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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
19 novembre 2009 (19.11.2009)

PCT

(10) Numéro de publication internationale
WO 2009/138641 A1

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

(21) Numéro de la demande internationale : PCT/FR2009/050717

(22) Date de dépôt international : 17 avril 2009 (17.04.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0852682 21 avril 2008 (21.04.2008) 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)* : **BEL, Vincent** [FR/FR]; 62 rue de Vouillé, F-75015 PARIS (FR). **MAUPETIT, Matthieu** [FR/FR]; 14 rue Nélaton, F-75015 Paris (FR). **CHARLES, Olivier** [FR/FR]; 218 avenue Jean Jaures, F-92140 Clamart (FR).

(74) Mandataire : **FRANCE TELECOM R&D/PIV/BREVETS**; RENARD Béatrice, 38-40 rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 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, 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, ST, 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, MK, 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).

[Suite sur la page suivante]

(54) Title : METHOD OF USE OF A HOST TERMINAL BY AN EXTERNAL DEVICE CONNECTED TO THE TERMINAL

(54) Titre : PROCEDE D'UTILISATION D'UN TERMINAL HOTE PAR UN DISPOSITIF EXTERNE CONNECTE AU TERMINAL

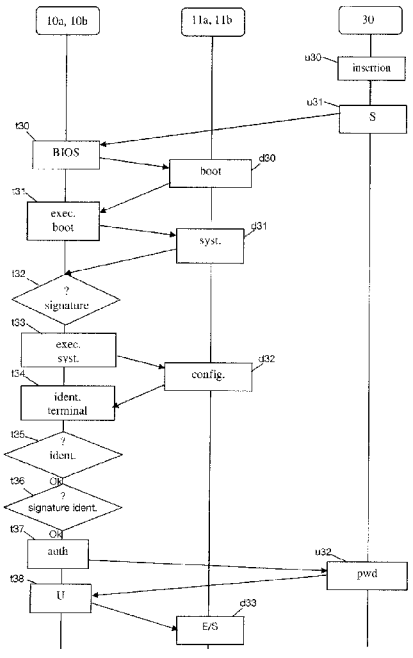

Figure 3

(57) Abstract : The invention relates to a method of using a host terminal with the aid of an external device connected to the terminal and hosting at least one program, comprising: - during a phase of starting the terminal, a step (t33) of starting the execution of the program hosted by the external device, on the host terminal, characterized in that, the external device storing a list, so-called "white list", of identifiers of authorized terminals, there is provided: - a step (t34) of determining, by the program of the external device, an identifier of the terminal on the basis of data relating to intrinsic hardware means of the terminal, - a step (t35) of verifying the determined identifier, in the course of which the program of the external device verifies that the determined identifier belongs to the white list, the execution of the program being continued if the verification of the identifier is positive.

(57) Abrégé : L'invention concerne un procédé d'utilisation d'un terminal hôte à l'aide d'un dispositif externe connecté au terminal et hébergeant au moins un programme, comprenant : - lors d'une phase de démarrage du terminal, une étape (t33) de démarrage de l'exécution du programme hébergé par le dispositif externe, sur le terminal hôte, caractérisé par le fait que, le dispositif externe mémorisant une liste, dite "liste blanche", d'identifiants de terminaux autorisés, il est prévu : - une étape (t34) de détermination, par le programme

[Suite sur la page suivante]

WO 2009/138641 A1

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

du dispositif externe, d'un identifiant du terminal à partir de données relatives à des moyens matériels intrinsèques du terminal, - une étape (t35) de vérification de l'identifiant déterminé, au cours de laquelle le programme du dispositif externe vérifie l'appartenance de l'identifiant déterminé à la liste blanche, l'exécution du programme étant poursuivie si la vérification de l'identifiant est positive.

Procédé d'utilisation d'un terminal hôte par un dispositif externe connecté au terminal

La présente invention concerne un procédé d'utilisation d'un terminal hôte par un dispositif externe connecté au terminal.

Le dispositif externe peut être un dispositif de stockage amovible apte à être connecté au terminal hôte. Il permet le transport d'un environnement informatique d'exécution de terminal. Un tel dispositif contient les programmes et données nécessaires au fonctionnement de ce terminal hôte : système d'exploitation, données d'accès au réseau, données de l'utilisateur, etc. C'est au moment du démarrage du terminal hôte que ce dernier charge les programmes accessibles via ce dispositif de stockage externe et les exécute.

Le document WO 2007/096554 décrit une solution pour accéder depuis un terminal hôte à un réseau de télécommunications prédéfini, à partir de données relatives à un environnement informatique stockées dans une mémoire externe amovible. Pour accéder au réseau à partir du terminal hôte, l'utilisateur connecte la mémoire externe amovible à ce terminal hôte puis démarre ce dernier. Au moment de son démarrage, le terminal charge les programmes dont il a besoin (système d'exploitation, etc.) et qui sont accessibles via la mémoire externe. Ainsi, la connexion est établie à partir de programmes stockés dans la mémoire externe amovible. Un cas d'usage de la solution décrite dans WO 2007/096554 peut être l'accès à distance par un utilisateur nomade, travaillant pour une entreprise, au réseau interne de cette entreprise depuis un terminal externe au réseau de l'entreprise. Dans ce cas, l'utilisateur connecte au terminal externe au réseau de l'entreprise une mémoire amovible contenant des programmes et/ou données d'environnement informatique fournis par l'entreprise et donc a priori fiables. A aucun moment, les logiciels et les données stockés dans le terminal hôte lui-même ne sont exécutés. Grâce à cela, l'utilisateur peut accéder au réseau interne de son entreprise à partir de n'importe quel terminal, dans des conditions de sécurité optimales puisque ce sont les programmes et/ou données de l'environnement informatique stockées dans la mémoire externe amovible qui sont utilisées pour

établir une telle connexion, et non des données stockées dans le terminal lui-même. Ainsi, l'utilisateur ne craint pas les éventuels programmes malveillants qui pourraient se trouver dans le terminal hôte, puisque de tels programmes ne sont pas utilisés.

Un des bénéfices procurés par cette solution est donc la sécurité.

Cependant, une telle solution permet d'utiliser l'environnement informatique stocké dans le dispositif externe, et donc les programmes qui y sont stockés, au mépris des licences de programmes qui sont généralement délivrées pour un terminal spécifique, ou pour un parc de terminaux spécifiques.

Il existe donc un besoin pour circonscrire la faculté d'utiliser un environnement informatique hébergé dans un périphérique externe, à un parc prédéfini de terminaux.

L'invention répond à ce besoin en proposant un procédé d'utilisation d'un terminal hôte à l'aide d'un dispositif externe connecté au terminal et hébergeant au moins un programme, comprenant :

- lors d'une phase de démarrage du terminal, une étape de démarrage de l'exécution du programme hébergé par le dispositif externe, sur le terminal hôte, caractérisé par le fait que, le dispositif externe mémorisant une liste, dite "liste blanche", d'identifiants de terminaux autorisés, il est prévu :

- une étape de détermination, par le programme du dispositif externe, d'un identifiant du terminal à partir de données relatives à des moyens matériels intrinsèques du terminal,

- une étape de vérification de l'identifiant déterminé, au cours de laquelle le programme du dispositif externe vérifie l'appartenance de l'identifiant déterminé à la liste blanche,

l'exécution du programme étant poursuivie si la vérification de l'identifiant est positive.

Le procédé de l'invention permet ainsi de limiter l'utilisation de l'environnement de l'utilisateur, stocké sur un dispositif portable, à un parc de terminaux hôtes potentiels identifiés. Ainsi, une entreprise qui délivre à ses

employés de tels environnements portables dans un contexte professionnel est assurée que ces environnements ne sont utilisés qu'à l'aide de terminaux autorisés, à l'exclusion de terminaux hôtes dédiés à un usage privé. Cela garantit un contrôle de l'utilisation des environnements, et des programmes y afférents. En particulier, lorsque de tels environnements sous soumis à des licences logicielles, cela garantit un respect des accords de licences passés avec un fournisseur de logiciels et donc fournit un cadre légal d'utilisation.

D'autre part, cela renforce la sécurité liée à l'utilisation de tels environnements. En effet, il existe un risque, lorsqu'on lance un tel environnement depuis un terminal quelconque, que ce terminal quelconque dispose d'un dispositif matériel d'enregistrement de touches saisies sur le clavier (le terme couramment utilisé pour désigner un tel dispositif est le terme anglais "keylogger") permettant de récupérer des identifiants et mots de passe de l'utilisateur. Un attaquant obtenant des informations d'identification peut ensuite usurper l'identité de l'utilisateur pour accéder au réseau de l'entreprise.

Dans une réalisation de l'invention, le dispositif externe stockant un programme d'amorçage et un système d'exploitation, il est prévu, lors de la phase de démarrage du terminal,

- une étape d'exécution dudit programme d'amorçage accessible via le dispositif externe.

- l'exécution dudit programme d'amorçage déclenchant l'étape de démarrage du système d'exploitation.

Dans une réalisation de l'invention, le procédé de l'invention comprend en outre une étape de vérification de l'intégrité du système d'exploitation hébergé par le dispositif externe, réalisée par le programme d'amorçage, l'étape de démarrage de l'exécution du système d'exploitation étant exécutée, seulement si la vérification est positive.

Avec l'invention, le lancement de l'environnement de l'utilisateur est hautement sécurisé. En effet, le programme de boot, non modifiable par un utilisateur, vérifie lors de son exécution l'intégrité de la zone comprenant le système d'exploitation, le système d'exploitation, lors de son exécution, vérifiant alors la liste blanche des terminaux hôtes autorisés. Ainsi, il n'est pas possible

pour un pirate, de modifier la zone système pour éventuellement insérer des routines erronées pour le traitement de la liste blanche des terminaux hôtes autorisés. En outre, l'utilisation d'un schéma cryptographique à clés publiques pour vérifier l'intégrité de la liste blanche des identifiants de terminaux n'implique aucune contrainte de sécurité sur le format de stockage de la clé publique. Cette clé, stockée soit dans le même bloc mémoire que celui où est stocké le programme d'amorçage, soit dans le même bloc que celui où est stocké le système d'exploitation, est accessible par le système d'exploitation pour effectuée le contrôle d'intégrité.

Dans une réalisation de l'invention, le procédé comprend :

- si la vérification de l'identifiant est négative, une étape d'envoi dudit identifiant vers un administrateur,
- une étape de contrôle de l'identifiant par l'administrateur afin de déterminer s'il est autorisé,
- si le contrôle est positif, une étape d'envoi par l'administrateur dudit identifiant vers le système d'exploitation, et
- une étape d'enregistrement dudit identifiant dans la liste blanche d'identifiants autorisés.

Un procédé de mise à jour d'une liste blanche de terminaux autorisés en mode connecté présente l'avantage de faciliter une mise à jour éventuelle de dispositifs externes puisqu'il n'est pas nécessaire pour un porteur de dispositif de ramener son dispositif à un administrateur lorsque la liste blanche des terminaux autorisés doit être mise à jour.

Dans une réalisation de l'invention, la liste blanche d'identifiants autorisés comprend en outre, pour au moins un identifiant, une information temporelle de validité.

La précision d'une date limite d'utilisation d'un dispositif sur un terminal permet à un administrateur de maîtriser la période pendant laquelle un dispositif peut être utilisé, ce qui peut être utile lorsqu'une licence logicielle est octroyée pendant une période prédéfinie. C'est le cas par exemple de licences accordées en prêt, dans un but de test.

L'invention concerne aussi un dispositif apte à connecté à un terminal hôte, comprenant des moyens de stockage contenant :

- au moins un programme,
- une liste dite "liste blanche" d'identifiants de terminaux hôtes autorisés,

ledit programme étant apte, au démarrage de son exécution, à

- déterminer un identifiant d'un terminal hôte auquel ledit dispositif est connecté, à partir de données relatives à des moyens matériels intrinsèques du terminal
- vérifier l'appartenance de l'identifiant déterminé à la liste blanche,
- poursuivre son exécution seulement si la vérification est positive.

Dans une réalisation du dispositif selon l'invention, les moyens de stockage comprennent un programme d'amorçage et un système d'exploitation, ledit programme d'amorçage vérifiant au démarrage de son exécution l'intégrité du système d'exploitation hébergé par le dispositif externe, le démarrage de l'exécution du système d'exploitation ne s'exécutant que si la vérification est positive.

Avantageusement, ledit programme est apte, si la vérification de l'identifiant est négative, à :

- envoyer ledit identifiant vers un administrateur apte à déterminer si ledit identifiant est autorisé, et le cas échéant, à renvoyer ledit identifiant,
- recevoir ledit identifiant,
- si le contrôle est positif, une étape d'envoi par l'administrateur dudit identifiant vers le système d'exploitation, et
- enregistrer ledit identifiant dans la liste blanche des identifiants de terminaux hôtes autorisés.

L'invention concerne aussi un programme destiné à être installé dans une mémoire d'un dispositif de stockage adapté pour être connecté à un terminal hôte, ledit dispositif mémorisant une liste, dite "liste blanche", d'identifiants de terminaux autorisés, et comprenant des portions de code pour :

- déterminer un identifiant du terminal hôte à partir de données relatives à des moyens matériels intrinsèques du terminal,

- vérifier l'appartenance de l'identifiant déterminé à la liste blanche,

- poursuivre son exécution si la vérification de l'identifiant est positive.

D'autres caractéristiques et avantages de la présente invention seront mieux compris à la lecture de la description de différents exemples de réalisation du périphérique externe de stockage de l'invention et un mode de réalisation particulier du procédé d'utilisation d'un terminal hôte à l'aide d'un tel dispositif, en référence aux schémas annexés donnés à titre non limitatif et dans lesquels :

- la figure 1a représente un premier exemple de réalisation du dispositif externe de stockage selon l'invention et un terminal hôte ;

- la figure 1b représente un deuxième exemple de réalisation du dispositif externe de stockage selon l'invention et un terminal hôte ;

- la figure 2 représente schématiquement une mémoire du périphérique externe de stockage représenté sur la figure 1a ;

- la figure 3 représente les étapes du procédé d'utilisation du terminal hôte avec le dispositif externe de stockage de la figure 1a, selon un mode de réalisation particulier de l'invention ;

- la figure 4 présente des étapes de mise à jour d'une liste blanche d'identifiants du dispositif externe de stockage de la figure 1a, selon un mode de réalisation de l'invention.

La figure 1a illustre un premier exemple de réalisation du périphérique externe de stockage 11a de l'invention et un terminal hôte 10a apte à être utilisé via le dispositif 11a.

Dans cet exemple de réalisation, le dispositif 11a est une clé, ici une clé de type "USB" (de l'anglais "Universal Serial Bus"), comprenant des moyens de stockage de données.

Le terminal 10a est ici, de manière classique, un ordinateur personnel "PC" (Personal Computer) disposant au moins d'une unité centrale de

traitement de données, d'un clavier, d'un écran et d'un bus de communication pour interconnecter des périphériques à l'unité centrale, par exemple un bus série répondant à la norme USB. Le terminal 10a comprend en outre au moins un port de connexion USB, auquel la clé USB 11a peut être connectée. On notera que le terminal 10a peut ne pas comprendre de disque dur car celui-ci n'est pas utilisé pour la mise en œuvre de l'invention.

Le terminal 10a comprend également de manière classique une mémoire dans laquelle est stocké un programme BIOS (Basic Input/Output System), ou système de base d'entrée/sortie. De façon bien connue de l'homme du métier, ce programme BIOS est apte à réaliser une détection, lors du démarrage du terminal 10a, de périphériques internes et externes du terminal 10a, ainsi que le démarrage d'un système d'exploitation.

La figure 1b illustre un deuxième exemple de réalisation du dispositif externe de stockage selon l'invention. Il s'agit dans ce cas d'un terminal de communication 11b, en l'espèce un téléphone mobile, comprenant une carte à puce et des moyens de stockage de données. Le terminal de communication 11b pourrait en variante être un assistant personnel ("PDA", pour "Personal Data Assistant"), ou autre. Sur la figure 1b, le terminal hôte est référencé 10b et identique au terminal 10a de la figure 1a.

En connectant le téléphone mobile 11b au terminal 10b par l'intermédiaire d'un câble USB, trois périphériques du téléphone mobile 11b sont alors accessibles par le terminal 10b via le même port USB :

- une mémoire du téléphone mobile 11b ;
- un module d'accès au réseau du téléphone mobile 11b, en l'espèce un modem d'accès au réseau mobile du téléphone 11b ; et
- une carte à puce, ici une carte "SIM" ("Subscriber Identity Module"), utilisée par le module d'accès au réseau pour des applications de téléphonie.

Dans ce deuxième exemple de réalisation, le téléphone 11b peut jouer le rôle d'une carte réseau ou d'un modem apte à fournir un accès au réseau mobile du téléphone 11b, vis-à-vis du terminal hôte 10b. En ce qui concerne l'utilisation de la carte SIM du module d'accès réseau comme carte à puce, on

utilise de préférence pour le terminal 10b un pilote virtuel tel que décrit dans la demande de brevet publiée sous le numéro WO2005/036822. Un tel pilote est susceptible d'être utilisé aussi bien avec une liaison filaire qu'avec une liaison non filaire, par exemple bluetooth, entre le terminal 10b et le terminal de communication 11b. De la sorte, le terminal 10b peut accéder à la carte SIM du terminal de communication 11b comme s'il s'agissait d'une carte à puce insérée dans un lecteur local du terminal 10b, et donc en faisant abstraction du lien USB et des contraintes d'accès liées à l'intégration de la carte SIM dans l'environnement du terminal de communication 11b.

Selon le même principe, un pilote virtuel est utilisable également pour le pilotage du module d'accès au réseau, de manière à ce que les programmes d'accès au réseau fonctionnent de la même manière que si le module d'accès au réseau était un module installé localement sur le terminal 10b.

La suite de la description se réfère aussi bien au premier exemple de réalisation (clé USB 11a) qu'au deuxième exemple de réalisation (terminal de communication 11b) du dispositif externe de stockage.

Le dispositif externe de stockage 11a (11b) comprend des moyens de stockage de données, comprenant une mémoire, partagée de manière classique en deux zones :

- une zone système qui contient :
  - un fichier contenant un système d'exploitation,
  - un programme d'amorçage, couramment appelé "boot" ou "bootstrap", situé dans des premiers octets de la zone système, adapté pour être déclenché par le BIOS d'un terminal hôte et pour démarrer le système d'exploitation,
- une zone utilisateur destinée à héberger des données et des programmes de l'utilisateur : documents de travail, logiciels, fichiers de configurations, etc.

L'invention utilise un découpage spécifique de la mémoire du dispositif de stockage externe 11a (11b), servant à la mise en œuvre du procédé selon l'invention.

Une forme de réalisation particulière de la mémoire du dispositif externe de stockage 11a (11b) selon l'invention va maintenant être décrit en relation avec la figure 2.

La mémoire représentée sur cette figure 2 est structurée, découpée en quatre blocs 20, 21, 22 et 23. L'ensemble de ces blocs constituent une partition de la mémoire.

Le premier bloc mémoire 20 correspond à une zone d'amorçage sécurisée. Ce premier bloc 20 comprend un programme d'amorçage B20, ou programme de boot, ayant pour rôle de déclencher le chargement d'un noyau d'un système d'exploitation dans un terminal hôte, ce noyau étant lui-même stocké dans le deuxième bloc mémoire 21.

Le premier bloc mémoire 20 est à accès en écriture sécurisé. Selon un premier exemple de réalisation, ce bloc de mémoire est du type mémoire morte ROM (Read Only Memory), rendant impossible la modification des données qui y sont stockées. Selon un deuxième exemple de réalisation, l'accès en écriture à ce bloc mémoire est possible, sous réserve de disposer d'un code d'accès. Une mise à jour est alors possible pour un administrateur autorisé disposant de ce code d'accès. Dans ce deuxième exemple de réalisation, on utilise par exemple une mémoire couplée à une carte à puce, par exemple la mémoire d'une clé USB comprenant une carte à puce. La mise à jour est alors possible :

- via l'interface série de la carte à puce, débloquée par le code d'accès de l'administrateur autorisé,

- dans le cas où la carte à puce offre des moyens d'accès à un réseau mobile, par exemple par envoi d'un "SMS" (de l'anglais "Short Message Service") signé. La mise à jour de la mémoire est alors effectuée selon un mécanisme de configuration automatique dit "OTA" (de l'anglais "Over The Air"). L'avantage d'une telle mise à jour est qu'elle utilise une interface complètement maîtrisée par un opérateur de téléphonie mobile.

L'administrateur autorisé effectue alors sa mise à jour par l'intermédiaire de l'opérateur.

Le deuxième bloc mémoire 21 est appelé zone système. Ce deuxième bloc 21 comprend un fichier S21 unique compressé, signé numériquement au moyen d'une clé privée propre à un administrateur autorisé. De manière classique, une clé publique permettant une vérification de ladite signature numérique est associée à la clé privée de signature. Le fichier S21 comprend notamment des données nécessaires au démarrage du système d'exploitation sur le terminal hôte ainsi qu'à la lecture et l'exploitation de données stockées dans les blocs mémoire 22 et 23. En particulier, le fichier S21 comprend :

- le noyau du système d'exploitation destiné à être lancé sur le terminal hôte,

- un pilote de gestion de données adapté pour construire un système de fichiers pour l'accès à des données stockées dans les blocs 22 et 23 de la mémoire,

- un pilote de périphérique adapté pour la saisie d'un mot de passe sur le clavier du terminal hôte, ou d'une donnée d'authentification de l'utilisateur,

Une signature numérique du fichier S21 est stockée dans la mémoire de manière à permettre la vérification de l'intégrité du fichier S21. Cette signature est stockée dans la zone système, par exemple en début du bloc mémoire 21, de manière à être facilement accessible. La clé publique de l'administrateur autorisé qui a signé le fichier S21 est stockée dans le bloc mémoire 20 correspondant à la zone de boot. Ainsi, la clé publique de l'administrateur est disponible, lors de l'exécution du programme d'amorçage, pour effectuer la vérification de la signature du fichier S21.

Le troisième bloc mémoire 22 correspond à une zone de configuration selon l'invention. Il comprend un fichier de configuration C22 contenant une liste d'identifiants signés de terminaux hôtes potentiels autorisés, pouvant être utilisés via le dispositif externe de stockage 11a (11b). Cette liste est appelée liste blanche. Dans un exemple de réalisation de l'invention, la liste blanche comprend un ensemble d'enregistrements, relatifs à des terminaux hôtes potentiels respectifs et structurés par exemple de la façon suivante :

[*identifiant du terminal* | *identifiant d'un administrateur* | *signature de l'administrateur*] ; le caractère '|' représentant une concaténation.

Le premier champ "identifiant du terminal" est une référence qui permet d'identifier le terminal de façon unique. Il est déterminé à partir de données relatives à des moyens matériels intrinsèques au terminal, c'est-à-dire à partir de caractéristiques ou paramètres concernant des moyens matériels appartenant au terminal. Par exemple, il peut être déterminé à partir d'un ou de plusieurs paramètres parmi lesquels : un numéro de série d'un disque dur, un numéro de série d'un processeur, un numéro de série d'une carte mère, une base de registre, une taille de mémoire, un temps de réponse du système de référence (processeur, connexion réseau, etc.), etc. Une méthode d'homogénéisation des paramètres peut éventuellement être utilisée, par souci de simplification, de sorte que les paramètres choisis pour identifier le terminal appartiennent au même espace de représentation. Cela permet d'avoir un format de codage uniforme pour chacun des paramètres ; une telle homogénéisation peut être obtenue par application de fonctions de hachage à certains des paramètres. Un autre exemple de détermination d'un identifiant unique de terminal est divulguée dans la demande publiée sous le numéro EP1667486.

Un deuxième champ identifiant de l'administrateur autorisé est par exemple un nom de serveur d'administration alloué par l'entreprise et identifiant le serveur d'administration de façon unique, ou un nom d'administrateur, personne physique, ou un identifiant de cet administrateur. Dans ce dernier cas, l'administrateur dispose de moyens informatiques qui lui permettent de faire des opérations d'administration, telles que des signatures, des mises à jour, etc.

La concaténation des champs associés à l'identifiant du terminal et à l'identifiant de l'administrateur est signée numériquement par l'administrateur au moyen d'une clé privée propre à l'administrateur. La signature obtenue est concaténée aux champs précédents pour obtenir l'enregistrement relatif au terminal dans la liste blanche.

Dans une première réalisation de l'invention, la clé publique associée à la clé privée de l'administrateur signataire est stockée dans le premier bloc de mémoire 20 correspondant à la zone d'amorçage.

Dans une deuxième réalisation de l'invention, la clé publique de l'administrateur signataire est stockée dans le deuxième bloc 21 de la mémoire correspondant à la zone système. Dans les deux cas, la clé publique de l'administrateur signataire est accessible lors du lancement du système d'exploitation dont un module est adapté pour vérifier l'intégrité des données relatives à un terminal de la liste blanche des identifiants.

La liste blanche ne peut être modifiée que par un administrateur autorisé pour lequel une clé publique associée à une clé privée de signature est déjà stockée dans le premier bloc 20, ou le deuxième bloc 21.

On remarquera qu'avec cette structure de liste, où chacun des administrateurs signataires est désigné et où chaque enregistrement relatif à un identifiant de terminal est signé par l'administrateur désigné, il est possible d'avoir différents administrateurs signataires d'un ou de plusieurs enregistrements de la liste blanche. Cela peut être intéressant dans une organisation d'entreprise où différents administrateurs sont en charge de différentes applications soumises à des licences logicielles, applications pour lesquelles il est donc nécessaire de vérifier que leur lancement sur un terminal est autorisé, selon les termes de la licence.

Dans une variante de réalisation de l'invention, un enregistrement de la liste blanche relatif à un terminal hôte particulier, comprend, outre l'identifiant de terminal et l'identifiant de l'administrateur, une information temporelle de validité, par exemple une date limite, qui permet à l'administrateur signataire de préciser qu'un dispositif peut être utilisé sur le terminal particulier pendant une durée limitée et jusqu'à la date limite. La concaténation de ces trois champs est signée par l'administrateur signataire. Cette variante est utile, d'une part pour prendre en compte des dates limites d'utilisation dans des licences logicielles et d'autre part, pour s'affranchir d'une mise à jour de la liste sur le dispositif 11a, 11b lorsque la date limite d'utilisation d'une licence logicielle est arrivée.

Le quatrième bloc 23 correspond à la zone utilisateur. De manière, classique, cette zone de la mémoire comprend des fichiers personnels de l'utilisateur. L'ensemble des données et/ou fichiers de la zone utilisateur est stocké sous forme d'un fichier F23 unique, chiffré et de préférence compressé. La zone utilisateur est débloquée par un mot de passe connu uniquement de l'utilisateur.

Les troisième et quatrième blocs de mémoire 22, 23 sont de préférence réinscriptibles, réalisés par exemple par des mémoires de type flash.

Les étapes d'un procédé d'utilisation du terminal hôte 10a par le dispositif externe de stockage 11a connecté audit terminal 10a, selon un mode particulier de réalisation de l'invention, vont maintenant être décrites en relation avec la figure 3.

Le procédé d'utilisation du terminal hôte 10b via le dispositif externe de stockage 11b est analogue la description qui suit.

Dans une étape initiale u30, un utilisateur 30, porteur du dispositif externe de stockage 11a insère ce dispositif 11a, dans le port USB du terminal 10a.

Dans une étape de démarrage u31, l'utilisateur 30 démarre le terminal 10a, ici par mise sous tension.

Dans une étape t30 de lancement du système de base des entrées/sorties, le programme BIOS du terminal 10a s'exécute et recherche un programme d'amorçage. De manière connue, le programme BIOS exécute une procédure de détection des périphériques du terminal hôte 10a, pouvant être des périphériques internes au terminal et permanents, ou bien des périphériques externes et amovibles, connectés à ce terminal. Puis, il recherche parmi les périphériques détectés, en respectant un ordre prédéfini par une liste de démarrage, le premier périphérique contenant un secteur d'amorçage comprenant un programme d'amorçage de système d'exploitation. De façon standard, la liste de démarrage prescrit d'interroger les périphériques connectés au bus USB avant le périphérique interne constitué par le disque dur du terminal hôte 10a. Par conséquent, dans l'invention, c'est la zone de démarrage

du dispositif externe de stockage 11a qui est détectée en premier et utilisée en priorité par rapport à un ou plusieurs disques durs éventuellement présents dans le terminal hôte 10a.

Le programme BIOS est inscrit dans une mémoire morte du terminal hôte 10a ; il n'est pas modifiable.

Dans une étape d30, le dispositif externe 11a réagit à la procédure de détection lancée par le terminal hôte 10a. Le programme BIOS du terminal 10a détecte la présence d'une mémoire de stockage sur le dispositif de stockage externe 11a. Le programme BIOS accède en lecture à la mémoire de stockage puis déclenche l'exécution du programme d'amorçage stocké dans la zone d'amorçage de la mémoire du dispositif 11a.

Dans une étape t31 d'exécution, le terminal 10a exécute le programme d'amorçage.

Dans une étape d31, le programme d'amorçage accède en lecture à la zone système de la mémoire du dispositif 11a.

Dans une étape de test t32, le programme d'amorçage vérifie la signature du fichier S21 qui est stocké dans le bloc mémoire 21 du dispositif 11a, au moyen d'une clé publique stockée dans le bloc mémoire 20 correspondant à la zone d'amorçage. Dans le cas où la signature n'est pas valide, alors le procédé se termine. Si la signature est valide, alors, dans une étape t33, le noyau système est chargé dans une mémoire vive du terminal 10a et exécuté. En particulier, le système de fichiers permettant d'accéder à des données stockées dans les blocs mémoire 22 et 23 est construit. L'exécution du noyau système comprend l'exécution d'une routine selon l'invention qui provoque l'accès à la zone de configuration stockée dans le bloc mémoire 22 du dispositif 11a, 11b.

Dans une étape d32, la routine accède en lecture au fichier de configuration C22 stocké dans le bloc mémoire 22 du dispositif 11a.

Dans une étape t34, le noyau système détermine un identifiant unique du terminal 10a, à partir de caractéristiques et/ou paramètres relatifs à des moyens matériels intrinsèques du terminal. Ces caractéristiques peuvent par exemple être obtenues à l'aide de requêtes au terminal. Une interface du noyau système

peut être utilisée, ou une routine spécifique du noyau aux fins de l'obtention de ces paramètres.

Dans une étape de recherche t35, le noyau système recherche l'identifiant unique qu'il vient de déterminer dans la liste blanche des identifiants de terminaux récupérée dans la zone de configuration à l'étape d32. Si l'identifiant n'est pas trouvé dans la liste blanche, alors une procédure de mise à jour, décrite en relation avec la figure 4 est exécutée.

Si l'identifiant figure dans un enregistrement de la liste blanche, alors dans une étape t36 de vérification, le noyau système vérifie la signature de cet enregistrement qui comprend l'identifiant unique du terminal. Si la vérification de la signature est positive, alors le noyau système déclenche, dans une étape t37, l'exécution d'un module d'authentification conçu pour demander à l'utilisateur 30 de saisir un mot de passe sur le clavier du terminal 10a.

Dans une étape u32, l'utilisateur 30 saisit son mot de passe sur le clavier du terminal 10a, mot de passe qui est ensuite analysé par le module d'authentification afin d'authentifier l'utilisateur du terminal 10a. Les étapes t37 et u32 peuvent éventuellement faire intervenir une carte à puce et un pilote de périphérique nécessaire au fonctionnement de cette carte à puce. En cas d'échec de l'authentification, le procédé s'arrête, à moins que l'utilisateur 30 ne soit autorisé à effectuer plusieurs tentatives d'authentification. De préférence, en cas d'échec, le démarrage complet du système d'exploitation sur le terminal 10a est interrompu de manière à ce qu'un utilisateur non authentifié ne soit pas en mesure d'utiliser le terminal.

Dans une étape t38, en cas d'authentification réussie, le pilote de gestion de données obtient une clé de déchiffrement des données de la zone utilisateur correspondant au bloc mémoire 23. Cette clé de déchiffrement est obtenue soit par interrogation de la carte à puce, conditionnellement à la présentation d'un mot de passe valide, soit par déchiffrement, au moyen du mot de passe fourni, d'une clé de déchiffrement stockée chiffrée dans la zone utilisateur. Le mot de passe fourni par l'utilisateur est également utilisable comme clé pour le chiffrement/déchiffrement des données de la zone utilisateur. Le pilote de gestion de données utilise la clé de déchiffrement pour déchiffrer le fichier F23

stocké chiffré dans la zone utilisateur. Le pilote construit ensuite dans une mémoire vive du terminal 10a, une structure logique de fichiers, sous forme d'arborescence des répertoires et fichiers, à partir de tout ou partie des données contenues dans le fichier F23 déchiffré. Les fichiers de cette arborescence sont ainsi accessibles par l'utilisateur selon des droits de lecture, écriture, exécution propres aux fichiers. Par exemple, l'utilisateur peut lancer un logiciel soumis à licence sur le terminal 10a puisqu'il a été vérifié lors d'étapes précédemment décrites que le terminal 10a était un terminal autorisé pour le dispositif 11a, notamment pour le lancement d'applications de l'utilisateur.

Dans une étape d34, à la demande du système d'exploitation qui s'exécute sur le terminal 10a, et suite à des commandes de l'utilisateur 30, le dispositif 11a lit et écrit dans la zone utilisateur.

Une procédure de mise à jour de la liste blanche des identifiants de terminaux autorisés va maintenant être décrite en relation avec la figure 4.

Cette procédure correspond à une mise à jour de la liste blanche des identifiants, dite en mode connecté (le terme couramment utilisé est le terme anglais "online"), car soumise à des conditions d'accès au réseau comme décrit ultérieurement. Cette procédure est exécutée à chaque fois qu'un identifiant de terminal n'est pas trouvée dans la liste blanche au cours de l'étape t35 selon la figure 3. Elle consiste à interroger un administrateur pour savoir s'il autorise l'utilisation du terminal 10a, par le dispositif 11a. Le cas échéant, l'identifiant du terminal 10a est ajouté à la liste blanche des terminaux autorisés qui figure dans le fichier C22 du troisième bloc mémoire 22.

Une mise à jour en mode déconnecté, c'est-à-dire sans condition préalable d'accès au réseau, existe et a déjà été présentée précédemment. Elle consiste à mettre à jour la liste blanche directement dans la mémoire du dispositif.

Si, au cours de l'étape de recherche t35 selon la figure 3 qui apparaît en pointillés sur la figure 4, l'identifiant du terminal n'est pas trouvé dans la liste blanche des terminaux autorisés, alors, dans une étape d'envoi t40, l'identifiant du terminal déterminé à l'étape t34 est envoyé à un administrateur 40. On

rappelle qu'un administrateur est assimilé à un serveur d'administration. A cette fin, un module de mise à jour de la liste blanche du système d'exploitation établit une connexion réseau avec l'administrateur 40. Par exemple, le module de mise à jour de la liste blanche utilise une connexion Ethernet du terminal 10a au réseau de l'entreprise. Dans un autre exemple de réalisation où le dispositif est couplé à une carte SIM, le module de mise à jour de la liste blanche utilise une connexion radio-cellulaire.

Dans une étape a40 de vérification d'autorisation, l'administrateur 40 détermine s'il autorise l'utilisation du terminal 10a comme terminal hôte pour démarrer le système d'exploitation contenu dans le dispositif 11a. Par exemple, l'administrateur 40 autorise l'utilisation du terminal 10a si celui-ci appartient au parc de terminaux de l'entreprise. Dans un autre exemple de réalisation, le lancement d'un système d'exploitation depuis le dispositif externe 11a est autorisé sur un nombre maximum prédéfini de terminaux. Si le nombre maximum prédéfini de terminaux hôtes n'est pas atteint, alors le lancement du système d'exploitation du dispositif 11a sur le terminal 10a est autorisé. Si l'utilisation du terminal 10a n'est pas autorisée, alors l'administrateur 40 renvoie au module de mise à jour de la liste blanche en cours d'exécution sur le terminal 10a un message de refus non représenté, ce qui interrompt le lancement du système d'exploitation.

Dans une étape a41 d'envoi d'une mise à jour, consécutive à une vérification d'autorisation positive, l'administrateur 40 renvoie au module de mise à jour de la liste blanche en cours d'exécution sur le terminal 10a un nouvel enregistrement relatif au terminal 10a signé au moyen de sa clé privée de signature.

Dans une étape t41 de mise à jour, le module de mise à jour de la liste blanche met à jour la liste blanche chargée dans la mémoire vive du terminal 10a, 10b en ajoutant à la liste blanche le nouvel enregistrement reçu de l'administrateur 40.

REVENDICATIONS

1. Procédé d'utilisation d'un terminal hôte à l'aide d'un dispositif externe connecté au terminal et hébergeant au moins un programme, comprenant :

- lors d'une phase de démarrage du terminal, une étape (t33) de démarrage de l'exécution du programme hébergé par le dispositif externe, sur le terminal hôte,

caractérisé par le fait que, le dispositif externe mémorisant une liste, dite "liste blanche", d'identifiants de terminaux autorisés, il est prévu :

- une étape (t34) de détermination, par le programme du dispositif externe, d'un identifiant du terminal à partir de données relatives à des moyens matériels intrinsèques du terminal,

- une étape (t35) de vérification de l'identifiant déterminé, au cours de laquelle le programme du dispositif externe vérifie l'appartenance de l'identifiant déterminé à la liste blanche,

l'exécution du programme étant poursuivie si la vérification de l'identifiant est positive.

2. Procédé selon la revendication 1, dans lequel, le dispositif externe stockant un programme d'amorçage et un système d'exploitation, il est prévu, lors de la phase de démarrage du terminal,

- une étape (t31) d'exécution dudit programme d'amorçage accessible via le dispositif externe.

- l'exécution dudit programme d'amorçage déclenchant l'étape (t33) de démarrage du système d'exploitation.

3. Procédé selon la revendication 2, comprenant en outre une étape (t32) de vérification de l'intégrité du système d'exploitation hébergé par le dispositif externe, réalisée par le programme d'amorçage, l'étape (t33) de démarrage de l'exécution du système d'exploitation étant exécutée, seulement si la vérification est positive.

4. Procédé selon la revendication 1, comprenant :

- si la vérification de l'identifiant est négative, une étape (t40) d'envoi dudit identifiant vers un administrateur,

- une étape (a40) de contrôle de l'identifiant par l'administrateur afin de déterminer s'il est autorisé,

- si le contrôle est positif, une étape (a41) d'envoi par l'administrateur dudit identifiant vers le système d'exploitation, et

- une étape (t41) d'enregistrement dudit identifiant dans la liste blanche d'identifiants autorisés.

5. Procédé selon la revendication 1, dans lequel la liste blanche d'identifiants autorisés comprend en outre, pour au moins un identifiant, une information temporelle de validité.

6. Dispositif (11a, 11b) apte à connecté à un terminal hôte, comprenant des moyens de stockage contenant :

- au moins un programme,

- une liste dite "liste blanche" d'identifiants de terminaux hôtes autorisés,

ledit programme étant apte, au démarrage de son exécution, à

- déterminer un identifiant d'un terminal hôte auquel ledit dispositif est connecté, à partir de données relatives à des moyens matériels intrinsèques du terminal
- vérifier l'appartenance de l'identifiant déterminé à la liste blanche,
- poursuivre son exécution seulement si la vérification est positive.

7. Dispositif selon la revendication 6, dans lequel les moyens de stockage comprennent un programme d'amorçage et un système d'exploitation, ledit programme d'amorçage vérifiant au démarrage de son exécution l'intégrité du système d'exploitation hébergé par le dispositif externe, le démarrage de

l'exécution du système d'exploitation ne s'exécutant que si la vérification est positive.

8. Dispositif selon la revendication 6, dans lequel ledit programme est apte, si la vérification de l'identifiant est négative, à :

- envoyer ledit identifiant vers un administrateur apte à déterminer si ledit identifiant est autorisé, et le cas échéant, à renvoyer ledit identifiant,
- recevoir ledit identifiant,
- si le contrôle est positif, une étape (a41) d'envoi par l'administrateur dudit identifiant vers le système d'exploitation, et
- enregistrer ledit identifiant dans la liste blanche des identifiants de terminaux hôtes autorisés.

9. Programme destiné à être installé dans une mémoire d'un dispositif de stockage adapté pour être connecté à un terminal hôte, ledit dispositif mémorisant une liste, dite "liste blanche", d'identifiants de terminaux autorisés, et comprenant des portions de code pour :

- déterminer un identifiant du terminal hôte à partir de données relatives à des moyens matériels intrinsèques du terminal,
- vérifier l'appartenance de l'identifiant déterminé à la liste blanche,
- poursuivre son exécution si la vérification de l'identifiant est positive.

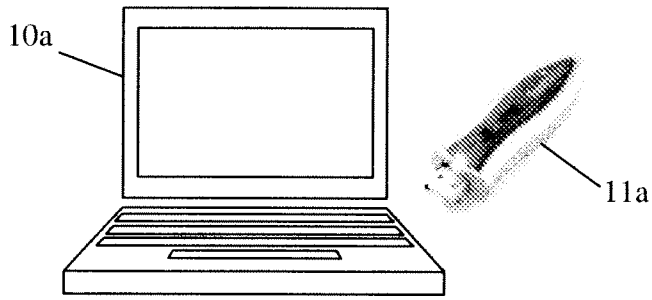

Figure 1a

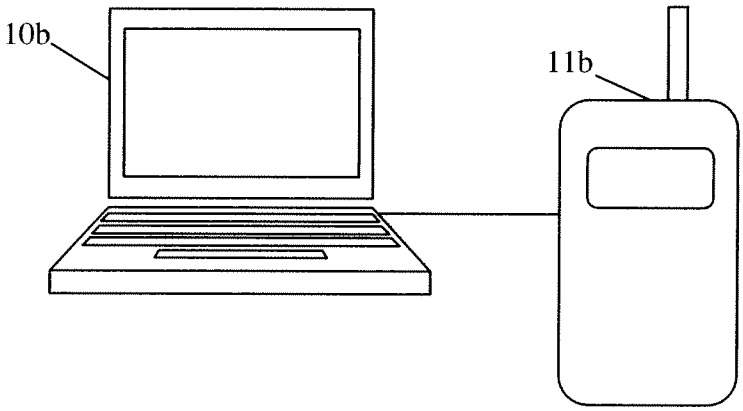

Figure 1b

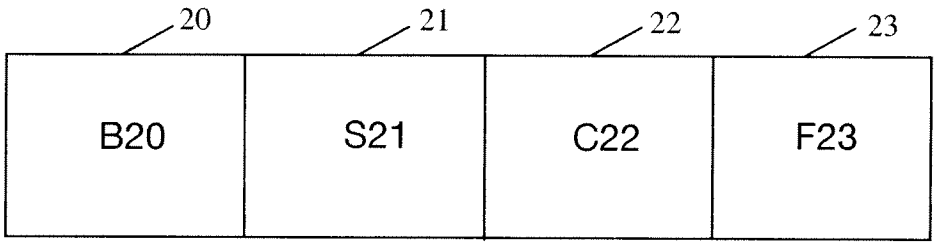

Figure 2

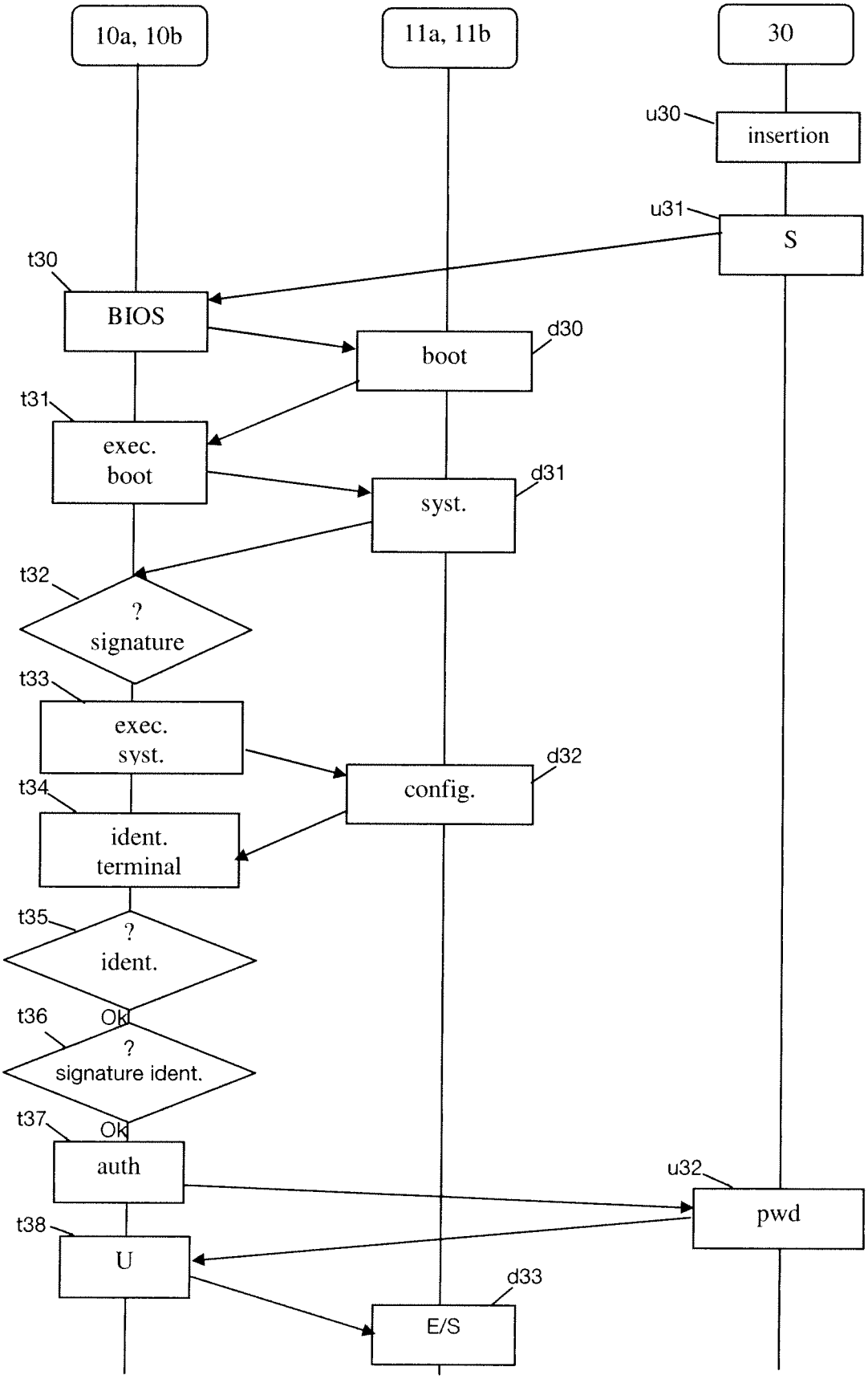
10a, 10b
11a, 11b
30
u30
insertion
u31
S
t30
BIOS
boot
d30
t31
exec.
boot
syst.
d31
t32
?
signature
t33
exec.
syst.
config.
d32
t34
ident.
terminal
t35
?
ident.
t36
Ok
?
signature ident.
t37
Ok
auth
u32
pwd
t38
U
E/S
d33

Figure 3

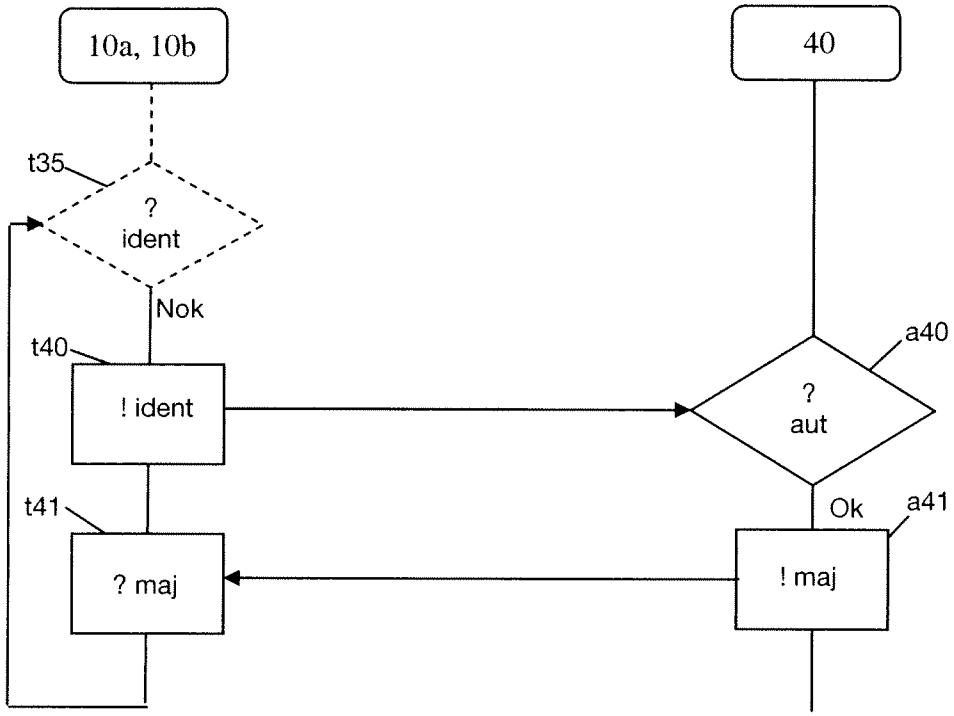

Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/050717

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BRAD BERGERON: "HOWTO: Install and Boot OS X On a Flash Drive" INTERNET ARTICLE, [Online] 29 November 2006 (2006-11-29), pages 1-23, XP002505116 Online Retrieved from the Internet: URL:http://blog.bradbergeron.com/2006/11/howto-install-and-boot-os-x-on-a-flash-drive/> [retrieved on 2008-11-20] Page 7, alinèa "Booting From the Flash Drive". Les remarques (pages 7-23) ne font pas partie de ce document. ----- -/--	1-9

[X] Further documents are listed in the continuation of Box C.

[X] 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
24 septembre 2009	01/10/2009

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, Fax: (+31-70) 340-3016	Alecu, Mihail

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/050717

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ARMIT SINGH: ""TPM DRM" In Mac OS X: A Myth That Won't Die" INTERNET ARTICLE, [Online] 6 February 2008 (2008-02-06), pages 1-9, XP002505117 Online Retrieved from the Internet: URL:http://web.archive.org/web/20080206090115/http://www.osxbook.com/book/bonus/chapter7/tpmdrmmyth/> [retrieved on 2008-11-21] page 1, last paragraph page 2 - alinéa "The Key to Understanding: Simple Minded Calculations"	1-9
X	US 2007/288886 A1 (MENSCH JAMES [US] ET AL) 13 December 2007 (2007-12-13) the whole document	1-9
A	AMIT SINGH: "Trusted Computing for Mac OS X" INTERNET ARTICLE, [Online] 6 January 2007 (2007-01-06), pages 1-12, XP002505118 Online Retrieved from the Internet: URL:http://web.archive.org/web/20070106150844/http://www.osxbook.com/book/bonus/chapter10/tpm/> [retrieved on 2008-11-21] the whole document	1-9
A	WO 01/61591 A (SONY ELECTRONICS INC [US]) 23 August 2001 (2001-08-23) abstract	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2009/050717

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007288886 A1	13-12-2007	NONE	
WO 0161591 A	23-08-2001	AU 3464301 A	27-08-2001
		US 2006271492 A1	30-11-2006
		US 7225164 B1	29-05-2007

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/050717

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 est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	BRAD BERGERON: "HOWTO: Install and Boot OS X On a Flash Drive" INTERNET ARTICLE, [Online] 29 novembre 2006 (2006-11-29), pages 1-23, XP002505116 Online Extrait de l'Internet: URL:http://blog.bradbergeron.com/2006/11/howto-install-and-boot-os-x-on-a-flash-drive/> [extrait le 2008-11-20] Page 7, alinèa "Booting From the Flash Drive". Les remarques (pages 7-23) ne font pas partie de ce document. ----- -/--	1-9

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention 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
24 septembre 2009	01/10/2009

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, Fax: (+31-70) 340-3016	Alecu, Mihail

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/050717

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	ARMIT SINGH: ""TPM DRM" In Mac OS X: A Myth That Won't Die" INTERNET ARTICLE, [Online] 6 février 2008 (2008-02-06), pages 1-9, XP002505117 Online Extrait de l'Internet: URL:http://web.archive.org/web/20080206090115/http://www.osxbook.com/book/bonus/chapter7/tpmdrmmyth/> [extrait le 2008-11-21] page 1, dernier alinéa page 2 - alinéa "The Key to Understanding: Simple Minded Calculations"	1-9
X	US 2007/288886 A1 (MENSCH JAMES [US] ET AL) 13 décembre 2007 (2007-12-13) le document en entier	1-9
A	AMIT SINGH: "Trusted Computing for Mac OS X" INTERNET ARTICLE, [Online] 6 janvier 2007 (2007-01-06), pages 1-12, XP002505118 Online Extrait de l'Internet: URL:http://web.archive.org/web/20070106150844/http://www.osxbook.com/book/bonus/chapter10/tpm/> [extrait le 2008-11-21] le document en entier	1-9
A	WO 01/61591 A (SONY ELECTRONICS INC [US]) 23 août 2001 (2001-08-23) abrégé	1-9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2009/050717

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2007288886 A1	13-12-2007	AUCUN	
WO 0161591 A	23-08-2001	AU 3464301 A	27-08-2001
		US 2006271492 A1	30-11-2006
		US 7225164 B1	29-05-2007