nécessaires au système de protection selon l'invention, telles que des valeurs pour les paramètres requis par le contrôleur de service CS et le générateur de clé GC.

Le contrôleur de service CS est apte à communiquer avec au moins un serveur de protection de service SPS, qui est par exemple localisé dans le réseau du fournisseur de service dispensant un service auquel est abonné l'utilisateur du terminal. Par souci de simplicité, on ne fera référence ci-dessous qu'à un seul serveur SPS, mais il est tout à fait possible dans le cadre de l'invention de prévoir plusieurs SPS ayant chacun les fonctionnalités décrites ci-dessous, de façon à ce que chaque fournisseur de service héberge au plus un serveur SPS. Le serveur de protection de service SPS est géré par exemple par le fournisseur de service lui-même ou par un tiers de confiance.

Les communications entre le contrôleur de service CS et le serveur de protection de service SPS sont également sécurisées, en utilisant par exemple le protocole d'accès entre objets distants SOAP

("Simple Object Access Protocol" en anglais) encapsulé dans le protocole de transfert sécurisé HTTPS.

Le serveur de protection de service SPS gère des listes de paramètres de service LPS associées à des services numériques de manière à ce que des identificateurs de service IS soient associés chacun à une et une seule liste de paramètres de service LPS. Une liste de paramètres de service LPS caractérise et identifie de manière unique et non ambiguë le service numérique correspondant parmi d'autres services. Chaque identificateur de service IS est en outre associé à un ou plusieurs identificateurs de ressource IR. Chaque identificateur de ressource IR est associé à une liste de paramètres de chiffrement/déchiffrement, appelée liste de paramètres de traitement LPT.

Par ailleurs, des identificateurs d'utilisateur IU peuvent être associés individuellement à au moins un identificateur de service IS. Un identificateur d'utilisateur IU est défini à partir de paramètres d'utilisateur qui caractérisent de manière non ambiguë l'utilisateur du service numérique. Les paramètres d'utilisateur incluent par exemple un identificateur d'un groupe d'utilisateurs et/ou un identificateur du terminal. Les paramètres d'utilisateur sont adaptés à chaque besoin commercial. Par exemple, un abonné n'aura pas les mêmes services en utilisant un téléviseur ou un terminal mobile. Ainsi, selon le contexte d'utilisation, des ressources système différentes seront accessibles pour un même service selon l'utilisation du téléviseur ou du terminal mobile, puisqu'il s'agit de deux identificateurs d'utilisateur différents bien que ces derniers

fassent référence à un seul et même utilisateur abonné. La notion d'utilisateur est donc très générale et englobe par exemple des individus, des sociétés, des machines ou bien des individus utilisant une machine déterminée à un endroit donné.

Le contrôleur de service CS contient en particulier des première, deuxième et troisième tables de correspondance TC1, TC2 et TC3. La première table TC1 met en correspondance des identificateurs de service IS et des listes de paramètres de service LPS, et la deuxième table TC2 met en correspondance les mêmes identificateurs de service IS et des listes d'identificateurs de ressource LIR respectives. La troisième table TC3 met en correspondance les identificateurs de ressource IR et des listes de paramètres de traitement LPT.

Une liste de paramètres de service LPS contient un ou plusieurs paramètres, tandis qu'une liste de paramètres de traitement LPT peut ne contenir aucun paramètre. Ces tables de correspondance TC1, TC2 et TC3 sont fournies ou actualisées par le serveur de protection de service SPS en fonction de l'identificateur IU de l'utilisateur du terminal.

Le terminal informatique comprend en outre des mémoires qui regroupent une ou plusieurs mémoires volatiles et une ou plusieurs mémoires persistantes dont l'accès à travers le système d'exploitation depuis le gestionnaire de ressource GR est garanti par le contrôleur d'accès CA du système de protection.

Le système d'exploitation du terminal exécute des applications AP et gère le partage des ressources du terminal entre les applications via le gestionnaire de ressources GR.

Une application AP qui est exécutée par le système d'exploitation du terminal et associée à un service numérique peut demander l'accès à l'une quelconque des ressources du système d'exploitation du terminal.

En particulier, le système de protection SP peut être mis en œuvre dans un composant électronique de type microcontrôleur, circuit à microprocesseur ou carte à puce, afin que le système ne soit pas piraté, espionné ou modifié. Ce mode de réalisation est particulièrement intéressant lorsque le composant électronique inclut, en plus du système de protection SP, une mémoire volatile, une mémoire persistante, stockant par exemple les codes applicatifs permettant au système d'exploitation de s'exécuter, et un processeur dans lequel s'exécute le code source du système de protection. En effet, une faiblesse du système de protection est que son exécution réclame que son code source soit écrit en "clair". Si le code source est écrit en mémoire volatile, il est possible de copier le code source de la mémoire, d'en comprendre le fonctionnement et de le détourner de ce fonctionnement. En revanche, si le code source du système de protection est exécuté au sein du composant électronique, il est beaucoup plus difficile de le pirater.

La mémoire persistante du composant électronique contient des applications critiques comme, par exemple, un système d'exploitation certifié mettant en œuvre le contrôleur d'accès, ou un navigateur certifié.

Quand un service doit être exécuté sur le terminal, le service est alors exécuté au moyen du système d'exploitation en utilisant le système de protection SP. Les demandes d'accès à des ressources

système émanant des services sont traitées par le système de protection qui vérifie les droits d'accès des services aux ressources système. Si le service n'a pas le droit d'accès à la ressource système demandée, la demande échoue. Si le service a le droit d'accès à la ressource système, le système de protection charge dans la mémoire du composant électronique, en les déchiffrant s'ils sont chiffrés, les éléments descriptifs de la ressource système demandée. De cette manière, les éléments descriptifs d'une ressource système ne sont pas divulgués dans la mémoire du terminal, dans laquelle un service malveillant aurait pu les copier.

Ainsi, même si un service malveillant possède des moyens matériels d'espionner la mémoire du terminal pour en extraire des données, le service ne peut pas accéder aux éléments descriptifs d'une ressource système préalablement déchiffrés par le système de protection. Par conséquent, il n'est pas possible d'extraire des éléments descriptifs d'une ressource système, de les pirater et de les utiliser pour accéder illégalement à une ressource système.

Par ailleurs, le système de chiffrement SC peut être réalisé en partie en logique câblée plutôt que sous forme de logiciel. Seul le contrôleur de service CS doit être réalisé en tout ou partie sous forme de logiciel puisqu'il stocke et gère des tables qui peuvent être actualisées. En effet, la logique câblée optimise le fonctionnement en augmentant considérablement les performances. Puisque le temps de traitement effectué par le système de chiffrement SC constitue le principal délai pour l'accès aux ressources système, si ce traitement est trop long, l'exécution des services peut être aussi perçue comme trop longue par l'utilisateur du terminal. Pour que

le fonctionnement du terminal ne soit pas pénalisé par le temps de traitement du système de chiffrement SC, ce dernier doit être de préférence optimisé, par exemple en ayant recours à une réalisation en logique câblée.

Lorsque les éléments descriptifs sont contenus sous forme chiffrée dans le gestionnaire de ressource GR, leur maintenance est gérée par un système de maintenance SM, qui est par exemple localisé sur le terminal de l'utilisateur et mis à jour par le serveur de protection de service SPS. Le système de maintenance SM modifie des éléments descriptifs d'une ressource avec des paramètres de traitement par exemple de la manière suivante.

Pour chaque ressource système, le système de maintenance SM transmet au contrôleur de chiffrement CC une demande d'accès à la ressource contenant l'identifiant de la ressource système. Le contrôleur de chiffrement CC, via le contrôleur de service CS et le module de chiffrement MC, identifie des éléments descriptifs chiffrés associés à l'identifiant de la ressource système et déchiffre les éléments descriptifs chiffrés à l'aide d'une liste de paramètres de traitement contenue dans le contrôleur de service CS. Le contrôleur de chiffrement CC donne ainsi accès aux éléments descriptifs de la ressource au système de maintenance SM. Ce dernier transmet au contrôleur de chiffrement CC une demande de chiffrement des éléments descriptifs de la ressource avec une autre liste de paramètres de traitement inclus dans la demande. Le contrôleur de chiffrement CC, via le module de chiffrement MC, chiffre les éléments descriptifs et fournit ces derniers au gestionnaire de ressource avant d'informer le système de maintenance SM du résultat de l'opération.

Dès que toutes les ressources système à modifier ont été traitées, le système de maintenance SM informe le serveur de protection de service SPS du résultat de l'opération de maintenance et le serveur SPS met à jour la troisième table TC3 du contrôleur de service CS mettant en correspondance les identificateurs de ressource IR et les listes de paramètres de traitement LPT.

En référence à la figure 2, le procédé selon l'invention comprend des étapes E1 à E10 exécutées automatiquement sous le contrôle du système de protection SP inclus dans le terminal et mises en œuvre par des instructions d'un programme d'ordinateur enregistré sur un support d'enregistrement lisible par le système de protection SP.

Au préalable, un utilisateur du terminal a souscrit un abonnement auprès d'un ou plusieurs fournisseurs de service offrant des services numériques et devient ainsi un abonné à au moins un service.

A une étape initiale E0, le contrôleur de service CS mémorise ou actualise des tables de correspondance TC1, TC2 et TC3 en fonction du ou des services numériques auxquels l'utilisateur est abonné avec le concours du serveur de protection de service SPS.

Dans un premier exemple, le contrôleur de service CS interroge le serveur de protection de service SPS en fournissant à ce dernier un identificateur d'utilisateur IU. Le contrôleur CS obtient en retour au moins un identificateur de service ou plus généralement des identificateurs de service IS associés à l'identificateur d'utilisateur,

ainsi que les listes de paramètres de service LPS et les listes d'identificateurs de ressource LIR associées aux identificateurs de service, et les listes de paramètres de traitement LPT associées aux identificateurs de ressource IR, afin d'actualiser ou mémoriser les tables de correspondance TC1, TC2 et TC3. Cette interrogation peut être effectuée à chaque fois que le terminal est mis sous tension, pour vérifier une éventuelle modification dans les tables de correspondance.

Dans un deuxième exemple, le serveur de protection de service SPS interroge une base de données pour connaître au moins le service ou plus généralement les services accessibles par l'utilisateur, cette base de données étant par exemple un enregistreur de localisation nominal HLR ("Home Location Register" en anglais) dans un réseau cellulaire GSM/GPRS ("Global System for Mobile communications"/"General Packet Radio System" en anglais) ou un serveur de service nominal HSS ("Home Service Server" en anglais) dans un réseau cellulaire UMTS ("Universal Mobile Telecommunications System" en anglais). Le serveur SPS associe l'identificateur IU de l'utilisateur et les identificateurs IS du ou des services auxquels l'utilisateur est abonné. Puis le serveur SPS transmet au contrôleur de service CS les identificateurs de service et les listes de paramètres de service associées, ainsi que les identificateurs de ressources associés aux services et les listes de paramètres de traitement associées aux identificateurs de ressource, pour une actualisation totale des tables de correspondance TC1, TC2 et TC3 mémorisées dans le contrôleur de service CS.

Dans un troisième exemple, le serveur de protection de service SPS procède à une actualisation partielle des tables de correspondance TC1, TC2 et TC3, uniquement lorsqu'un changement a lieu. Ce changement peut être de plusieurs natures comme par exemple la création, la modification ou la suppression d'un service, et peut être à l'initiative d'un enregistreur HLR dans un réseau cellulaire GSM/GPRS ou d'un serveur HSS dans un réseau cellulaire UMTS. Le serveur de protection de service SPS transmet alors au contrôleur de service CS un fichier tenant compte de ces changements pour actualiser seulement les tables de correspondance concernées par ces changements.

Le contrôleur de service CS contient alors des tables de correspondance actualisées qui sont relatives à des identificateurs IS des services auxquels l'utilisateur est abonné et à des ressources d'exploitation qui sont accessibles par ces services.

Dans la première table de correspondance TC1, chaque identificateur de service IS est associé à une liste de paramètres de service LPS qui caractérise et identifie de manière unique et non ambiguë le service numérique correspondant parmi d'autres services. Chaque liste de paramètres de service contient des champs qui sont spécifiques au service numérique et qui sont renseignés par des valeurs de paramètres de service par le fournisseur du service numérique. Les paramètres de service sont par exemple un identificateur d'une application AP et/ou un identificateur de fournisseur de service.

Dans la deuxième table de correspondance TC2, chaque identificateur de service IS est associé à une liste d'identificateurs de ressource LIR. Chaque identificateur de service IS peut être

individuellement associé à un ou plusieurs identificateurs de ressource IR. Dans un exemple de mise en œuvre particulièrement simple, un identificateur de service est associé soit à au moins une ressource système accessible, soit à au moins une interdiction d'usage d'au moins une ressource. En d'autres termes, la deuxième table TC2 associe à chaque service des droits d'accès aux ressources système.

Dans la troisième table de correspondance TC3, chaque identificateur de ressource IR est en outre associé à une liste de paramètres de traitement LPT. Chaque liste de paramètres de traitement contient des champs qui sont spécifiques au service numérique et qui sont optionnellement renseignés par des valeurs de paramètres de traitement par le fournisseur du service numérique. Les paramètres de traitement sont par exemple un identificateur d'une application AP et/ou un identificateur de l'utilisateur, et peuvent donc être en partie du même type que les paramètres de service. Une liste de paramètres de traitement peut cependant être vide.

A l'étape E1, une application AP relative à un service est exécutée dans le terminal dans le contexte du service. Par exemple, l'utilisateur du terminal a sélectionné le lancement de l'application via une interface homme-machine du terminal indiquant à l'utilisateur les services auxquels ce dernier est abonné et les applications disponibles pour ces services. A titre d'exemple, l'application est un lecteur de média qui est exécuté pour un service d'écoute de musique à la demande.

L'application exécutée AP transmet une requête d'accès système RA à destination du système

d'exploitation du terminal afin d'accéder à l'une des ressources système du terminal. La requête d'accès système RA inclut un identificateur de ressource IR indiquant la ressource système à laquelle l'application requiert l'accès. A titre d'exemple, la requête d'accès système RA requiert l'accès à un haut-parleur pour l'écoute d'une musique.

A l'étape E2, la requête RA destinée au système d'exploitation est interceptée par le contrôleur d'accès CA du système de protection SP qui est à l'écoute de toute requête provenant de toute application à destination du système d'exploitation du terminal. Le contrôleur d'accès CA identifie alors l'application AP qui est à l'origine de la requête RA, par exemple au moyen d'une correspondance entre un processus système et un identificateur de l'application.

Le contrôleur d'accès CA modifie la requête interceptée RA en une requête modifiée RM en la complétant par un ou plusieurs champs de paramètres de contexte CP, et associe ainsi un ou des paramètres de contexte non renseignés à la requête.

Les champs sont destinés à être renseignés par les valeurs de paramètres de contexte qui peuvent être associés directement ou indirectement à l'application. Un paramètre de contexte associé directement à l'application est par exemple un identificateur de l'application AP, ou un identificateur de l'utilisateur. Un paramètre de contexte associé indirectement à l'application est par exemple un identificateur d'un ensemble fini de données associé au service, ou bien un identificateur de fournisseur de service. Optionnellement, le contrôleur d'accès CA mémorise temporairement la requête modifiée RM.

A l'étape E3, le contrôleur d'accès CA transmet la requête modifiée RM au contrôleur de chiffrement CC du système de chiffrement SC. Le contrôleur de chiffrement CC mémorise la requête modifiée RM, notamment l'identificateur de ressource IR inclus dans la requête RM.

A l'étape E4, le contrôleur de chiffrement CC interroge le serveur de paramètres SVP afin de renseigner les champs de paramètres de contexte CP dans la requête modifiée RM.

Le serveur de paramètres SVP détermine et fournit les valeurs de paramètres relatifs à l'application AP afin de renseigner les champs de la requête modifiée par ces valeurs.

Par exemple, le système d'exploitation du terminal gère une correspondance entre l'application AP, dont l'exécution est à l'origine de la requête RA dans le terminal, et un identificateur de l'application AP.

Le serveur de paramètres SVP transmet les champs de paramètres de contexte renseignés CPR au contrôleur de chiffrement CC qui les mémorise. Les paramètres de contexte renseignés sont alors associés à la requête et exploitables par le système de chiffrement SC.

En variante, les étapes E3 et E4 sont remplacées respectivement par des étapes E31 et E41.

A l'étape E31, le contrôleur d'accès CA interroge le serveur de paramètres SVP afin de renseigner les champs de paramètres de contexte CP dans la requête modifiée RM. Le serveur de paramètres SVP détermine et transmet les champs de paramètres de contexte renseignés CPR au contrôleur d'accès CA.

A l'étape E41, le contrôleur d'accès CA renseigne les champs de la requête modifiée RM au moyen des champs de paramètres de contexte renseignés CPR transmis par le serveur SVP et transmet la requête modifiée RM au contrôleur de chiffrement CC du système de chiffrement SC qui la mémorise.

A l'étape E5, le contrôleur de chiffrement CC transmet les champs de paramètres de contexte renseignés CPR au contrôleur de service CS.

Le contrôleur de service recherche dans la première table de correspondance TC1 l'identificateur IS du service numérique à l'origine de la requête.

Par exemple, le contrôleur CS met en correspondance un à un les champs de paramètres de contexte renseignés CPR avec les champs des différentes listes de paramètres de service LPS mémorisées.

Si tous les champs d'une et une seule liste de paramètres de service LPS sont inclus dans l'ensemble des champs de paramètres de contexte renseignés CPR, le contrôleur de service CS détermine à l'étape E6 ladite liste de paramètres de service LPS et déduit de la table TC1 l'identificateur de service IS associé à cette liste de paramètres de service. Par conséquent le contrôleur de service CS identifie le service numérique relatif à l'identificateur de service IS ainsi déduit.

Si tous les champs de plusieurs listes de paramètres de service LPS sont inclus dans l'ensemble des champs de paramètres de contexte renseignés CPR, le contrôleur de service CS transmet un message d'erreur au contrôleur de chiffrement CC, comme indiqué sur la figure 2 à une étape ER, et le procédé se termine.

Si aucune liste de paramètres de service LPS n'a des champs identiques à au moins une partie des champs de paramètres de contexte renseignés CPR, le contrôleur de service CS transmet un message d'erreur au contrôleur de chiffrement CC comme indiqué à l'étape ER, et le procédé se termine.

Si quelques champs d'une ou plusieurs listes de paramètres de service LPS sont inclus dans l'ensemble des champs de paramètres de contexte renseignés CPR, ces listes sont sélectionnées à une étape E51 par le contrôleur de service CS qui identifie l'ensemble des champs de la ou des listes de paramètres de service sélectionnées pour lesquels des champs de paramètres de contexte renseignés n'ont pu être mis en correspondance. Les champs identifiés sont considérés comme des champs de paramètres de contexte à renseigner. Le contrôleur de service CS transmet ensuite au contrôleur de chiffrement CC les champs identifiés pour que ces derniers soient renseignés au moyen du serveur de paramètres SVP puis retransmis au contrôleur de service CS. L'étape E5 est alors répétée une fois pour mettre en correspondance un à un les champs de paramètres de contexte renseignés CPR complétés par les champs identifiés renseignés avec les champs des différentes listes de paramètres de service LPS mémorisées. L'étape E51 ne peut plus être alors répétée puisque tous les champs de paramètres de contexte nécessaires à ladite mise en correspondance ont été renseignés.

En variante, l'identificateur de service IS est déjà renseigné dans les champs de paramètres de contexte renseignés CPR. L'identificateur de service IS est par exemple déjà fourni par le service auquel est dédiée l'application AP et donc inclus dans la

requête d'accès système RA. Dans cette variante, lors de l'identification du service numérique à l'origine de la requête, le contrôleur CS met en correspondance directement l'identificateur de service de la requête avec chacun des identificateurs de service de la première table de correspondance TC1.

Le contrôleur de service CS identifie alors le service numérique relatif à l'identificateur de service IS de la requête lorsque ce dernier est présent dans la première table TC1. Si l'identificateur de service IS de la requête est absent de la première table TC1, le contrôleur de service CS transmet un message d'erreur au contrôleur de chiffrement CC, comme indiqué à une étape ER, et le procédé se termine.

A l'étape E7, après identification du service à l'origine de la requête, le contrôleur de service CS recherche dans la deuxième table de correspondance TC2 les identificateurs de ressource associés à l'identificateur de service IS déduit à l'étape E6. Le contrôleur de service CS détermine ainsi la liste LIR des identificateurs des ressources associées au service identifié.

Le contrôleur de service CS vérifie alors si l'identificateur de ressource IR inclus dans la requête RA est l'un des identificateurs des ressources associées au service identifié, c'est-à-dire si l'identificateur de ressource IR appartient à la liste d'identificateurs de ressource LIR associée à l'identificateur de service IS. Si l'identificateur de ressource IR inclus dans la requête est bien associé à l'identificateur de service IS, le service est considéré comme autorisé à accéder à la ressource système correspondant audit identificateur de

ressource, et le contrôleur de service CS valide l'identificateur de ressource IR inclus dans la requête. Dans le cas contraire, le procédé se termine, et un message d'erreur est émis à l'intention de l'utilisateur du terminal.

A l'étape E8, le contrôleur de service CS détermine la liste de paramètres de traitement LPT associée à l'identificateur de ressource validé IR dans la troisième table de correspondance TC3 et transmet la liste LPT au contrôleur de chiffrement CC.

La liste de paramètres de traitement LPT détermine la manière de traiter les éléments descriptifs ED de la ressource système accessibles par le gestionnaire de ressources GR afin d'interpréter ces derniers. La liste LPT peut avoir des contenus de trois types différents qui sont traités par le système de protection SP à l'étape E9 constituée par l'une des étapes E91, E92 et E93 décrites ci-après selon le contenu de la liste LPT.

Dans un premier cas, la liste de paramètres de traitement LPT ne contient aucun élément, ce qui signifie que les éléments descriptifs ED ne sont pas chiffrés et sont directement interprétables par l'application AP sans recourir aux paramètres de traitement. La liste LPT est traitée à l'étape E91 par le système de protection SP.

Dans un deuxième cas, la liste de paramètres de traitement LPT contient une clé de chiffrement KC et une clé de déchiffrement KD. La liste LPT est traitée à l'étape E92 par le système de protection SP.

Dans un troisième cas, la liste de paramètres de traitement LPT contient des paramètres de chiffrement/déchiffrement nécessaires à la génération

d'une clé de chiffrement et d'une clé de déchiffrement. La liste LPT est traitée à l'étape E93 par le système de protection SP.

Dans les deuxième et troisième cas, les éléments descriptifs ED sont chiffrés en des éléments descriptifs chiffrés EDC et sont interprétables après avoir été déchiffrés en éléments descriptifs déchiffrés EDD. L'identificateur de ressource IR doit alors être également chiffré pour accéder aux éléments descriptifs chiffrés associés.

A l'étape E91, le contrôleur de chiffrement CC analyse une liste de paramètres de traitement vide et demande au contrôleur d'accès CA de charger les éléments descriptifs ED associés à l'identificateur de la ressource par l'intermédiaire du gestionnaire de ressource GR. Par exemple, les éléments descriptifs peuvent être mémorisés dans une mémoire volatile dont l'adresse est transmise à l'application AP pour que cette dernière interprète les éléments descriptifs mémorisés.

A l'étape E92, le contrôleur de chiffrement CC transmet l'identificateur de ressource IR et la clé de chiffrement KC au module de chiffrement MC. Ce dernier chiffre l'identificateur de ressource IR en fonction de la clé de chiffrement KC et transmet l'identificateur de ressource chiffré IRC au contrôleur de chiffrement CC. Le contrôleur CC demande au contrôleur d'accès CA de fournir les éléments descriptifs chiffrés EDC associés à l'identificateur de la ressource chiffré IRC, par exemple dans une mémoire volatile, par l'intermédiaire du gestionnaire de ressource GR. Le contrôleur de chiffrement CC charge alors les éléments descriptifs chiffrés EDC pour les transmettre avec la clé de déchiffrement KD au module

de chiffrement MC. Ce dernier déchiffre les éléments descriptifs chiffrés en fonction de la clé de déchiffrement et retransmet les éléments descriptifs déchiffrés EDD au contrôleur de chiffrement CC. Comme à l'étape E91, les éléments descriptifs déchiffrés peuvent être mémorisés dans une mémoire volatile dont l'adresse est transmise à l'application AP pour que cette dernière interprète les éléments descriptifs mémorisés.

A l'étape E93, le contrôleur de chiffrement CC transmet la liste de paramètres de traitement LPT au générateur de clé GC afin que ce dernier génère une clé de chiffrement KC et une clé de déchiffrement KD en fonction des valeurs des paramètres de traitement lus dans la liste LPT et retransmette les clés générées au contrôleur de chiffrement CC. En variante, si des champs de la liste de paramètres de traitement LPT transmise par le contrôleur de service CS ne sont pas renseignés dans la table de correspondance TC3, ces derniers sont renseignés au moyen du serveur de paramètres SVP. Le contrôleur de chiffrement CC procède ensuite comme à l'étape E92, afin de rendre accessibles en clair les éléments descriptifs à l'application AP.

A titre de remarque concernant l'étape E93, le module de chiffrement MC possède au moins deux types d'algorithme pour le traitement des données, par exemple un algorithme de chiffrement auquel est applicable toute clé de chiffrement et un algorithme de déchiffrement auquel est applicable toute clé de déchiffrement. Par conséquent, l'algorithme de chiffrement utilisé par le module de chiffrement MC est dual de l'algorithme de génération des clés de chiffrement utilisé par le générateur de clé GC, et l'algorithme de déchiffrement utilisé par le module

de chiffrement MC est dual de l'algorithme de génération des clés de déchiffrement utilisé par le générateur de clé GC.

A l'issue de l'étape E9, le contrôleur de chiffrement CC a éventuellement déchiffré les éléments descriptifs ED en fonction de la liste de paramètres de traitement LPT et rend alors accessible à l'étape E10 la ressource à l'application AP qui peut interpréter les éléments descriptifs en clair.

A titre d'exemple, le contrôleur de chiffrement CC mémorise les éléments descriptifs en clair dans une mémoire volatile dont l'adresse est transmise au contrôleur d'accès CA. Ce dernier transmet alors au système d'exploitation l'identificateur de l'application AP correspondant à un processus système et les éléments descriptifs ED associés à l'identificateur de ressource IR ainsi que l'adresse mémoire des éléments descriptifs. Le système d'exploitation qui exécute l'application AP et gère les ressources du terminal rend alors accessible la ressource à l'application.

Dans un souci de synchronisation entre les opérations exécutées dans le système de protection SP, par exemple exécutées par le générateur de clé GC et le module de chiffrement MC, le contrôleur de chiffrement CC reçoit une clé de chiffrement générée par le générateur de clé GC et associe la clé générée à la donnée à traiter préalablement chargée, telle qu'un identificateur de ressource, avant de les transmettre au module de chiffrement MC. Cette association garantit que la clé et la donnée à traiter transmises au module de chiffrement MC correspondent à une même requête. Ainsi, plusieurs

requêtes peuvent être traitées simultanément et indépendamment les unes des autres par le contrôleur de chiffrement CC.

En variante, les fonctionnalités du contrôleur de chiffrement CC sont intégrées partiellement ou totalement dans le contrôleur d'accès CA et/ou le générateur de clé GC et/ou le module de chiffrement MC et/ou le contrôleur de service CS. Dans ce cas, le contrôleur d'accès CA communique directement avec le générateur de clé GC, le module de chiffrement MC et le contrôleur de service CS et ces trois derniers communiquent également directement entre eux.

L'invention décrite ici concerne un procédé et un système pour gérer un accès à une ressource d'un terminal requise par une application dédiée à un service numérique et exécutée dans le terminal. Selon une mise en œuvre, les étapes du procédé de l'invention sont déterminées par les instructions d'un programme d'ordinateur incorporé dans le système de protection selon l'invention. Le programme comporte des instructions de programme qui, lorsque ledit programme est exécuté dans le système dont le fonctionnement est alors commandé par l'exécution du programme, réalisent les étapes du procédé selon l'invention.

En conséquence, l'invention s'applique également à un programme d'ordinateur, notamment un programme d'ordinateur enregistré sur ou dans un support d'enregistrement lisible par un ordinateur et tout dispositif de traitements de données, adapté à mettre en œuvre l'invention. Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code

intermédiaire entre code source et code objet tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable pour mettre en œuvre le procédé selon l'invention.

L'invention concerne également un support d'enregistrement, qui peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage sur lequel est enregistré le programme d'ordinateur selon l'invention, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore une clé USB, ou un moyen d'enregistrement magnétique, par exemple une disquette ("floppy disc") ou un disque dur.

D'autre part, le support d'enregistrement peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type internet.

Alternativement, le support d'enregistrement peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé selon l'invention.

REVENDICATIONS

1 - Procédé pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution (AP) d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution (AP) étant dédiée à un service numérique et ayant émis une requête d'accès système (RA) incluant un identificateur de ressource (IR) à destination d'un système d'exploitation du terminal, ledit procédé étant caractérisé en ce qu'il comprend les étapes de :

après interception (E2) de ladite requête (RA), identifier l'unité d'exécution (AP) à l'origine de ladite requête,

déterminer (E4) au moins un paramètre de contexte (CPR) relatif à ladite unité d'exécution identifiée (AP), et associer à la requête (RA) ledit paramètre de contexte (CPR),

identifier (E6) ledit service en fonction du paramètre de contexte (CPR),

déterminer (E7) des identificateurs des ressources associées audit service identifié, et

si ledit identificateur de ressource (IR) inclus dans la requête (RA) est l'un desdits identificateurs des ressources associées au service identifié, déterminer (E8) des paramètres de traitement (LPT) associés à cet identificateur de ressource (IR), et traiter (E9), en fonction desdits paramètres de traitement déterminés (LPT), des éléments descriptifs (ED) de la ressource, afin de rendre la ressource accessible à l'unité d'exécution (AP).

2 - Procédé conforme à la revendication 1, selon lequel les éléments descriptifs (ED) de la ressource ne sont pas chiffrés.

3 - Procédé conforme à la revendication 1, selon lequel les éléments descriptifs (ED) de la ressource sont chiffrés et sont interprétables par l'unité d'exécution après un déchiffrement des éléments descriptifs chiffrés (EDC) en fonction des paramètres de traitement.

4 - Procédé conforme à l'une quelconque des revendications 1 à 3, selon lequel des paramètres de service sont associés au service, et le service est identifié (E6) si tous les paramètres de service associés au service et seulement audit service sont inclus dans un ensemble de paramètres de contexte (CPR) relatifs à l'unité d'exécution identifiée et associés à la requête.

5 - Système pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution (AP) d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution (AP) étant dédiée à un service numérique et ayant émis une requête d'accès système (RA) incluant un identificateur de ressource (IR) à destination d'un système d'exploitation du terminal, ledit système étant caractérisé en ce qu'il comprend :

un moyen (CA) pour intercepter ladite requête (RA) et pour identifier l'unité d'exécution (AP) à l'origine de ladite requête,

un moyen (SVP) pour déterminer au moins un paramètre de contexte (CPR) relatif à ladite unité d'exécution identifiée (AP),

un moyen (CA ; CC) pour associer à la requête (RA) ledit paramètre de contexte (CPR),

un moyen (CS) pour identifier ledit service en fonction du paramètre de contexte (CPR),

un moyen (CS) pour déterminer des identificateurs des ressources associées audit service identifié,

un moyen (CS) pour déterminer des paramètres de traitement (LPT) associés à cet identificateur de ressource (IR) si ledit identificateur de ressource (IR) inclus dans la requête (RA) est l'un desdits identificateurs des ressources associées au service identifié, et

un moyen (CC) pour traiter, en fonction desdits paramètres de traitement déterminés (LPT), des éléments descriptifs (ED) de la ressource, afin de rendre la ressource accessible à l'unité d'exécution (AP).

6 - Système conforme à la revendication 5, dans lequel le moyen (CS) pour identifier le service contient une première table (TC1) mettant en correspondance des identificateurs de service (IS) et des listes de paramètres de service (LPS), une deuxième table (TC2) mettant en correspondance les identificateurs de service (IS) et des listes d'identificateurs de ressource (LIR), et une troisième table (TC3) mettant en correspondance les identificateurs de ressource (IR) et des listes de paramètres de traitement (LPT), lesdites tables de correspondance étant actualisées par au moins un moyen serveur (SPS) en fonction des services numériques auxquels l'utilisateur du terminal est abonné.

7 - Système conforme à la revendication 5 ou 6, inclus dans un composant électronique.

8 - Programme d'ordinateur apte à être mis en œuvre dans un système pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution (AP) d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution (AP) étant dédiée à un service numérique et ayant émis une requête d'accès système (RA) incluant un identificateur de ressource (IR) à destination d'un système d'exploitation du terminal, ledit programme étant caractérisé en ce qu'il comprend des instructions qui, lorsque le programme est exécuté dans ledit système, réalisent les étapes de :

après interception (E2) de ladite requête (RA), identifier l'unité d'exécution (AP) à l'origine de ladite requête,

déterminer (E4) au moins un paramètre de contexte (CPR) relatif à ladite unité d'exécution identifiée (AP), et associer à la requête (RA) ledit paramètre de contexte (CPR),

identifier (E6) ledit service en fonction du paramètre de contexte (CPR),

déterminer (E7) des identificateurs des ressources associées audit service identifié, et

si ledit identificateur de ressource (IR) inclus dans la requête (RA) est l'un desdits identificateurs des ressources associées au service identifié, déterminer (E8) des paramètres de traitement (LPT) associés à cet identificateur de ressource (IR), et traiter (E9), en fonction desdits paramètres de traitement déterminés (LPT), des éléments descriptifs (ED) de la ressource, afin de rendre la ressource accessible à l'unité d'exécution (AP).

9 - Support d'enregistrement lisible par un système pour gérer un accès à une ressource d'un terminal requise par une unité d'exécution (AP) d'un programme applicatif exécuté dans le terminal, ladite unité d'exécution (AP) étant dédiée à un service numérique et ayant émis une requête d'accès système (RA) incluant un identificateur de ressource (IR) à destination d'un système d'exploitation du terminal, caractérisé en ce qu'il a enregistré un programme d'ordinateur comportant des instructions pour l'exécution des étapes suivantes :

après interception (E2) de ladite requête (RA), identifier l'unité d'exécution (AP) à l'origine de ladite requête,

déterminer (E4) au moins un paramètre de contexte (CPR) relatif à ladite unité d'exécution identifiée (AP), et associer à la requête (RA) ledit paramètre de contexte (CPR),

identifier (E6) ledit service en fonction du paramètre de contexte (CPR),

déterminer (E7) des identificateurs des ressources associées audit service identifié, et

si ledit identificateur de ressource (IR) inclus dans la requête (RA) est l'un desdits identificateurs des ressources associées au service identifié, déterminer (E8) des paramètres de traitement (LPT) associés à cet identificateur de ressource (IR), et traiter (E9), en fonction desdits paramètres de traitement déterminés (LPT), des éléments descriptifs (ED) de la ressource, afin de rendre la ressource accessible à l'unité d'exécution (AP).

FIG. 1

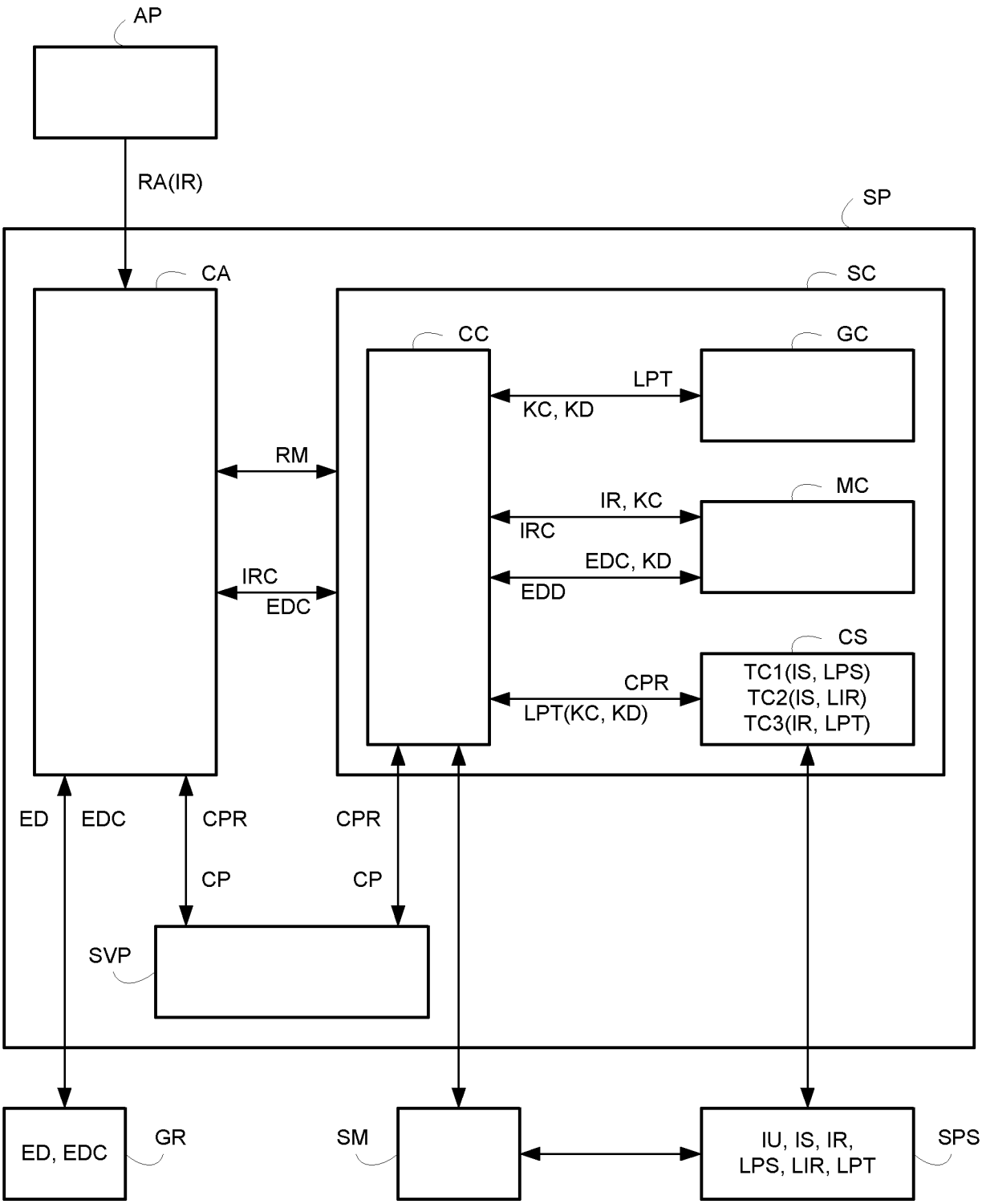
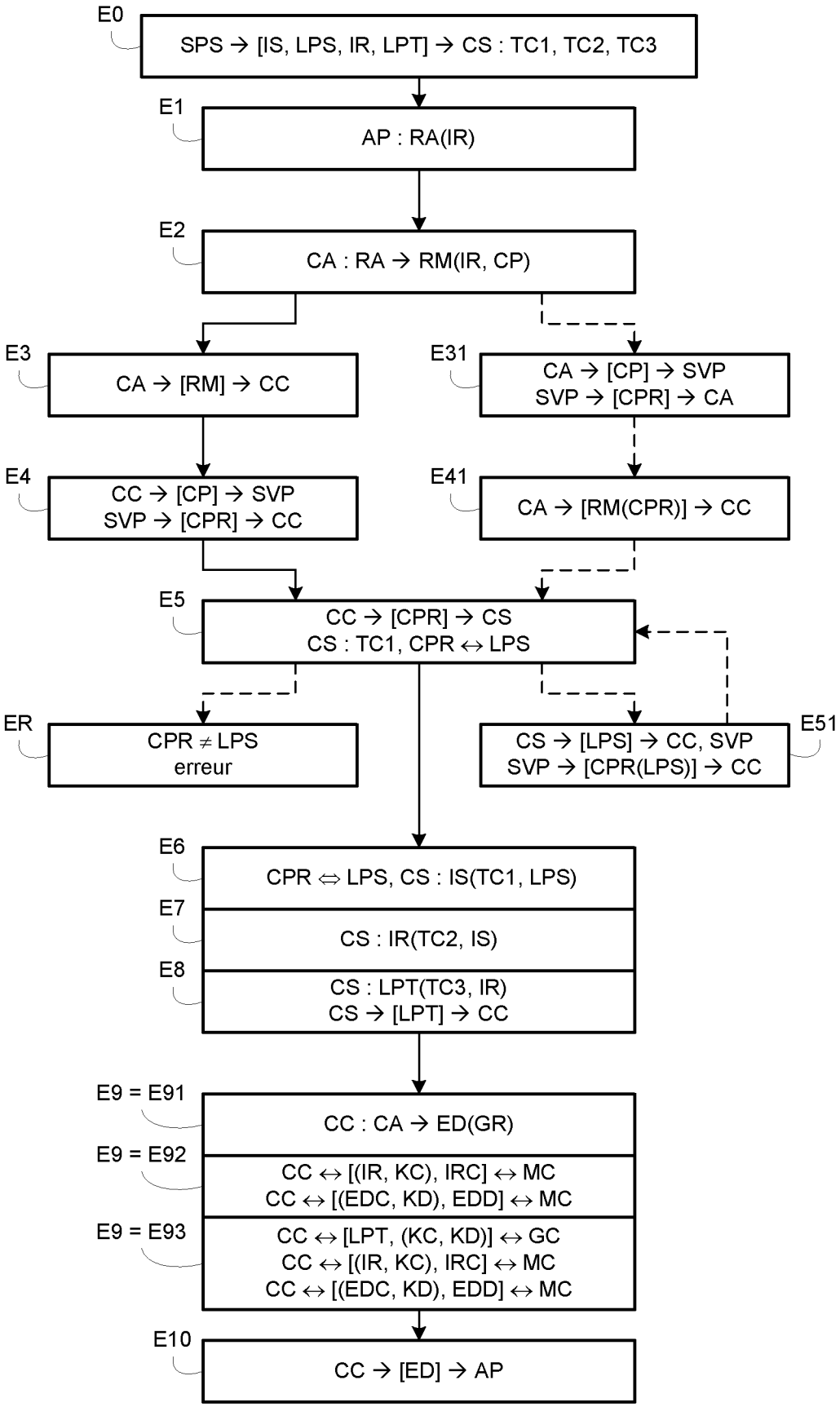

AP
RA(IR)
SP
CA
SC
CC
GC
LPT
KC, KD
RM
MC
IR, KC
IRC
EDC, KD
EDD
IRC
EDC
CS
TC1(IS, LPS)
TC2(IS, LIR)
TC3(IR, LPT)
CPR
LPT(KC, KD)
ED
EDC
CPR
CPR
CP
CP
SVP
ED, EDC
GR
SM
IU, IS, IR,
LPS, LIR, LPT
SPS

FIG. 2


E0
SPS → [IS, LPS, IR, LPT] → CS : TC1, TC2, TC3
E1
AP : RA(IR)
E2
CA : RA → RM(IR, CP)
E3
CA → [RM] → CC
E31
CA → [CP] → SVP
SVP → [CPR] → CA
E4
CC → [CP] → SVP
SVP → [CPR] → CC
E41
CA → [RM(CPR)] → CC
E5
CC → [CPR] → CS
CS : TC1, CPR ↔ LPS
ER
CPR ≠ LPS
erreur
E51
CS → [LPS] → CC, SVP
SVP → [CPR(LPS)] → CC
E6
CPR ⇔ LPS, CS : IS(TC1, LPS)
E7
CS : IR(TC2, IS)
E8
CS : LPT(TC3, IR)
CS → [LPT] → CC
E9 = E91
CC : CA → ED(GR)
E9 = E92
CC ↔ [(IR, KC), IRC] ↔ MC
CC ↔ [(EDC, KD), EDD] ↔ MC
E9 = E93
CC ↔ [LPT, (KC, KD)] ↔ GC
CC ↔ [(IR, KC), IRC] ↔ MC
CC ↔ [(EDC, KD), EDD] ↔ MC
E10
CC → [ED] → AP

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2008/050538

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 526 429 A (MICROSOFT CORP [US]) 27 April 2005 (2005-04-27) page 1 - page 6 figures 1,2	1-9
A	WO 03/021467 A (QUALCOMM INC [US]; SPRIGG STEPHEN A [US]; LUNDBLADE LAURENCE [US]) 13 March 2003 (2003-03-13) page 1 - page 13	1-9
A	EP 0 813 132 A2 (IBM [US]) 17 December 1997 (1997-12-17) the whole document	1-9
A	US 2006/075381 A1 (LABORCZFALVI LEE G [AU] ET AL) 6 April 2006 (2006-04-06) paragraph [0089]	1,5,8,9

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 septembre 2008	02/10/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Segura, Gustavo

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2008/050538

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1526429 A	27-04-2005	CN 1617101 A	18-05-2005
		JP 2005129066 A	19-05-2005
		KR 20050039661 A	29-04-2005
		US 2005091658 A1	28-04-2005
		US 2005091214 A1	28-04-2005
WO 03021467 A	13-03-2003	BR 0211884 A	21-09-2004
		CA 2457357 A1	13-03-2003
		CN 1556959 A	22-12-2004
		EP 1417588 A1	12-05-2004
		JP 2005502128 T	20-01-2005
		MX PA04001386 A	03-06-2004
		NZ 531131 A	23-12-2005
		RU 2307390 C2	27-09-2007
		TW 281107 B	11-05-2007
EP 0813132 A2	17-12-1997	DE 69732323 D1	03-03-2005
		DE 69732323 T2	22-12-2005
		JP 3701773 B2	05-10-2005
		JP 10083310 A	31-03-1998
		US 5825877 A	20-10-1998
US 2006075381 A1	06-04-2006	CN 101065727 A	31-10-2007
		CN 101073058 A	14-11-2007
		CN 101069156 A	07-11-2007
		CN 101069157 A	07-11-2007

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2008/050538

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 526 429 A (MICROSOFT CORP [US]) 27 avril 2005 (2005-04-27) page 1 - page 6 figures 1,2	1-9
A	WO 03/021467 A (QUALCOMM INC [US]; SPRIGG STEPHEN A [US]; LUNDBLADE LAURENCE [US]) 13 mars 2003 (2003-03-13) page 1 - page 13	1-9
A	EP 0 813 132 A2 (IBM [US]) 17 décembre 1997 (1997-12-17) le document en entier	1-9
A	US 2006/075381 A1 (LABORCZFALVI LEE G [AU] ET AL) 6 avril 2006 (2006-04-06) alinéa [0089]	1,5,8,9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
25 septembre 2008	02/10/2008

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Segura, Gustavo

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2008/050538

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1526429 A	27-04-2005	CN 1617101 A	18-05-2005
		JP 2005129066 A	19-05-2005
		KR 20050039661 A	29-04-2005
		US 2005091658 A1	28-04-2005
		US 2005091214 A1	28-04-2005
WO 03021467 A	13-03-2003	BR 0211884 A	21-09-2004
		CA 2457357 A1	13-03-2003
		CN 1556959 A	22-12-2004
		EP 1417588 A1	12-05-2004
		JP 2005502128 T	20-01-2005
		MX PA04001386 A	03-06-2004
		NZ 531131 A	23-12-2005
		RU 2307390 C2	27-09-2007
		TW 281107 B	11-05-2007
EP 0813132 A2	17-12-1997	DE 69732323 D1	03-03-2005
		DE 69732323 T2	22-12-2005
		JP 3701773 B2	05-10-2005
		JP 10083310 A	31-03-1998
		US 5825877 A	20-10-1998
US 2006075381 A1	06-04-2006	CN 101065727 A	31-10-2007
		CN 101073058 A	14-11-2007
		CN 101069156 A	07-11-2007
		CN 101069157 A	07-11-2007