(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 959 632**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **10 53429**

(51) Int Cl[8] : ***H 04 L 12/12*** *(2006.01), G 06 F 21/22*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 03.05.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.11.11 Bulletin 11/44.

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

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

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

(72) **Inventeur(s) :** DEDIEU GERARD.

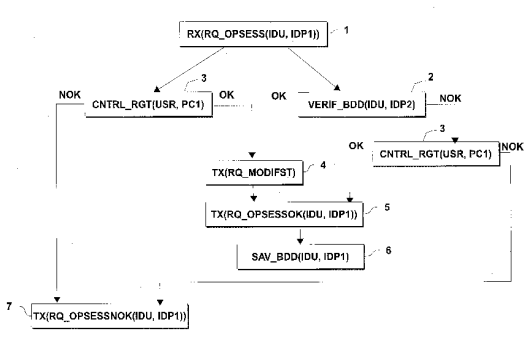
(73) **Titulaire(s) :** EVIDIAN Société anonyme.

(74) **Mandataire(s) :** CABINET CAMUS LEBKIRI.

(54) PROCEDE D'OUVERTURE DE SESSION D?UNE MACHINE APPARTENANT A UN PARC DE MACHINES.

(57) La présente invention concerne un procédé d'ouverture de session d'une première machine par un service de contrôle de sessions pour un parc de machines comprenant au moins ladite première machine et une deuxième machine, ladite deuxième machine comportant un service de sécurité. Le procédé comportant les étapes de:

- recevoir par le service de contrôle de sessions une requête d'ouverture de session de ladite première machine, ladite requête comprenant au moins une information d'identification d'un utilisateur;
- vérifier par le service de contrôle de sessions si ladite au moins information d'identification dudit utilisateur est associée dans un référentiel à une donnée d'identification de ladite deuxième machine;
- contrôler par le service de contrôle de sessions si l'utilisateur a le droit d'ouvrir une session sur la première machine;
- dans l'affirmative de ladite vérification et dudit contrôle, envoyer par le service de contrôle de sessions audit service de sécurité de ladite deuxième machine une requête de modification d'état de session de ladite deuxième machine; et
- si la modification d'état de session de la deuxième machine se réalise, envoyer par le service de contrôle de sessions à la première machine une requête d'autorisation d'ouverture de session; et
- sauvegarder dans ledit référentiel par le service de contrôle de sessions ladite au moins information d'identification dudit utilisateur associée à une donnée d'identification de ladite première machine.



FR 2 959 632 - A1

PROCEDE D'OUVERTURE DE SESSION D'UNE MACHINE APPARTENANT A UN PARC DE MACHINES

DOMAINE TECHNIQUE DE L'INVENTION

La présente invention concerne un procédé d'ouverture de session d'une première machine par un service de contrôle de sessions. L'invention concerne également un service de contrôle de sessions apte à mettre en œuvre le procédé d'ouverture de session.

Elle trouve une application particulière, mais non limitative, dans le domaine hospitalier.

ARRIÈRE-PLAN TECHNOLOGIQUE DE L'INVENTION

Un procédé d'ouverture de session d'une première machine par un service de contrôle de sessions, connu de l'homme du métier, permet d'ouvrir une session par un utilisateur avec son identifiant utilisateur (couramment appelé en anglais « login ») qui comprend en général un nom d'utilisateur et un mot de passe associé.

Dans le domaine hospitalier, un parc de machines comprenant une pluralité de machines est couramment utilisé. Les différentes machines comprennent des applications communes et une machine peut également comprendre une ou plusieurs applications qui lui est propre.
Plusieurs opérateurs tels que les médecins ou les infirmières peuvent avoir accès aux différentes machines afin d'accéder aux applications communes et aux applications propres à chaque machine. Pour y accéder ils ouvrent une session avec leur « login ».
Ainsi, dans une journée, un opérateur peut ouvrir une session utilisateur sur plusieurs machines du parc de machines.

Un inconvénient de cet état de la technique est que souvent un opérateur oublie de sortir de sa session après utilisation de la machine. En conséquence, un autre opérateur peut utiliser les applications de la machine

via une session utilisateur qui n'est pas la sienne et a donc accès à des applications de manière non autorisée.

DESCRIPTION GENERALE DE L'INVENTION

La présente invention a pour but un procédé d'ouverture de session d'une première machine par un service de contrôle de sessions, qui permette de résoudre le problème énoncé ci-dessus.

Ce but est atteint par un procédé d'ouverture de session d'une première machine par un service de contrôle de sessions pour un parc de machines comprenant au moins ladite première machine et une deuxième machine, ladite deuxième machine comportant un service de sécurité, le procédé comportant les étapes de :

- recevoir par le service de contrôle de sessions une requête d'ouverture de session de ladite première machine, ladite requête comprenant au moins une information d'identification d'un utilisateur ;
- vérifier par le service de contrôle de sessions si ladite au moins information d'identification dudit utilisateur est associée dans un référentiel à une donnée d'identification de ladite deuxième machine ;
- contrôler par le service de contrôle de sessions si l'utilisateur a le droit d'ouvrir une session sur la première machine ;
- dans l'affirmative de ladite vérification et dudit contrôle, envoyer par le service de contrôle de sessions audit service de sécurité de ladite deuxième machine une requête de modification d'état de session de ladite deuxième machine ; et
- si la modification d'état de session de la deuxième machine se réalise, envoyer par le service de contrôle de sessions à la première machine une requête d'autorisation d'ouverture de session ; et
- sauvegarder dans ledit référentiel par le service de contrôle de sessions ladite au moins information d'identification dudit utilisateur associée à une donnée d'identification de ladite première machine.

Comme on va le voir en détail par la suite, le fait de vérifier si un utilisateur a déjà une session d'ouverte sur une autre machine et de modifier son état de session avant de permettre d'ouvrir une autre session sur une autre machine permet de sécuriser la machine qui n'est plus utilisée par l'utilisateur.

Selon des modes de réalisation non limitatifs, le procédé peut comporter en outre une ou plusieurs caractéristiques supplémentaires parmi les suivantes :

- La requête de modification d'état de session est de type verrouillage de session ou fermeture de session.

- Le type d'une requête de modification d'état de session est paramétré dans le service de contrôle de session. Ainsi, la fermeture ou le verrouillage d'une session sur la deuxième machine est décidé en amont par un administrateur du parc de machine.

- Le procédé comporte une étape supplémentaire d'envoyer par la première machine au service de contrôle de session une requête de paramétrage comprenant le type de la requête de modification d'état de session. Ainsi, le choix est laissé à l'utilisateur qui accède à la première machine de verrouiller ou fermer la session ouverte sur la deuxième machine.

- Le procédé comporte une étape supplémentaire d'envoyer par le service de contrôle de sessions audit service de sécurité de ladite deuxième machine une requête de modification d'état de session de ladite deuxième machine qui est de type verrouillage de session si la modification d'état de session de la deuxième machine correspondant à une fermeture de session échoue. Cela permet de sécuriser la deuxième machine en verrouillant la session ouverte sur cette machine, même si la fermeture de session échoue.

- Une requête reçue ou émise par le service de contrôle de sessions est une requête TCP/IP ou UDP. Cela permet une communication entre deux machines d'un même réseau informatique.

- Le procédé il comporte une étape supplémentaire d'envoyer un message applicatif de modification d'état de session correspondant à la requête de modification d'état de session à un module de gestion de session de la deuxième machine. Cela permet au module de gestion de session de procéder au verrouillage/fermeture de la deuxième machine.

- Le procédé comporte une étape supplémentaire d'envoyer un message applicatif de modification d'état de session correspondant à la requête de modification d'état de session à un greffon d'un module de gestion de session de la deuxième machine. Cela évite de modifier l'interface utilisateur de gestion de session qui est comprise dans le module de gestion de session de la deuxième machine.

- Les étapes de vérification et d'envoi de la requête de modification d'état de session sont effectuées pour toute machine appartenant au parc de machines et différente de la première machine. Cela permet de sécuriser l'ensemble des machines du parc de machines sur lesquelles une session de l'utilisateur est ouverte.

L'invention concerne également un service de contrôle de sessions pour un parc de machines apte à effectuer une ouverture de session d'une première machine, ledit parc de machines comprenant au moins ladite première machine et une deuxième machine, ladite deuxième machine comportant un service de sécurité, ledit service de contrôle de sessions étant apte à :

- recevoir une requête d'ouverture de session de ladite première machine, ladite requête comprenant au moins une information d'identification d'un utilisateur ;
- vérifier si ladite au moins information d'identification dudit utilisateur est associée dans un référentiel à une donnée d'identification de ladite deuxième machine ;
- contrôler si l'utilisateur a le droit d'ouvrir une session sur la première machine ;

- dans l'affirmative de ladite vérification et dudit contrôle, envoyer audit service de sécurité de ladite deuxième machine une requête de modification d'état de session de ladite deuxième machine ;
- si la modification d'état de session de la deuxième machine se réalise, envoyer à la première machine une requête d'autorisation d'ouverture de session ; et
- sauvegarder dans ledit référentiel par le service de contrôle de sessions ladite au moins information d'identification dudit utilisateur associée à une donnée d'identification de ladite première machine.

L'invention concerne également une machine de gestion d'un parc de machines apte à effectuer une ouverture de session d'une première machine par un service de contrôle de sessions pour ledit parc de machines comprenant au moins ladite première machine et une deuxième machine, ladite deuxième machine comportant un service de sécurité, ladite machine de gestion comprenant ledit service de contrôle de sessions selon la caractéristique précédente.

L'invention concerne également un système informatique apte à effectuer une ouverture de session d'une première machine par un service de contrôle de sessions pour un parc de machines comprenant au moins ladite première machine et une deuxième machine, ladite deuxième machine comportant un service de sécurité, ledit système comprenant :
- le service de contrôle de sessions selon la caractéristique précédente apte à coopérer avec la première machine et la deuxième machine ;
- ladite deuxième machine apte à recevoir du service de contrôle de sessions via ledit service de sécurité une requête de modification d'état de session ; et
- ladite première machine apte à :
  - émettre une requête d'ouverture de session vers ledit service de contrôle de sessions ; et
  - si la modification d'état de session de la deuxième machine se réalise, recevoir dudit service de contrôle de sessions une requête d'autorisation d'ouverture de session.

Selon un mode de réalisation non limitatif, le module de gestion de session de la deuxième machine comporte un greffon.

L'invention et ses différentes applications seront mieux comprises à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent.

BREVE DESCRIPTION DES FIGURES

Celles-ci ne sont présentées qu'à titre indicatif et nullement limitatif de l'invention.

- La Fig.1a est un organigramme du procédé d'ouverture de session selon l'invention selon un premier mode de réalisation non limitatif ;
- La Fig.1b est un organigramme du procédé d'ouverture de session de la Fig. 1a comprenant en outre deux étapes supplémentaires ;
- La Fig.1c est un organigramme du procédé d'ouverture de session de la Fig. 1b comprenant une étape supplémentaire de paramétrage d'un type de requête de modification de session ;
- La Fig.1d est un organigramme du procédé d'ouverture de session selon l'invention selon un deuxième mode de réalisation non limitatif ;
- La Fig.2a est une première représentation schématique d'un système informatique selon un premier mode de réalisation, comprenant une première machine, une deuxième machine, et un service de contrôle de sessions compris dans une machine de gestion, le service de contrôle de sessions étant apte à mettre en œuvre le procédé d'ouverture de session des figures 1a à 1c ;
- La Fig.2b est une représentation schématique d'un système informatique selon un deuxième mode de réalisation, comprenant une première machine, une deuxième machine, et un service de contrôle de sessions compris dans la deuxième machine, le service de contrôle de sessions étant apte à mettre en œuvre le procédé d'ouverture de session des figures 1a à 1c ;
- La Fig.3 illustre schématiquement des échanges de requêtes et de messages entre une première machine et un service de contrôle de sessions du système informatique de la Fig. 2a, selon un mode de

réalisation non limitatif du procédé d'ouverture de session des figures 1a à 1c ;

- La Fig.4 est une deuxième représentation schématique d'un système informatique selon le premier mode de réalisation de la Fig.2a ; et
- La Fig.5 est une deuxième représentation schématique d'un système informatique selon le deuxième mode de réalisation de la Fig.2a.

DESCRIPTION DE MODES DE REALISATION DE L'INVENTION

Le procédé d'ouverture de session d'une première machine par un service de contrôle de sessions d'un parc de machines comprenant au moins ladite première machine et une deuxième machine, ladite deuxième machine comportant un service de sécurité, est décrit dans un mode de réalisation non limitatif aux figures 1a à 1d.

Le procédé d'ouverture de session est mis en œuvre par un service de contrôle de sessions SRV représenté à la Fig. 2a et à la Fig. 2b.

Par machine, on entend tout matériel informatique comprenant une interface utilisateur par laquelle un utilisateur peut s'authentifier avec son identifiant et son mot de passe (couramment appelé « login » en anglais). Dans des exemples non limitatifs, une machine peut être un poste de travail individuel ou un serveur.

Dans un premier mode de réalisation illustré sur la Fig. 2a, ce service de contrôle de sessions SRV est compris dans une machine de gestion MGN du parc de machines. Cette dernière fait partie d'un système informatique SYS comprenant également la première machine PC1 et la deuxième machine PC2.

Dans un deuxième mode de réalisation illustré sur la Fig. 2b, ce service de contrôle de sessions SRV est compris dans la deuxième machine PC2. Ce deuxième mode évite d'avoir une machine de gestion MGN supplémentaire telle qu'un serveur.

Lorsqu'un utilisateur USR veut accéder à la deuxième machine PC2, il se connecte sous une session utilisateur qui lui est propre via un identifiant

qui lui est propre et un mot de passe associé, le tout formant le « login ». La connexion (appelée également ouverture d'une session) se fait via une interface utilisateur de gestion de session UI2 qui est un composant de l'interface utilisateur (non représentée) de la machine.

Dans la suite de la description, on utilisera indifféremment le terme session utilisateur ou le terme session.

Lorsque le même utilisateur USR veut accéder à la première machine PC1, il se connecte sous une session utilisateur qui lui est propre via le même « login ». La connexion (appelée également ouverture d'une session sur la machine) se fait via une interface utilisateur de gestion de session UI1 qui est un composant de l'interface utilisateur (non représentée) de la machine.

Lors de cet essai de connexion qui correspond à une demande d'ouverture de session DDE_OPSESS de la part de l'utilisateur, la première machine PC1 émet une requête d'ouverture de session RQ_OPSESS vers le service de contrôle de sessions SRV.

A ce moment, le procédé d'ouverture de session est mis en œuvre.

Il comporte les étapes suivantes, telles qu'illustrées à la Fig. 1.

- recevoir par le service de contrôle de sessions SRV une requête d'ouverture de session RQ_OPSESS de ladite première machine PC1, ladite requête comprenant au moins une information d'identification IDU d'un utilisateur USR (étape RX(RQ_OPSESS(IDU, IDP1))) ;
- vérifier par le service de contrôle de sessions SRV si ladite au moins information d'identification IDU dudit utilisateur USR est associée dans un référentiel BDD à une donnée d'identification IDU de ladite deuxième machine PC2 (étape VERIF_BDD(IDU, IDP2)) ;
- contrôler par le service de contrôle de sessions SRV si l'utilisateur USR a le droit d'ouvrir une session sur la première machine PC1 (étape CNTRL_RGT(USR, PC1)) ;
- dans l'affirmative de ladite vérification et dudit contrôle, envoyer par le service de contrôle de sessions SRV audit service de sécurité SES2 de ladite deuxième machine PC2 une requête de modification d'état de session

RQ_MODIFST de ladite deuxième machine PC2 (étape TX(RQ_MODIFST)) ;

- si la modification d'état de session de la deuxième machine PC2 se réalise, envoyer par le service de contrôle de sessions SRV à la première machine PC1 une requête d'autorisation d'ouverture de session RQ_OPSESSOK (étape TX(RQ_OPSESSOK(IDU, IDP1))) ;
- sauvegarder dans ledit référentiel BDD par le service de contrôle de sessions SRV ladite au moins information d'identification IDU dudit utilisateur USR associée à une donnée d'identification IDP de ladite première machine PC1 (étape SAV_BDD(IDU, IDP1))).

Dans un mode de réalisation non limitatif, la requête de modification d'état de session RQ_MODIFST est de type Tp verrouillage de session (état de session verrouillé, ST = slo) ou fermeture de session (état de session fermé, ST = scl).
On notera qu'on entend par verrouillage d'une machine, le fait de verrouiller une session utilisateur qui est déverrouillée.

Dans un mode de réalisation non limitatif, le procédé d'ouverture de session comporte une étape supplémentaire d'envoyer un message applicatif de modification d'état de session MSG_MODIFST correspondant à la requête de modification d'état de session RQ_MODIFST à un module de gestion de session M2 de la deuxième machine PC2.

Dans un mode de réalisation non limitatif, le procédé d'ouverture de session comporte une étape supplémentaire selon laquelle le module de gestion de session M2 de la deuxième machine PC2 procède à la modification d'état de session de ladite deuxième machine PC2.

Pour la suite de la description, dans le mode de réalisation non limitatif du procédé décrit, le procédé comprend ces modes de réalisation non limitatifs.

Les étapes du procédé d'ouverture de session sont décrites en détail ci-après en se référant aux figures 1b, 2a, 2b, 3, 4 et 5. On notera que les

figures 3 et 4 se réfèrent à la Fig. 2a et la Fig. 5 se réfère à la Fig. 2b. Bien entendu, une figure similaire à la Fig. 3 peut être utilisée pour la Fig. 2b.

On notera que la deuxième machine PC2 comporte une interface utilisateur de gestion de session UI2, cette dernière étant située dans un module de gestion de session M2, tel qu'illustré à la Fig. 2a et à la Fig. 2b.

Dans une première étape 1), le service de contrôle de sessions SRV reçoit une requête d'ouverture de session RQ_OPSESS pour ladite première machine PC1, ladite requête comprenant au moins une information d'identification IDU d'un utilisateur USR.

On notera que cette information d'identification IDU permet d'identifier l'auteur de la demande d'ouverture de session DDE_OPSESS vue précédemment. Dans un exemple non limitatif, cette information d'identification IDU est un identifiant unique associé à l'utilisateur (couramment appelé en anglais « Global Unique Identifier »).

Dans des modes de réalisation non limitatifs, la requête d'ouverture de session RQ_OPSESS est une requête TCP/IP (« Transmition Control Protocol/Internet Protocol » en anglais) ou UDP («User Datagram Protocol » en anglais).

Dans une deuxième étape 2), le service de contrôle de sessions SRV vérifie si ladite au moins information d'identification IDU dudit utilisateur USR est associée dans un référentiel BDD à une donnée d'identification IDU de ladite deuxième machine PC2.

Ainsi, on vérifie dans le référentiel BDD s'il existe un couple IDU, IDP avec le même identifiant unique utilisateur IDU et un identifiant machine IDP qui est différent de la première machine PC1, ici qui est celui de la deuxième machine PC2.
Si c'est le cas, cela signifie que l'utilisateur USR a précédemment ouvert une session sur une autre machine, ici la deuxième machine PC2.

Bien entendu, cela sous-entend que lors de l'ouverture de session qui a été faite précédemment sur la deuxième machine PC2 par l'utilisateur USR, le service de contrôle de sessions SRV avait sauvegardé dans le référentiel BDD une information d'identification de l'utilisateur IDU ainsi qu'une donnée d'identification IDP2 de la deuxième machine PC2 associée.

Dans un mode de réalisation non limitatif, le référentiel BDD est géré par le service de contrôle de session SRV.
Dans le premier mode de réalisation où le service de contrôle de session SRV est compris dans une machine de gestion MGN, le référentiel BDD est compris dans ladite machine de gestion MGN.
Dans le deuxième mode de réalisation où le service de contrôle de session SRV est compris dans la deuxième machine PC2, le référentiel BDD est un référentiel distant.

On notera que la donnée d'identification IDP d'une machine permet d'identifier de manière unique ladite machine. Dans des exemples non limitatifs, une donnée d'identification IDU d'une machine est son nom, son adresse IP, ou encore son identifiant unique couramment appelé en anglais « Global Unique Identifier ».

Dans une troisième étape 3), le service de contrôle de sessions SRV contrôle si l'utilisateur USR a le droit d'ouvrir une session sur la première machine PC1.
On notera que le contrôle de droits d'un utilisateur pour ouvrir une session sur une machine étant connu de l'homme du métier, il n'est pas décrit ici.

Dans une quatrième étape 4), dans l'affirmative de ladite vérification et dudit contrôle (une session d'un utilisateur a été ouverte sur la deuxième machine PC2 et ce même utilisateur a le droit d'ouvrir une session sur la première machine PC1), le service de contrôle de sessions SRV envoie audit service de sécurité SES2 de ladite deuxième machine PC2 une requête de modification d'état de session RQ_MODIFST de ladite deuxième machine PC2.

La requête de modification d'état de session RQ_MODIFST est de type Tp verrouillage de session RQ_MODIFST(slo) ou fermeture de session RQ_MODIFST(scl).

Ainsi, soit la session sur la deuxième machine PC2 sera verrouillée, soit elle sera fermée.

Dans un premier mode de réalisation non limitatif, le type Tp d'une requête de modification d'état de session RQ_MODIFST est paramétré dans le service de contrôle de session SRV (étape 0 appelée PARAM(Tp) telle qu'illustrée en traits discontinus à la Fig. 1c). Ainsi, le choix entre la fermeture ou le verrouillage est effectué lors du paramétrage du service de contrôle de sessions SRV. Cela permet à un administrateur du parc de machines GRP de déterminer en amont si une session ouverte sur une autre machine doit être fermée ou seulement verrouillée.

Dans un deuxième mode de réalisation non limitatif, le choix de la fermeture/verrouillage est donné à l'utilisateur lui-même. Ainsi, l'interface utilisateur de gestion de session UI1 de la première machine PC1 est apte à:

- informer l'utilisateur USR qu'il existe déjà une session ouverte sur la deuxième machine PC2 ; et

- à proposer audit utilisateur USR de choisir entre la fermeture ou le verrouillage de la session sur la deuxième machine PC2. Cela permet à un utilisateur USR de gérer lui-même ses sessions ouvertes sur les autres machines que la première machine PC1.

Ainsi, dans ce deuxième mode, le procédé d'ouverture de session comporte les étapes supplémentaires suivantes, telles qu'illustrées à la Fig. 1c :

- dans l'affirmative de la vérification (il existe une session ouverte sur la deuxième machine PC2), le service de contrôle de session SRV envoie à la première machine PC1, une information de confirmation INF de l'existence d'une session ouverte sur la deuxième machine PC2 (étape 2' appelée TX(INF(IDU, IDP2)) ; et

- suite au choix de l'utilisateur USR de fermer ou verrouiller la session sur la deuxième machine PC2, la première machine PC1 envoie au service de

contrôle de session SRV une requête de paramétrage RQ_PARAM comprenant le type Tp de la requête de modification d'état de session RQ_MODIFST (étape 2'' appelée TX(RQ_PARAM(Tp)), type choisi par l'utilisateur USR.

Ces deux étapes supplémentaires sont effectuées avant l'étape d'envoi de la requête de modification d'état de session RQ_MODIFST.

On notera que dans un mode de réalisation non limitatif, la première machine PC1 comporte à cet effet un service de sécurité SES1, tel qu'illustré sur la Fig. 2a et la Fig. 2b, apte à :

- recevoir l'information de confirmation INF de l'existence d'une session ouverte sur la deuxième machine PC2 ;

- envoyer la requête de paramétrage RQ_PARAM.

Dans des modes de réalisation non limitatifs, une requête de modification d'état de session RQ_MODIFST est une requête TCP/IP (« Transmition Control Protocol/Internet Protocol » en anglais) ou UDP («User Datagram Protocol » en anglais). Dans ce dernier cas, les requêtes sont appelées des datagrammes. Le protocole de communication UDP est un protocole simple qui permet d'envoyer des requêtes à une autre machine sans demande de communication préalable. Bien entendu, d'autres protocoles de communication permettant un envoi de requête entre deux machines peuvent être utilisés.

On notera que le service de sécurité SES2 est une tâche de fond qui fonctionne de façon indépendante d'une session utilisateur, c'est-à-dire même en l'absence d'une session utilisateur.
Ainsi, le fait que le service de sécurité SES2 soit autonome du module utilisateur de gestion de session M2 de la deuxième machine PC2 (module de gestion de session M2 qui gère les sessions utilisateurs) permet d'éviter que ledit service de sécurité SES2 ne s'arrête de fonctionner lorsque ledit module utilisateur de gestion de session M2 n'est plus actif comme c'est le cas avec certains systèmes d'exploitation (non représenté sur les figures) tel que par exemple Windows Vista™ sur lesquels s'appuie ledit module M2.

Par ailleurs, on notera que de manière générale, les droits d'un utilisateur sur une machine sont limités à certain environnement et donc à certaines actions.

Comme le service de sécurité SES2 est indépendant de la session utilisateur, l'interface utilisateur de gestion de session UI2 n'a pas les mêmes droits que ledit service de sécurité SES2 et n'a donc pas accès aux actions exécutées par le service de sécurité SES2.

Les explications données ci-dessus pour le service de sécurité SES2 de la deuxième machine PC2 s'appliquent au service de sécurité SES1 de la première machine PC1.

On notera que si la vérification effectuée à la deuxième étape est négative (aucune session n'a été ouverte sur la deuxième machine PC2), la troisième étape est tout de même effectuée (comme illustré sur les figures 1a à 1d). En effet, les droits de l'utilisateur USR pour ouvrir une session sur la première machine PC1 doivent de toute manière être contrôlés. Les étapes 7) et 8) décrites ci-après sont également effectuées.

Par ailleurs, on notera que si le contrôle effectué à la troisième étape est négatif (l'utilisateur n'a pas les droits pour ouvrir une session sur la première machine PC1), le service de contrôle de sessions SRV envoie à la première machine PC1 une requête d'interdiction d'ouverture de session RQ_OPSESSOK (neuvième étape TX(RQ_OPSESSNOK(IDU, IDP1) illustrée sur les figures 1a à 1d).

Sur réception de la requête de modification d'état de session RQ_MODIFST par le service de sécurité SES2 de la deuxième machine PC2, **dans une cinquième étape 5)**, comme illustré sur les figures 1b, 1c, 1d ou à la Fig.3, ledit service de sécurité SES2 envoie un message applicatif de modification d'état de session MSG_MODIFST correspondant à la requête de modification d'état de session RQ_MODIFST au module de gestion de session M2 de la deuxième machine PC2.

On notera qu'un message applicatif de modification d'état de session MSG_MODIFST est un message applicatif qui est défini en fonction du module de gestion de session M2 de la deuxième machine PC2 et plus particulièrement en fonction de l'interface utilisateur de gestion de session UI2.
Ainsi, par exemple, dans le cas d'une interface utilisateur de gestion de session Windows™, un message de modification d'état de session est une notification généré par Windows. Dans un autre exemple, dans le cas d'une interface utilisateur de gestion de session Linux™, un message de modification d'état de session est un événement généré par Linux™.

Dans un premier mode de réalisation non limitatif, le message applicatif de modification d'état de session MSG_MODIFST est directement envoyé à l'interface utilisateur de gestion de session UI2 du module de gestion de session M2, tel qu'illustré sur la Fig. 3 par un flèche en trait plein (étape TX(MSG_MODIFST)). Sur réception de ce message, ladite interface UI2 appelle une fonction de modification d'état de session bas niveau, FCTv(slo) pour la fonction de verrouillage ou FCTc(scl) pour la fonction de fermeture, du système d'exploitation (non représenté) de ladite deuxième machine PC2.

Dans un deuxième mode de réalisation non limitatif, le message applicatif de modification d'état de session MSG_MODIFST est envoyé à un greffon PLGN2 du module de gestion de session M2, tel qu'illustré sur la Fig. 3 par une flèche sous forme de tirets (étape TX(MSG_MODIFST)). Le greffon PLGN2, couramment appelé « Plugin » en anglais, sollicite alors l'interface utilisateur de gestion de session UI2 du module de gestion de session M2. Sur cette sollicitation, l'interface UI2 appelle la fonction de modification d'état de session bas niveau, FCTv(slo) pour la fonction de verrouillage) ou FCTc(scl) pour la fonction de fermeture, du système d'exploitation (non représenté) de ladite deuxième machine PC2.

L'utilisation d'un greffon PLGN2 évite de modifier l'interface utilisateur de gestion de session existante dans une machine pour intégrer une fonction de réception d'un message applicatif MSG_MODIFST ou de la remplacer par

une nouvelle interface utilisateur de gestion de session intégrant la fonction de réception d'un message applicatif MSG_MODIFST, comme c'est le cas dans le premier mode de réalisation ci-dessus.

Dans un exemple non limitatif, les fonctions de modification d'état de session bas niveau FCTv(slo), FCTc(scl) se trouvent dans une bibliothèque de liens dynamique. Selon les types de systèmes d'exploitation, cette bibliothèque aura une extension différente (par exemple .dll pour « dynamic link library » en anglais ; .so pour « shared object » en anglais ; .dylib pour « dynamic library » en anglais ; .a pour « archive » en anglais ; .sl « pour shared library » en anglais ; .sa pour « archive » en anglais). De telles bibliothèques étant connues de l'homme du métier, elles ne sont pas décrites plus en détail ici.

Dans un autre exemple non limitatif, les fonctions de modification d'état de session bas niveau FCTv(slo), FCTc(scl) sont des fonctions binaires. Dans ce cas, contrairement aux bibliothèques de liens dynamiques, elles nécessitent une recompilation du module utilisateur de gestion de session M2.

Ainsi, **dans une sixième étape 6)**, sur réception du message applicatif de modification d'état de session MSG_MODIFST, ledit module de gestion de session M2 procède à ladite modification d'état de session (étape MODIFST(slo, scl) illustrée aux figures 1b, 1c, 1d et à la Fig. 3).

En particulier, cette modification d'état de session est effectuée par l'interface utilisateur de gestion de session UI2 avec la fonction bas niveau FCTv(slo) ou FCTc(scl), comme expliqué ci-dessus.

Ainsi, dans l'exemple pris, la session ouverte par l'utilisateur USR sur la deuxième machine PC2 est soit verrouillée (état verrouillé ST=slo), soit fermée (état fermé ST=scl).

On rappelle que lorsqu'une la session utilisateur est verrouillée, cela signifie qu'aucune action utilisateur n'est possible, mis à part via le clavier de la deuxième machine PC2 par lequel la seule action possible est la réactivation de la session utilisateur en entrant l'identifiant utilisateur et le mot de passe associé de l'utilisateur USR.

Dans une septième étape 7), si la modification d'état de session de la deuxième machine PC2 se réalise, le service de contrôle de sessions SRV envoie à la première machine PC1 une requête d'autorisation d'ouverture de session RQ_OPSESSOK.

Finalement, une session est ouverte sur la première machine PC1. On notera que la première machine PC1 comporte également un module de gestion de session M1, tel qu'illustré sur la Fig. 2a et la Fig. 2b, apte à effectuer l'ouverture de session sur réception d'une requête d'autorisation d'ouverture de session (non représentée) du service de contrôle de sessions SRV. Ce module de gestion de session M1 comporte l'interface utilisateur de gestion de session UI1.
On notera que dans un mode de réalisation non limitatif, lorsque la première machine PC1 comporte un service de sécurité SES1, ledit service de sécurité reçoit cette requête d'autorisation d'ouverture de session RQ_OPSSSOK.

Dans une huitième étape 8), le service de contrôle de sessions SRV, sauvegarde dans ledit référentiel BDD ladite au moins information d'identification IDU dudit utilisateur USR associée à une donnée d'identification IDP de ladite première machine PC1.

Ainsi, cela permet d'enregistrer le fait que l'utilisateur USR a ouvert une session sur la première machine PC1.

Dans un exemple non limitatif, le référentiel BDD est un annuaire LDAP géré par un administrateur du parc de machines GRP.

On notera que suite à la réception d'un message applicatif de modification d'état de session MSG_MODIFST tel que décrit à l'étape 6), une modification d'état de session qui correspond à une fermeture de session de la deuxième machine PC2 peut échouer, dans le cas où une application est ouverte et refuse de se terminer, par exemple lorsque des documents sont déjà ouverts sous cette session. On notera que dans ce

cas, le type de fermeture de session est classique, c'est-à-dire qu'elle ne termine pas de manière forcée une application.

Dans ce cas, **dans une neuvième étape 9)**, dans un premier mode de réalisation non limitatif, si la modification d'état de session de la deuxième machine PC2 échoue, le service de contrôle de sessions SRV envoie à la première machine PC1 une requête d'interdiction d'ouverture de session RQ_OPSESSOK (étape TX(RQ_OPSESSNOK(USR, IDP1) illustrée sur les figures 1a à 1c et à la Fig. 3).

Dans un deuxième mode de réalisation non limitatif, tel qu'illustré sur la Fig. 1d, si la modification d'état de session de la deuxième machine PC2 correspondant à une fermeture de session échoue, le service de contrôle de sessions SRV envoie audit service de sécurité SES2 de ladite deuxième machine PC2 une requête de modification d'état de session RQ_MODIFST de ladite deuxième machine PC2 qui est de type Tp verrouillage de session (ST=slo). Les étapes 4) à 8) décrites précédemment sont alors effectuées. Ainsi, en cas d'échec d'une fermeture de session, la session sur la deuxième machine PC2 est au moins verrouillée.

On notera que les étapes de vérification et d'envoi de la requête de modification d'état de session décrites ci-dessus sont effectuées pour toute machine PC appartenant au parc de machines GRP et différente de la première machine. Ainsi, dans le parc de machines, il n'existera qu'une seule session utilisateur d'un même utilisateur qui sera soit déverrouillée, soit ouverte. Les machines du parc de machines sont ainsi sécurisées. Une tierce personne ne pourra utiliser de manière illicite la session utilisateur de l'utilisateur lorsque ce dernier n'utilise plus sa session, et les machines ne seront pas occupées inutilement par des sessions utilisateurs non usitées.

Ainsi, le procédé d'ouverture de session évite que plusieurs sessions au nom d'un même utilisateur ne soient déverrouillées sur plusieurs machines à la fois (lorsque la modification d'état de session est un

verrouillage). Cela permet de sécuriser les accès aux applications des machines.

Ainsi, le procédé d'ouverture de session évite que plusieurs sessions au nom d'un même utilisateur ne soient ouvertes sur plusieurs machines à la fois (lorsque la modification d'état de session est une fermeture). Cela évite de mobiliser des machines inutilement.

Le procédé d'ouverture de session est mis en œuvre par le service de contrôle de sessions SRV pour un parc de machines PC1, PC2 apte à effectuer une ouverture de session d'une première machine PC1, ledit parc de machines comprenant au moins ladite première machine PC1 et une deuxième machine PC2, ladite deuxième machine PC2 comportant un service de sécurité SES2.

Le service de contrôle de sessions SRV est apte à :

- recevoir une requête d'ouverture de session RQ_OPSESS de ladite première machine PC1, ladite requête comprenant au moins une information d'identification IDU d'un utilisateur USR ;
- vérifier si ladite au moins information d'identification IDU dudit utilisateur USR est associée dans un référentiel BDD à une donnée d'identification IDU de ladite deuxième machine PC2 ;
- contrôler si l'utilisateur USR a le droit d'ouvrir une session sur la première machine PC1 ;
- dans l'affirmative de ladite vérification et dudit contrôle, envoyer audit service de sécurité SES2 de ladite deuxième machine PC2 une requête de modification d'état de session RQ_MODIFST de ladite deuxième machine PC2 ;
- si la modification d'état de session de la deuxième machine PC2 se réalise, envoyer à la première machine PC1 une requête d'autorisation d'ouverture de session RQ_OPSESSOK ; et
- sauvegarder dans ledit référentiel BDD par le service de contrôle de sessions SRV ladite au moins information d'identification IDU dudit utilisateur USR associée à une donnée d'identification IDP de ladite première machine PC1.

Un système informatique SYS apte à effectuer une ouverture de session de la première machine PC1 par un service de contrôle de sessions SRV pour un parc de machines PC1, PC2 comprenant au moins ladite première machine PC1 et une deuxième machine PC2, ladite deuxième machine PC2 comportant un module de gestion de session M2, est illustré selon un premier mode de réalisation non limitatif à la Fig. 2a et à la Fig. 4, et selon un deuxième mode de réalisation à la Fig.2b et à la Fig. 5.

Le système informatique SYS comprend :
- le service de contrôle de sessions SRV apte à coopérer avec la première machine PC1 et la deuxième machine PC2 ;
- ladite deuxième machine PC2 apte à recevoir du service de contrôle de sessions SRV via ledit service de sécurité SES2 une requête de modification d'état de session RQ_MODIFST ; et
- ladite première machine PC1 apte à :
  - émettre une requête d'ouverture de session RQ_OPSESS vers ledit service de contrôle de sessions SRV ; et
  - si la modification d'état de session de la deuxième machine PC2 se réalise, recevoir dudit service de contrôle de sessions SRV une requête d'autorisation d'ouverture de session RQ_OPSESSOK.

Dans un premier mode de réalisation non limitatif, une machine de gestion MGN d'un parc de machines PC1, PC2 comprend ledit service de contrôle de sessions SRV, telle qu'illustrée sur les figures 2a, 3 et 4. Elle est ainsi apte à coopérer avec la première machine PC1 et la deuxième machine PC2. La machine de gestion MGN est ainsi apte à effectuer une ouverture de session d'une première machine PC1 par le service de contrôle de sessions SRV pour ledit parc GRP de machines PC1, PC2 comprenant au moins ladite première machine PC1 et une deuxième machine PC2, ladite deuxième machine PC2 comportant un service de sécurité SES2.
La machine de gestion MGN, la première machine PC1 et la deuxième machine PC2 forment le système informatique SYS.

Dans un deuxième mode de réalisation non limitatif, la deuxième

machine PC2 comprend ledit service de contrôle de sessions SRV, telle qu'illustrée sur les figures 2b et 5.

Dans un mode de réalisation non limitatif illustré sur la Fig. 2a et la Fig. 2b sous forme de traits et cadre illustrés par des tirets, le module de gestion de session M2 de la deuxième machine PC2 comprend :
- un greffon PLGN2 apte à recevoir un message applicatif de modification d'état de session MSG_MODIFST correspondant à une requête de modification d'état de session RQ_MODIFST envoyée par le service de contrôle de sessions SRV ; et
- une interface utilisateur de gestion de session UI2 apte à être sollicitée par ledit greffon PLGN2 pour modifier l'état de session ladite deuxième machine PC2.

Bien entendu la description n'est pas limitée à l'application, aux modes de réalisation et aux exemples décrits ci-dessus.

- Ainsi, dans un mode de réalisation non limitatif, l'envoi d'une requête RQ peut s'effectuer par un protocole de communication autre que TCP/IP ou UDP. Tout protocole de communication qui permet un échange de données sur un réseau informatique entre plusieurs machines peut être utilisé.

- Ainsi, le procédé décrit peut être utilisé dans des applications autres que celle décrite du domaine hospitalier. Par exemple il peut s'appliquer dans le cadre d'une gestion d'un parc de machines :
  - d'une centrale nucléaire,
  - d'un réseau téléphonique,
  - d'un réseau ferroviaire,
  - dans une tour de contrôle,
  - dans un parc d'ascenseurs etc.…

et de manière générale dans toute application permettant l'ouverture de session sur plusieurs machines par un même utilisateur.

Ainsi, l'invention décrite présente notamment les avantages suivants :

- elle est simple à mettre en œuvre ;
- elle permet de verrouiller ou fermer de manière centralisée via le service de contrôle de sessions des sessions utilisateur ouverts par un même utilisateur sur différentes machines ;
- elle permet ainsi de sécuriser les machines d'un même parc de machines (lorsque la modification d'état de session est un verrouillage ou une fermeture) ;
- elle permet de réduire le nombre de ressources utilisées (machines, applications, etc.) (lorsque la modification d'état de session est une fermeture) ;
- elle pallie l'oubli d'un utilisateur de verrouiller ou fermer sa session sur une machine ;
- elle est sécurisée du fait du service de sécurité SES1, SES2, respectivement de la première, deuxième machine, qui se trouve à l'extérieur du module utilisateur de gestion de session M1, M2 et qui est donc indépendant de ce dernier ; et
- elle donne le choix entre une fermeture ou un verrouillage de session, ce choix étant déterminé soit en amont par paramétrage, soit par l'utilisateur lui-même.

REVENDICATIONS

1. Procédé d'ouverture de session d'une première machine (PC1) par un service de contrôle de sessions (SRV) pour un parc (GRP) de machines (PC1, PC2) comprenant au moins ladite première machine (PC1) et une deuxième machine (PC2), ladite deuxième machine (PC2) comportant un service de sécurité (SES2), le procédé comportant les étapes de :
- recevoir par le service de contrôle de sessions (SRV) une requête d'ouverture de session (RQ_OPSESS) de ladite première machine (PC1), ladite requête comprenant au moins une information d'identification (IDU) d'un utilisateur (USR) ;
- vérifier par le service de contrôle de sessions (SRV) si ladite au moins information d'identification (IDU) dudit utilisateur (USR) est associée dans un référentiel (BDD) à une donnée d'identification (IDU) de ladite deuxième machine (PC2) ;
- contrôler par le service de contrôle de sessions (SRV) si l'utilisateur (USR) a le droit d'ouvrir une session sur la première machine (PC1) ;
- dans l'affirmative de ladite vérification et dudit contrôle, envoyer par le service de contrôle de sessions (SRV) audit service de sécurité (SES2) de ladite deuxième machine (PC2) une requête de modification d'état de session (RQ_MODIFST) de ladite deuxième machine (PC2) ; et
- si la modification d'état de session de la deuxième machine (PC2) se réalise, envoyer par le service de contrôle de sessions (SRV) à la première machine (PC1) une requête d'autorisation d'ouverture de session (RQ_OPSESSOK) ; et
- sauvegarder dans ledit référentiel (BDD) par le service de contrôle de sessions (SRV) ladite au moins information d'identification (IDU) dudit utilisateur (USR) associée à une donnée d'identification (IDP) de ladite première machine (PC1).

2. Procédé d'ouverture de session selon la revendication 1, selon lequel la requête de modification d'état de session (RQ_MODIFST) est de type (Tp) verrouillage de session (RQ_MODIFST (slo)) ou fermeture de session (RQ_MODIFST(scl)).

3. Procédé d'ouverture de session selon la revendication 2, selon lequel le type (Tp) d'une requête de modification d'état de session (RQ_MODIFST) est paramétré dans le service de contrôle de session (SRV).

4. Procédé d'ouverture de session selon la revendication 2 ou la revendication 3, selon lequel il comporte une étape supplémentaire d'envoyer par la première machine (PC1) au service de contrôle de session (SRV) une requête de paramétrage comprenant le type (Tp) de la requête de modification d'état de session (RQ_MODIFST).

5. Procédé d'ouverture de session selon la revendication précédente, selon lequel il comporte une étape supplémentaire d'envoyer par le service de contrôle de sessions (SRV) audit service de sécurité (SES2) de ladite deuxième machine (PC2) une requête de modification d'état de session (RQ_MODIFST) de ladite deuxième machine (PC2) qui est de type (Tp) verrouillage de session si la modification d'état de session de la deuxième machine (PC2) correspondant à une fermeture de session échoue.

6. Procédé d'ouverture de session selon l'une quelconque des revendications précédentes, selon lequel une requête (RQ_OPSESS, RQ_OPSESSOK, RQ_MODIFST) reçue ou émise par le service de contrôle de sessions (SRV) est une requête TCP/IP ou UDP.

7. Procédé d'ouverture de session selon l'une quelconque des revendications précédentes, selon lequel il comporte une étape supplémentaire d'envoyer un message applicatif de modification d'état de session (MSG_MODIFST) correspondant à la requête de modification d'état de session (RQ_MODIFST) à un module de gestion de session (M2) de la deuxième machine (PC2).

8. Procédé d'ouverture de session selon l'une quelconque des revendications précédentes, selon lequel il comporte une étape supplémentaire d'envoyer un message applicatif de modification d'état de session (MSG_MODIFST) correspondant à la requête de modification

d'état de session (RQ_MODIFST) à un greffon (PLGN2) d'un module de gestion de session (M2) de la deuxième machine (PC2).

9. Procédé d'ouverture de session selon l'une quelconque des revendications précédentes, selon lequel les étapes de vérification et d'envoi de la requête de modification d'état de session (RQ_MODIFST) sont effectuées pour toute machine appartenant au parc de machines (GRP) et différente de la première machine (PC1).

10. Service de contrôle de sessions (SRV) pour un parc de machines (PC1, PC2) apte à effectuer une ouverture de session d'une première machine (PC1), ledit parc de machines comprenant au moins ladite première machine (PC1) et une deuxième machine (PC2), ladite deuxième machine (PC2) comportant un service de sécurité (SES2), ledit service de contrôle de sessions (SRV) étant apte à :
- recevoir une requête d'ouverture de session (RQ_OPSESS) de ladite première machine (PC1), ladite requête comprenant au moins une information d'identification (IDU) d'un utilisateur (USR) ;
- vérifier si ladite au moins information d'identification (IDU) dudit utilisateur (USR) est associée dans un référentiel (BDD) à une donnée d'identification (IDU) de ladite deuxième machine (PC2) ;
- contrôler si l'utilisateur (USR) a le droit d'ouvrir une session sur la première machine (PC1) ;
- dans l'affirmative de ladite vérification et dudit contrôle, envoyer audit service de sécurité (SES2) de ladite deuxième machine (PC2) une requête de modification d'état de session (RQ_MODIFST) de ladite deuxième machine (PC2) ;
- si la modification d'état de session de la deuxième machine (PC2) se réalise, envoyer à la première machine (PC1) une requête d'autorisation d'ouverture de session (RQ_OPSESSOK) ; et
- sauvegarder dans ledit référentiel (BDD) par le service de contrôle de sessions (SRV) ladite au moins information d'identification (IDU) dudit utilisateur (USR) associée à une donnée d'identification (IDP) de ladite première machine (PC1).

11. Machine de gestion (MGN) d'un parc de machines (PC1, PC2) apte à effectuer une ouverture de session d'une première machine (PC1) par un service de contrôle de sessions (SRV) pour ledit parc (GRP) de machines (PC1, PC2) comprenant au moins ladite première machine (PC1) et une deuxième machine (PC2), ladite deuxième machine (PC2) comportant un service de sécurité (SES2), ladite machine de gestion (MGN) comprenant ledit service de contrôle de sessions (SRV) selon la revendication précédente 6.

12. Système informatique (SYS) apte à effectuer une ouverture de session d'une première machine (PC1) par un service de contrôle de sessions (SRV) pour un parc de machines (PC1, PC2) comprenant au moins ladite première machine (PC1) et une deuxième machine (PC2), ladite deuxième machine (PC2) comportant un service de sécurité (SES2), ledit système (SYS) comprenant :
- le service de contrôle (SRV) selon la revendication 6 apte à coopérer avec la première machine (PC1) et la deuxième machine (PC2) ;
- ladite deuxième machine (PC2) apte à recevoir du service de contrôle de sessions (SRV) via ledit service de sécurité (SES2) une requête de modification d'état de session (RQ_MODIFST) ; et
- ladite première machine (PC1) apte à :
  - émettre une requête d'ouverture de session (RQ_OPSESS) vers ledit service de contrôle de sessions (SRV) ; et
  - si la modification d'état de session de la deuxième machine (PC2) se réalise, recevoir dudit service de contrôle de sessions (SRV) une requête d'autorisation d'ouverture de session (RQ_OPSESSOK).

13. Système informatique (SYS) selon la revendication précédente, selon lequel la deuxième machine (PC2) comporte un module de gestion de session (M2) comprenant un greffon (PLGN2).

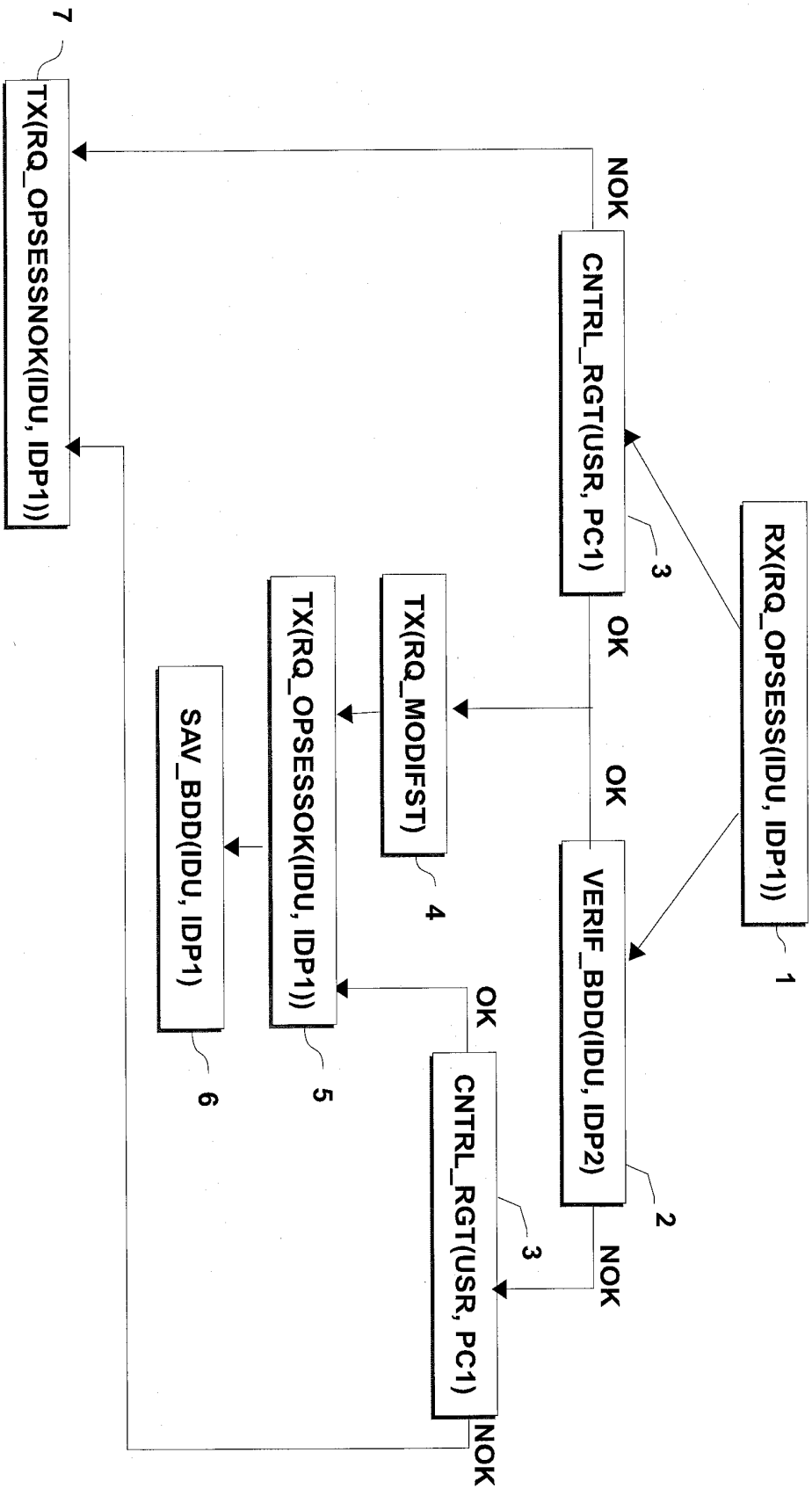

RX(RQ_OPSESS(IDU, IDP1))
1
VERIF_BDD(IDU, IDP2)
2
NOK
CNTRL_RGT(USR, PC1)
3
OK
NOK
CNTRL_RGT(USR, PC1)
3
OK
TX(RQ_MODIFST)
4
TX(RQ_OPSESSOK(IDU, IDP1))
5
SAV_BDD(IDU, IDP1)
6
NOK
TX(RQ_OPSESSNOK(IDU, IDP1))
7

FIG. 1a

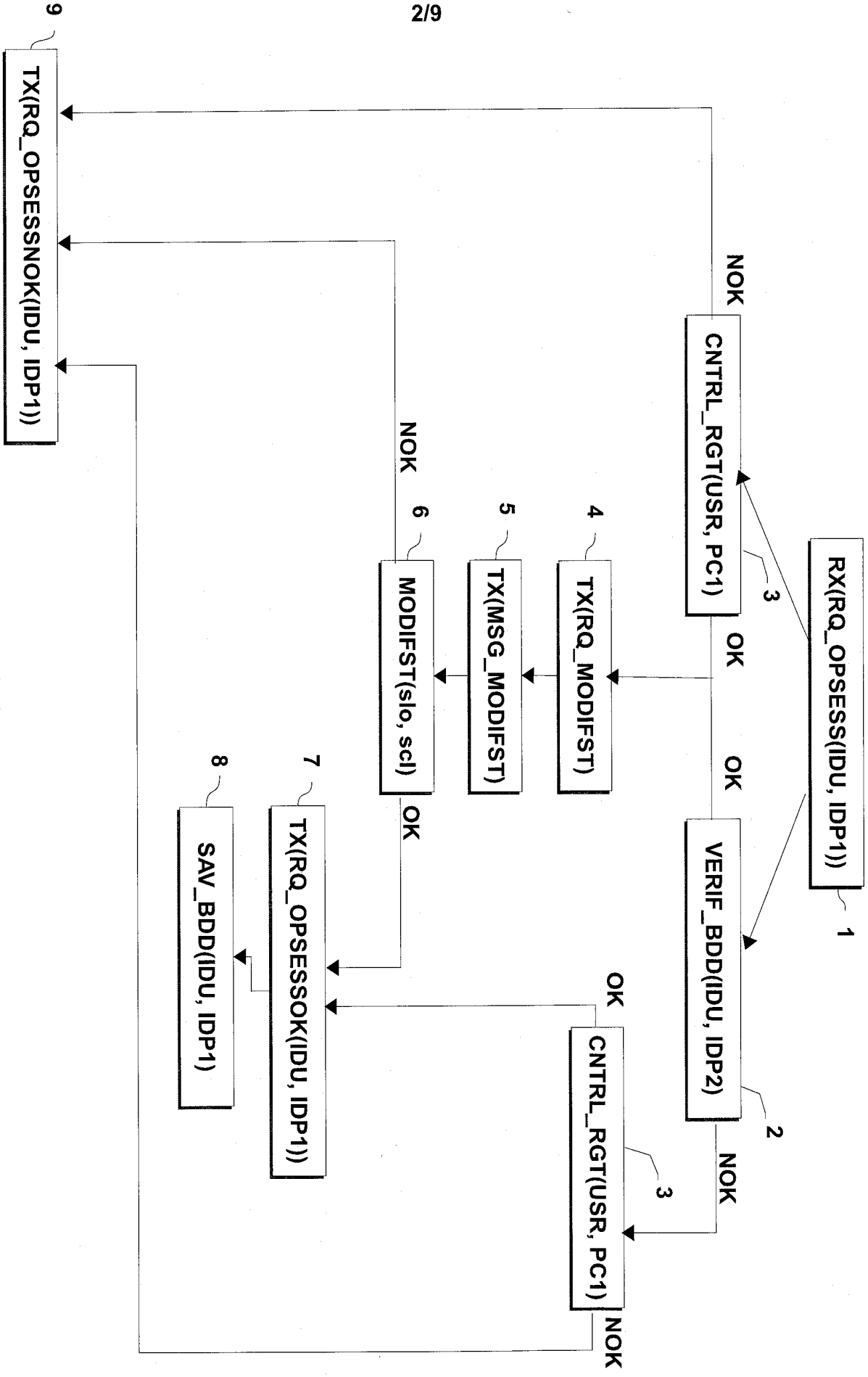

RX(RQ_OPSESS(IDU, IDP1))
1
VERIF_BDD(IDU, IDP2)
2
CNTRL_RGT(USR, PC1)
3
TX(RQ_MODIFST)
4
TX(MSG_MODIFST)
5
MODIFST(slo, scl)
6
TX(RQ_OPSESSOK(IDU, IDP1))
7
SAV_BDD(IDU, IDP1)
8
TX(RQ_OPSESSNOK(IDU, IDP1))
9
OK
NOK

FIG. 1b

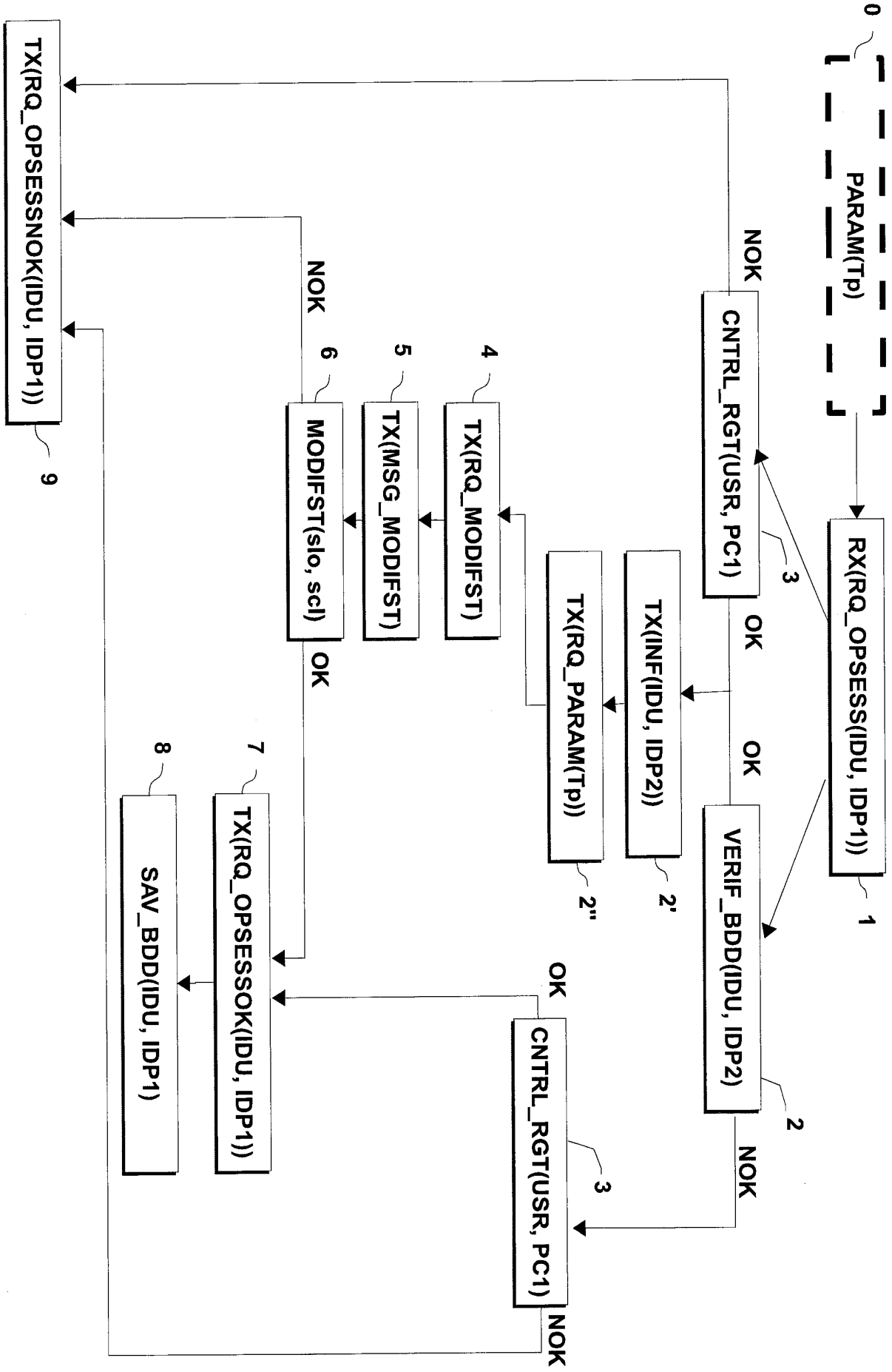

0
PARAM(Tp)
RX(RQ_OPSESS(IDU, IDP1))
1
CNTRL_RGT(USR, PC1)
NOK
3
OK
TX(INF(IDU, IDP2))
2'
TX(RQ_PARAM(Tp))
2"
VERIF_BDD(IDU, IDP2)
OK
2
NOK
CNTRL_RGT(USR, PC1)
3
OK
NOK
TX(RQ_OPSESSNOK(IDU, IDP1))
9
MODIFST(slo, scl)
6
NOK
OK
TX(MSG_MODIFST)
5
TX(RQ_MODIFST)
4
TX(RQ_OPSESSOK(IDU, IDP1))
7
SAV_BDD(IDU, IDP1)
8

FIG. 1c

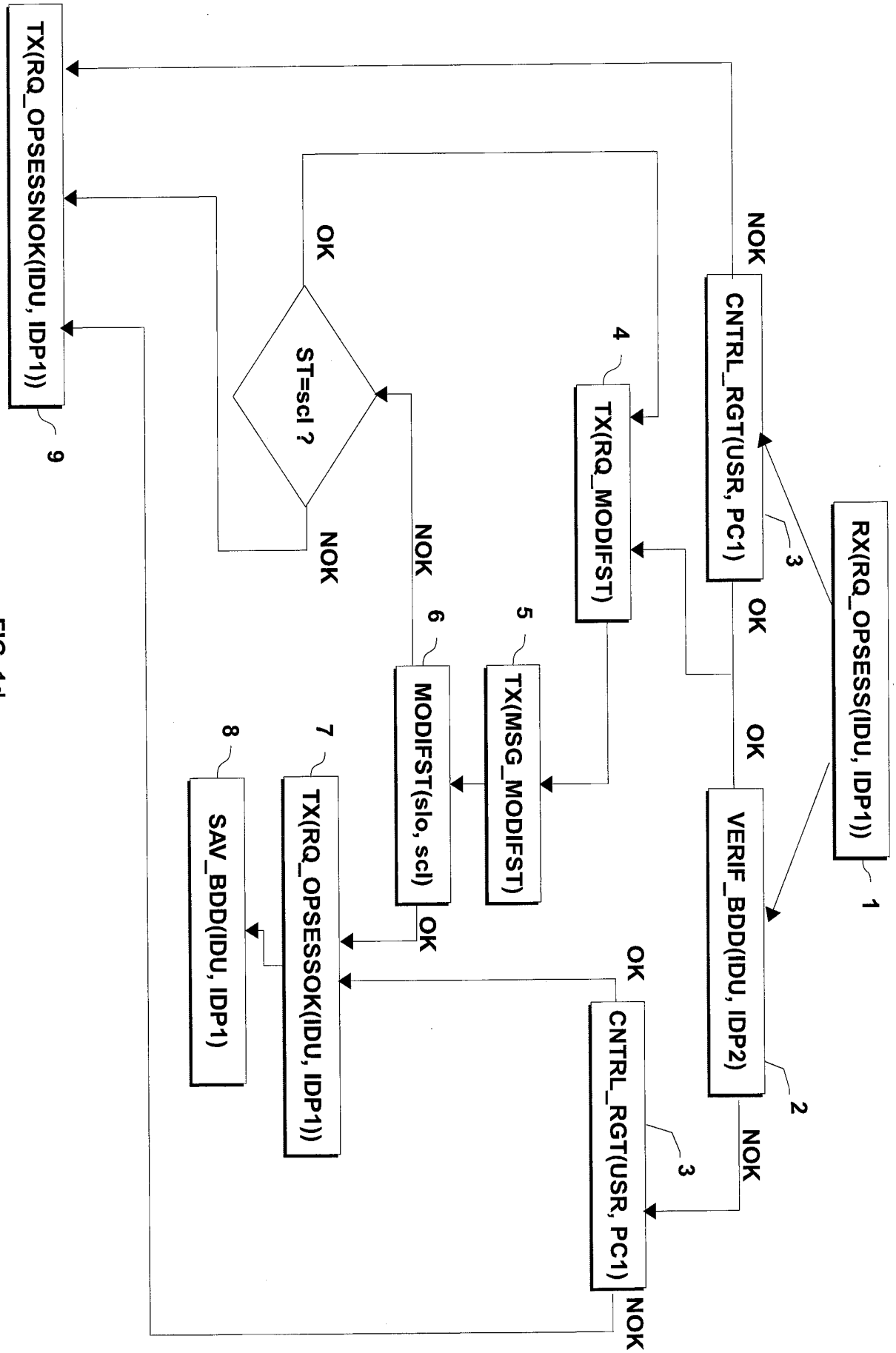

RX(RQ_OPSESS(IDU, IDP1))
1
VERIF_BDD(IDU, IDP2)
2
CNTRL_RGT(USR, PC1)
3
TX(RQ_MODIFST)
4
TX(MSG_MODIFST)
5
MODIFST(slo, scl)
6
TX(RQ_OPSESSOK(IDU, IDP1))
7
SAV_BDD(IDU, IDP1)
8
TX(RQ_OPSESSNOK(IDU, IDP1))
9
ST=scl ?
OK
NOK

FIG. 1d

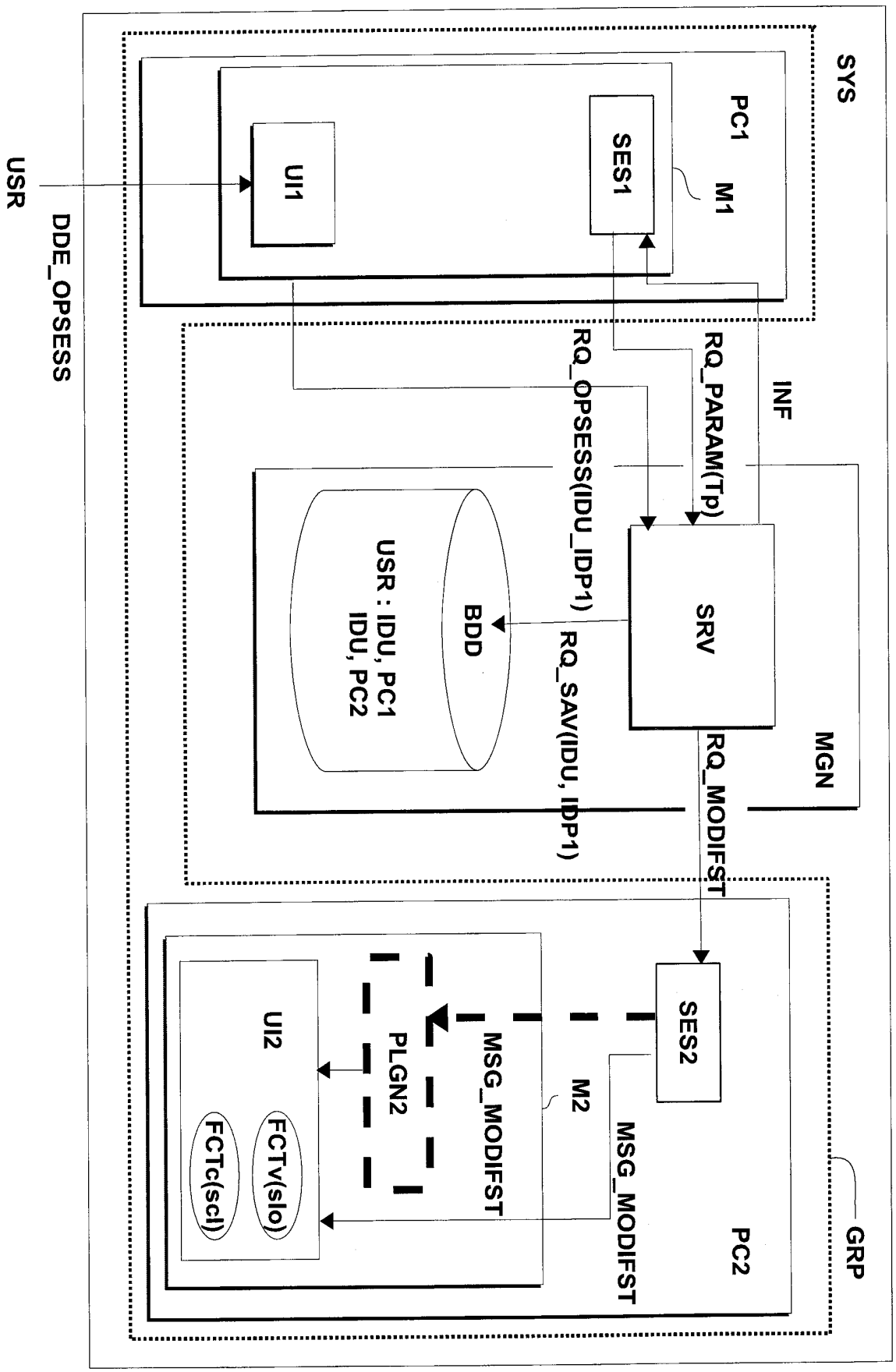

USR
DDE_OPSESS
SYS
PC1
M1
SES1
UI1
RQ_OPSESS(IDU_IDP1)
RQ_PARAM(Tp)
INF
MGN
BDD
USR : IDU, PC1
IDU, PC2
SRV
RQ_SAV(IDU, IDP1)
RQ_MODIFST
GRP
SES2
M2
MSG_MODIFST
MSG_MODIFST
PC2
PLGN2
UI2
FCTv(slo)
FCTc(scl)

FIG. 2a

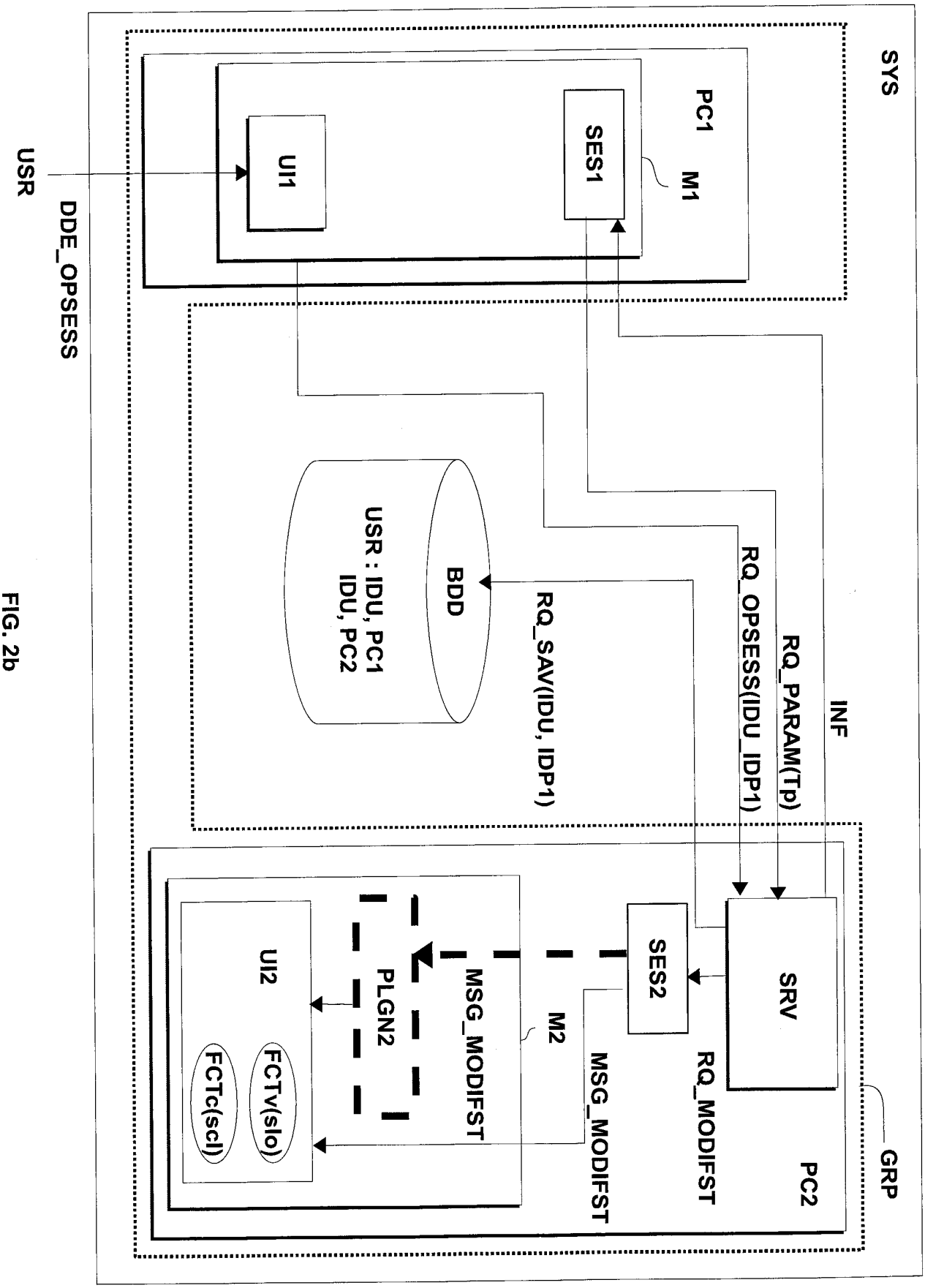

SYS
PC1
M1
SES1
UI1
USR
DDE_OPSESS
INF
RQ_PARAM(Tp)
RQ_OPSESS(IDU_IDP1)
RQ_SAV(IDU, IDP1)
BDD
USR : IDU, PC1
IDU, PC2
SRV
SES2
RQ_MODIFST
MSG_MODIFST
M2
MSG_MODIFST
PLGN2
UI2
FCTv(slo)
FCTc(scl)
PC2
GRP

FIG. 2b

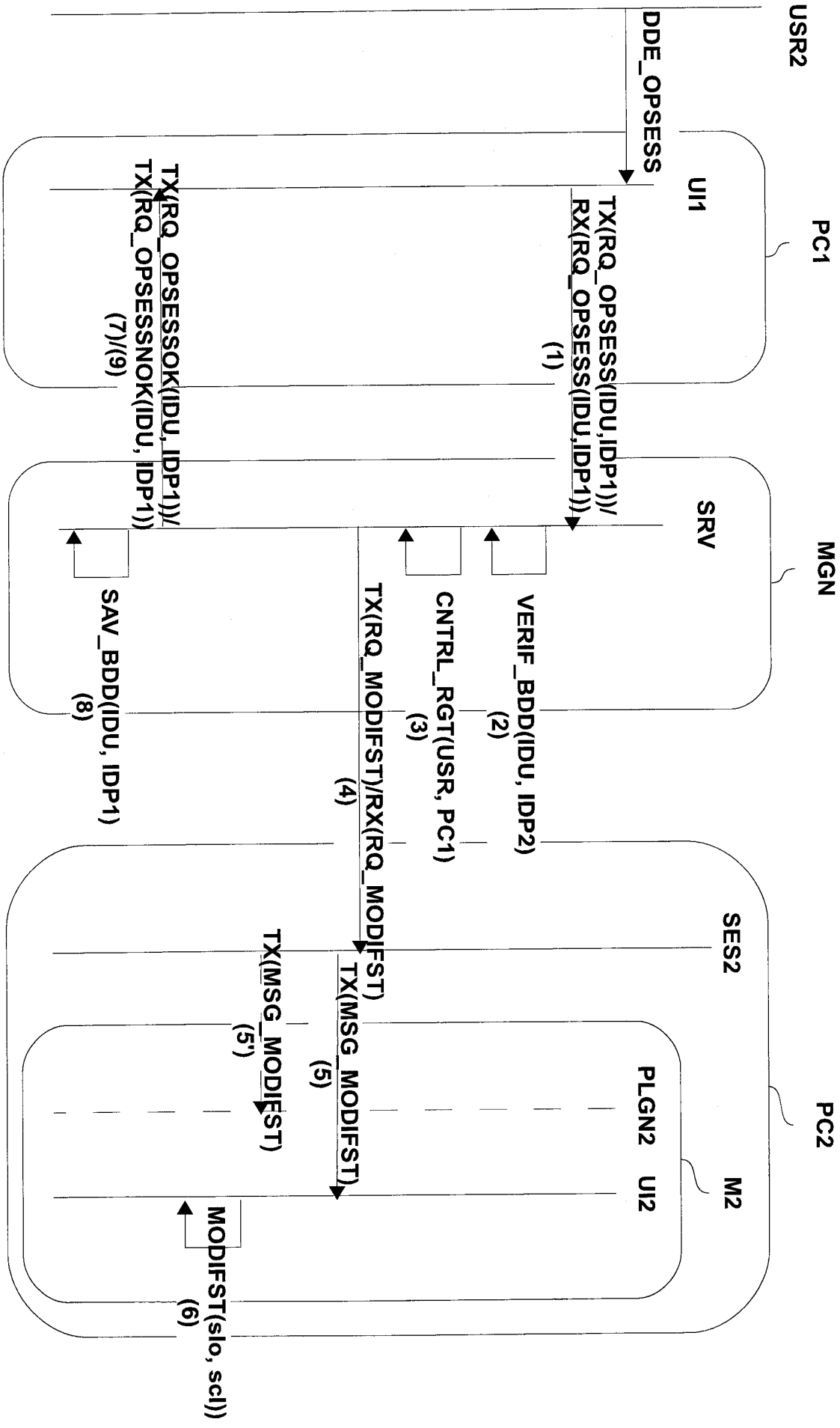

USR2
PC1
MGN
PC2
DDE_OPSESS
UI1
SRV
SES2
PLGN2
UI2
M2
TX(RQ_OPSESS(IDU,IDP1))/
RX(RQ_OPSESS(IDU,IDP1))
(1)
VERIF_BDD(IDU, IDP2)
(2)
CNTRL_RGT(USR, PC1)
(3)
TX(RQ_MODIFST)/RX(RQ_MODIFST)
(4)
TX(MSG_MODIFST)
(5)
TX(MSG_MODIFST)
(5')
MODIFST(slo, scl)
(6)
SAV_BDD(IDU, IDP1)
(8)
TX(RQ_OPSESSOK(IDU, IDP1))/
TX(RQ_OPSESSNOK(IDU, IDP1))
(7)/(9)

FIG. 3

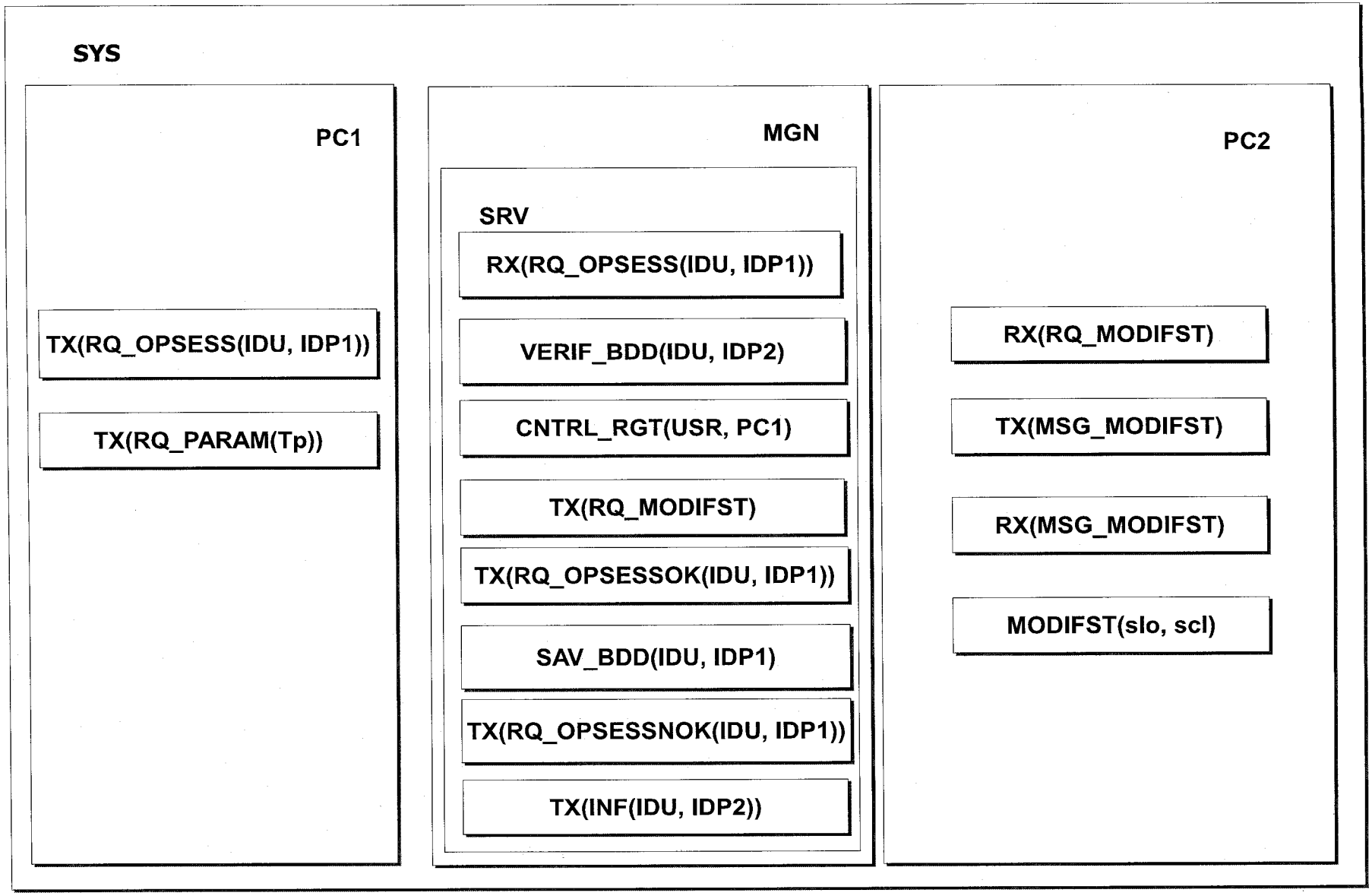

SYS
PC1
TX(RQ_OPSESS(IDU, IDP1))
TX(RQ_PARAM(Tp))
MGN
SRV
RX(RQ_OPSESS(IDU, IDP1))
VERIF_BDD(IDU, IDP2)
CNTRL_RGT(USR, PC1)
TX(RQ_MODIFST)
TX(RQ_OPSESSOK(IDU, IDP1))
SAV_BDD(IDU, IDP1)
TX(RQ_OPSESSNOK(IDU, IDP1))
TX(INF(IDU, IDP2))
PC2
RX(RQ_MODIFST)
TX(MSG_MODIFST)
RX(MSG_MODIFST)
MODIFST(slo, scl)

FIG. 4

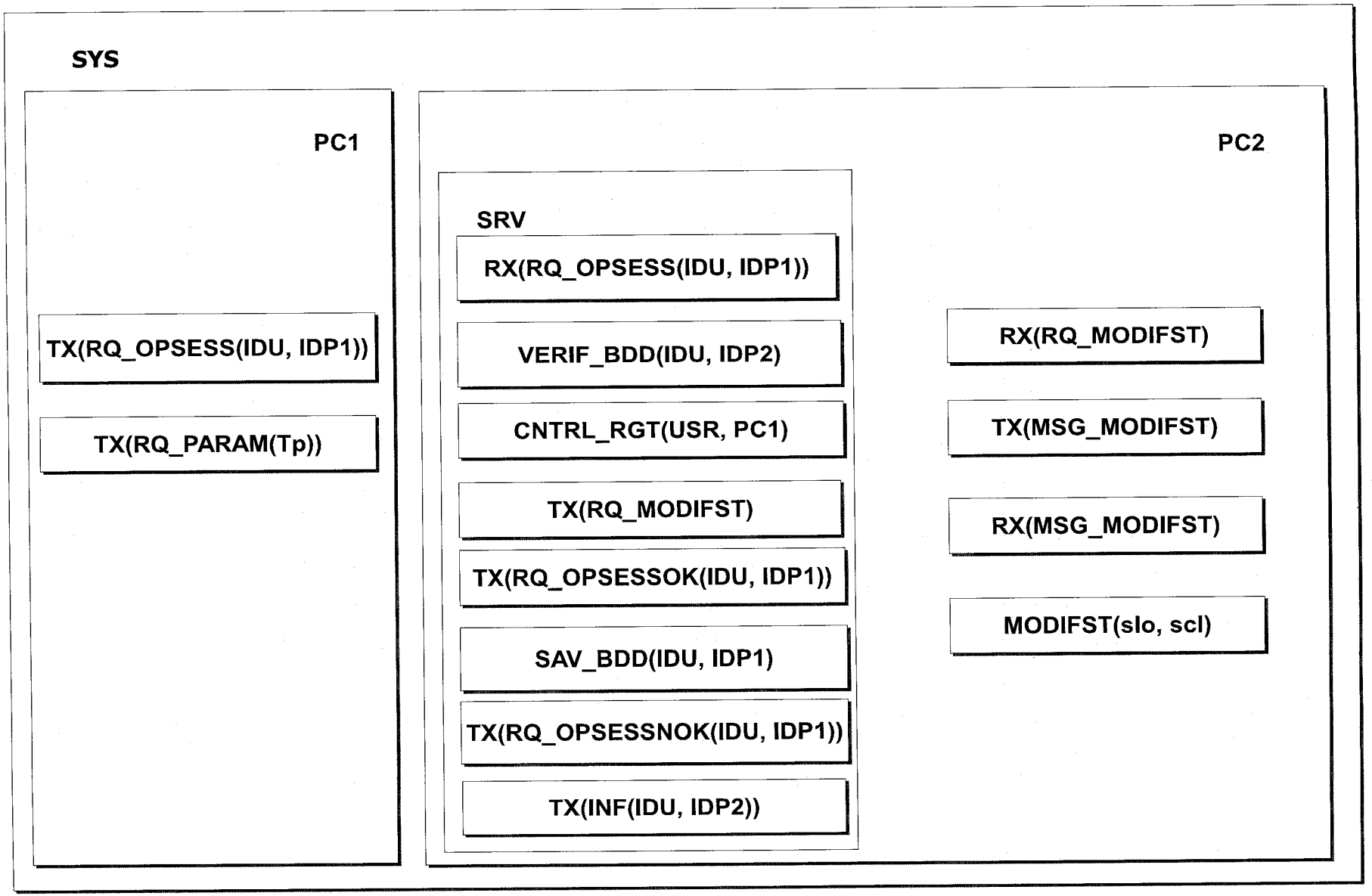

SYS
PC1
TX(RQ_OPSESS(IDU, IDP1))
TX(RQ_PARAM(Tp))
PC2
SRV
RX(RQ_OPSESS(IDU, IDP1))
VERIF_BDD(IDU, IDP2)
CNTRL_RGT(USR, PC1)
TX(RQ_MODIFST)
TX(RQ_OPSESSOK(IDU, IDP1))
SAV_BDD(IDU, IDP1)
TX(RQ_OPSESSNOK(IDU, IDP1))
TX(INF(IDU, IDP2))
RX(RQ_MODIFST)
TX(MSG_MODIFST)
RX(MSG_MODIFST)
MODIFST(slo, scl)

FIG. 5

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 736222
FR 1053429

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2005/080906 A1 (PEDERSEN BRADLEY J [US]) 14 avril 2005 (2005-04-14) * figure 1 * * alinéas [0024], [0027], [0037] * * alinéas [0038], [0041], [0046] * * alinéa [0047] * -----	1-13	H04L12/12 G06F21/22 H04L29/08N13 H04L29/08N1A H04L29/08N11M G06F21/00N5R T04L29/06S10
X	US 2007/162605 A1 (CHALASANI NANCHARIAH R [US] ET AL) 12 juillet 2007 (2007-07-12) * figures 3A,3B * * alinéas [0002], [0003], [0017] * * alinéas [0021], [0023], [0025] * * alinéas [0027] - [0028] * -----	1-13	
A	US 2006/277536 A1 (STEIN MICHAEL V [US] ET AL) 7 décembre 2006 (2006-12-07) * figure 2 * * alinéas [0003], [0006], [0027] * * alinéas [0028], [0034] - [0036] * -----	1-13	
A	US 2007/169175 A1 (HALL KYLENE J [US] ET AL) 19 juillet 2007 (2007-07-19) * alinéas [0001] - [0012], [0031] * * alinéas [0034], [0036], [0055] * * alinéas [0061], [0065], [0067] - [0069] * -----	1-13	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L G06F
A	Anonymous: "Symantec pcAnywhere Solution User Guide Version 12.5"[Online] 25 février 2010 (2010-02-25), pages 1-63, XP002607050 Symantec Extrait de l'Internet: URL:http://www.symantec.com/business/support/index?page=content&id=DOC2087pc> [extrait le 2011-10-26] Table 2-4 Ending an active session, page 49-50 -----	1-13	

Date d'achèvement de la recherche	Examinateur
27 octobre 2010	Kufer, Léna

CATÉGORIE DES DOCUMENTS CITÉS

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

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1053429 FA 736222

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 27-10-2010
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2005080906 A1	14-04-2005	AU 2004281457 A1	28-04-2005
		CA 2541987 A1	28-04-2005
		EP 1671226 A2	21-06-2006
		EP 2000905 A1	10-12-2008
		JP 2007508617 T	05-04-2007
		KR 20060131739 A	20-12-2006
		US 2010011113 A1	14-01-2010
		WO 2005038649 A2	28-04-2005
US 2007162605 A1	12-07-2007	CN 101009576 A	01-08-2007
US 2006277536 A1	07-12-2006	AUCUN	
US 2007169175 A1	19-07-2007	AUCUN	

EPO FORM P0465