(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 895 611**

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

(21) **N° d'enregistrement national :** **05 13220**

(51) Int Cl[8] : **H 04 L 9/32** (2006.01), H 04 L 29/10, G 06 K 1/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 23.12.05.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 29.06.07 Bulletin 07/26.

(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) :** *THALES Société anonyme* — FR.

(72) **Inventeur(s) :** WEBER ERIC, GRANJARD DAVID et ALCOUFFE FABIEN.

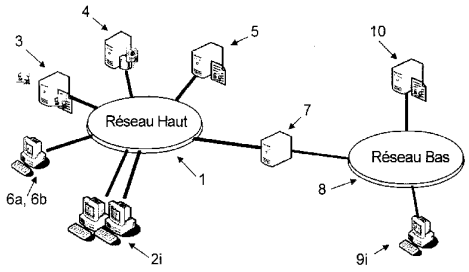
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** MARKS & CLERK FRANCE.

(54) ARCHITECTURE ET PROCEDE POUR CONTROLER LE TRANSFERT D'INFORMATIONS ENTRE UTILISATEURS.

(57) Système et procédé pour marquer et contrôler le transfert d'informations entre plusieurs utilisateurs (2i, 9i) comportant au moins les éléments suivants:

- Une autorité (3) permettant de marquer une information à transmettre,
- Un annuaire (4) ou dispositif contenant les certificats de tous les utilisateurs ainsi que les certificats de tous les composants de l'architecture,
- Un bureau de sécurité (5),
- Un dispositif (6a) de gestion de clé et un dispositif (6b) de gestion des privilèges.



FR 2 895 611 - A1

ARCHITECTURE ET PROCEDE POUR CONTROLER LE TRANSFERT D'INFORMATIONS ENTRE UTILISATEURS

L'invention concerne notamment une architecture de système et un procédé pour contrôler le transfert d'informations entre plusieurs utilisateurs, en fonction du niveau de sensibilité des informations.

Elle s'applique, notamment, pour contrôler des flux d'information sortant d'un premier réseau ayant un niveau de confidentialité donné vers un deuxième réseau ayant un niveau de confidentialité inférieur au premier.

On utilisera le mot « labellisation » pour désigner une solution de marquage d'informations ou d'objets numériques qui permet notamment :

- De contrôler l'accès aux objets en fonction des droits des utilisateurs conformément à une politique de sécurité, définie par exemple par le responsable d'un système,
- De filtrer des objets transmis entre entités de niveaux de sécurités différents, en assurant que seules les informations autorisées transitent.

A la connaissance du demandeur, à l'heure actuelle, les techniques de l'art antérieur ne permettent pas de poser un label avec un niveau de confiance suffisant.

L'invention concerne un procédé pour marquer et contrôler le transfert d'informations entre plusieurs utilisateurs caractérisé en ce qu'il comporte au moins les étapes suivantes :

- Un utilisateur émet une requête de demande de labellisation d'information,
- La demande de labellisation est transmise vers une autorité de labellisation sur laquelle l'utilisateur s'authentifie,
- L'autorité de labellisation :

- nettoie l'information transmise conformément à une politique de sécurité définie,
- vérifie auprès d'un annuaire les droits de l'utilisateur à manipuler l'information,
- associe de façon fiable le couple information+label, en utilisant une ressource cryptographique,

- L'autorité de labellisation transmet ensuite le couple information+label vers l'utilisateur pour vérification de la non-altération de l'information labellisée et, après vérification, elle transmet ce couple à un bureau de sécurité qui enregistre l'objet (information + label),
- Le bureau de sécurité délivre ensuite l'information aux utilisateurs qui en font la demande en fonction des informations contenues dans le label, des droits de l'utilisateur demandeur authentifié, et conformément à une politique donnée. La politique de sécurité peut être définie par un administrateur de réseau.

Le transfert d'informations s'effectue, par exemple, entre des premiers clients d'un premier réseau de niveau de confidentialité donné et des deuxièmes clients d'un deuxième réseau de niveau de confidentialité inférieure à celui du premier réseau et en ce qu'il comporte au moins les étapes suivantes :

- une passerelle filtrante vérifie l'intégrité du couple (information et label), l'identité de l'utilisateur et transfère le fichier si la politique de sécurité l'autorise,
- on stocke l'information labellisée sur le deuxième réseau,
- lorsqu'un client émet une requête pour récupérer les informations, un bureau de sécurité vérifie, en fonction des droits du client et par rapport aux informations du label et de la politique de sécurité, si la délivrance de l'information est autorisée.

L'invention concerne aussi un système pour marquer et contrôler le transfert d'informations entre plusieurs utilisateurs caractérisé en ce qu'il comporte au moins les éléments suivants :

- Une autorité permettant de marquer (ou déposer un label) une information à transmettre,
- Un annuaire ou dispositif contenant les certificats de tous les utilisateurs ainsi que les certificats de tous les composants de l'architecture,
- Un bureau de sécurité,
- Un dispositif de gestion de clé et un dispositif de gestion des privilèges.

Le système peut comporter au moins deux réseaux, un premier réseau sur lequel sont connectés des premiers utilisateurs et un second réseau sur lequel sont connectés un ou des seconds utilisateurs, le niveau de confidentialité du second réseau ayant un niveau de confidentialité inférieur à celui du premier réseau et peut comporter une passerelle filtrante disposée entre les deux réseaux.

La présente invention permet, notamment, de délivrer de l'information aux seules personnes autorisées à la recevoir. Elle assure que l'information est autorisée à sortir du réseau de confiance dans le cadre de transfert d'informations entre réseaux.

L'invention permet d'augmenter le niveau de sécurité de la solution en réduisant les possibilités de canaux cachés sur le flux, le procédé traitant des objets, des informations et non des flux.

D'autres caractéristiques et avantages de la présente invention apparaîtront mieux à la lecture de la description donnée à titre illustratif et nullement limitatif annexé des figures qui représentent :

- La figure 1 un exemple d'ensemble d'éléments mis en œuvre dans le système selon l'invention, et
- La figure 2 un exemple d'architecture de système selon l'invention.

La figure 1 représente un ensemble d'éléments mis en œuvre selon l'invention, pour le transfert d'informations entre plusieurs utilisateurs faisant partie d'un ou plusieurs réseaux différents, les informations transmises présentant un caractère confidentiel.

Une information est, par exemple, un objet numérique, un message électronique, un fichier, etc.

L'architecture comprend, par exemple, un ou plusieurs clients 2i, une autorité de labellisation 3, un annuaire 4, un bureau de sécurité 5, un dispositif 6a et un dispositif 6b schématisés dans un bloc commun sur la figure, dont les fonctions sont décrites ci-après.

Un poste client 2i élabore les requêtes de demande de labellisation de l'information. Le poste comprend aussi un moyen adapté à vérifier les informations après labellisation.

L'autorité de labellisation 3 a notamment pour fonction de poser les labels sur tous les objets ou informations des utilisateurs du système. Elle comprend aussi une ressource cryptographique afin d'associer de façon fiable le couple information + label.

Le dispositif 6a est une infrastructure ayant notamment pour fonction, la gestion des clés. Elle génère les certificats de clés du réseau de confiance pour l'ensemble des intervenants du système, les clients, les dispositifs mis en œuvre dans le procédé selon l'invention.

Le dispositif 6b est une infrastructure de gestion des privilèges. Il permet notamment la gestion des droits des différents intervenants du système. Il génère par exemple les certificats des privilèges.

L'annuaire 4 stocke, notamment, les créations des dispositifs 6a et 6b habituellement désignés IGC (Infrastructure de gestion des clés) et IGP (infrastructure de gestion des privilèges).

Le procédé et le système selon l'invention s'appliquent, par exemple, pour des flux sortant d'un premier réseau d'un niveau de confiance

donné vers un second réseau de niveau de confiance inférieur à celui du premier réseau. La figure 2 décrit un exemple d'architecture d'un tel système.

Le système comprend, par exemple, un premier réseau de haute sensibilité 1 dénommé « réseau haut » sur lequel sont connectés différents éléments tels que : un ou plusieurs premiers clients 2i, une autorité de labellisation 3, un annuaire 4, un bureau de sécurité 5, un dispositif 6a et un dispositif 6b schématisés dans un bloc commun sur la figure, dont les fonctions sont décrites ci-après.

Le réseau haut 1 est relié par une passerelle filtrante 7 à un second réseau de basse sensibilité 8, appelé « réseau bas » car il présente un niveau de confiance inférieur à celui du réseau haut. Sur le réseau de basse sensibilité sont connectés un ou plusieurs seconds clients 9i et un bureau de sécurité 10.

La passerelle filtrante 7 a notamment pour fonction de vérifier que l'information peut transiter ou non d'un réseau vers un autre. Elle assure l'interconnexion des réseaux. Elle filtre, par exemple, le niveau de l'information, les protocoles réseaux, etc.

La solution mise en œuvre dans cet exemple s'appuie sur un annuaire 4 qui contient les certificats de tous les utilisateurs ainsi que les certificats de tous les composants de l'architecture, pour les identifications.

La mise en œuvre du système s'effectue, par exemple, de la manière décrite ci-après.

Un demandeur ou client 2i du réseau de haute sensibilité 1 qui souhaite transférer des informations vers le réseau de basse sensibilité 8, émet une requête de pose de label sur une information, à l'autorité de labellisation. Pour créer une demande de labellisation d'information, le demandeur ou client 2i remplit un formulaire comprenant un ensemble de champs. Ceci se fait par exemple sur le poste client lui-même. Les champs peuvent contenir des données associées aux informations à transmettre

telles que le nom de l'émetteur de l'information, le niveau de classification de cette information, le destinataire de l'information, etc.

La demande est ensuite transmise vers l'autorité de labellisation 3. La transmission des informations (objet + formulaire), entre l'autorité de labellisation et le client demandeur, est sécurisée. La sécurisation des échanges entre les 2 réseaux est mise en œuvre par un procédé d'authentification et de chiffrement connu de l'Homme du métier tel que par exemple le protocole de sécurisation par couche SSL (abrégé anglo-saxon de secure socket layer).

A la réception de l'information, l'autorité de labellisation exécute différentes étapes, par exemple :

- Elle « nettoie » l'information transmise (suppression des canaux cachés) conformément à la politique de sécurité définie par l'organisation utilisatrice responsable de la sécurité. Les canaux cachés sont par exemple les moyens qui permettent de transférer des informations à l'insu de l'utilisateur ; par exemple, les champs cachés des fichiers Word commercialisé par la société Microsoft, non vus par l'utilisateur lors de l'ouverture d'un fichier avec Word,
- Elle vérifie auprès de l'annuaire 4 les droits de l'utilisateur 2i pour labelliser des informations,
- Elle utilise sa ressource cryptographique pour associer de façon sûre, par scellement par exemple, le couple information + label.

Le nouvel objet (information + label) est ensuite retransmis à l'utilisateur ou client demandeur 2i pour vérification et vers le « serveur bureau de sécurité » 5 apte à stocker et délivrer de l'information labellisée vers d'autres utilisateurs. La vérification consiste, par exemple, à contrôler que l'information n'a pas été altérée par le nettoyage et la pose du label.

- Le bureau de sécurité 5 enregistre une copie de l'objet (information et label), puis transmet l'information labellisée à travers une passerelle de sécurité, vers l'extérieur.

- Au passage, la passerelle filtrante 7 vérifie, le scellement, l'intégrité du couple (information et label), l'identité de l'utilisateur et transfère le fichier si la politique de sécurité l'autorise.
- L'information est stockée sur le serveur bureau de sécurité du réseau de basse sensibilité.

Lorsqu'un client 9i du réseau bas demande au serveur bureau de sécurité de lui délivrer de l'information, le bureau de sécurité 10 vérifie, en fonction des droits de l'utilisateur par rapport au label associé à l'information et à la politique de sécurité, s'il peut lui délivrer l'information.

Il est possible d'utiliser le standard XML comme conteneur pour l'information labellisée. Les méta-données exige la prise en compte des normes XML.

Le système et le procédé décrits ci-dessus s'appliquent, par exemple, dans les domaines suivants : les réseaux pharmaceutiques, la recherche, les réseaux bancaires, et tous les systèmes dans lesquels on souhaite transmettre des informations d'un réseau ayant un niveau de confiance vers un réseau de niveau de confiance moins important.

Sans sortir du cadre de l'invention, on peut utiliser une autorité de labellisation centralisée ou distribuée sur tous ou sur certains postes clients.

REVENDICATIONS

1 - Procédé pour marquer et contrôler le transfert d'informations entre plusieurs utilisateurs (2i, 9i) caractérisé en ce qu'il comporte au moins les étapes suivantes :

- Un utilisateur (2i) émet une requête de demande de labellisation d'informations,
- La demande de labellisation est transmise vers une autorité de labellisation (3) sur laquelle l'utilisateur (2i) s'authentifie,
- L'autorité de labellisation (3) :
  - nettoie l'information transmise conformément à une politique de sécurité définie,
  - vérifie auprès d'un annuaire (4) les droits de l'utilisateur(2i) à manipuler l'information,
  - associe de façon sure le couple information+label, en utilisant une ressource cryptographique,
- L'autorité de labellisation transmet ensuite le couple information+label vers l'utilisateur (2i) pour vérification de la non-altération de l'information labellisée et après vérification elle transmet ce couple à un bureau de sécurité (5, 10) qui enregistre l'objet (information + label),
- Le bureau de sécurité délivre ensuite l'information aux utilisateurs qui en font la demande en fonction des informations contenues dans le label, des droits de l'utilisateur authentifié, et conformément à une politique donnée.

2 – Procédé selon la revendication 1 caractérisé en ce que le transfert d'informations s'effectue entre des premiers clients (2i) d'un premier réseau de niveau de confidentialité donné et des deuxièmes clients (9i) d'un

deuxième réseau de niveau de confidentialité inférieure à celui du premier réseau et en ce qu'il comporte au moins les étapes suivantes :

- une passerelle filtrante (7) vérifie l'intégrité du couple (information et label), l'identité de l'utilisateur et transfère le fichier si la politique de sécurité l'autorise,
- on stocke l'information labellisée sur le deuxième réseau,
- lorsqu'un client (9i) émet une requête pour récupérer les informations, un bureau de sécurité vérifie en fonction des droits du client et par rapport aux informations du label et de la politique de sécurité si la délivrance de l'information est autorisée.

3 - Système pour marquer et contrôler le transfert d'informations entre plusieurs utilisateurs (2i, 9i) caractérisé en ce qu'il comporte au moins les éléments suivants :

- Une autorité (3) permettant de marquer une information à transmettre,
- Un annuaire (4) ou dispositif contenant les certificats de tous les utilisateurs ainsi que les certificats de tous les composants de l'architecture,
- Un bureau de sécurité (5),
- Un dispositif (6a) de gestion de clé et un dispositif (6b) de gestion des privilèges.

4 – Système selon la revendication 3 caractérisé en ce qu'il comporte au moins deux réseaux, un premier réseau (1) sur lequel sont connectés des premiers utilisateurs (2i) et un second réseau (8) sur lequel sont connectés des deuxièmes utilisateurs (9i), le niveau de confidentialité du second réseau ayant un niveau de confidentialité inférieur à celui du premier réseau et en ce qu'il comporte une passerelle filtrante (7) disposée entre les deux réseaux.

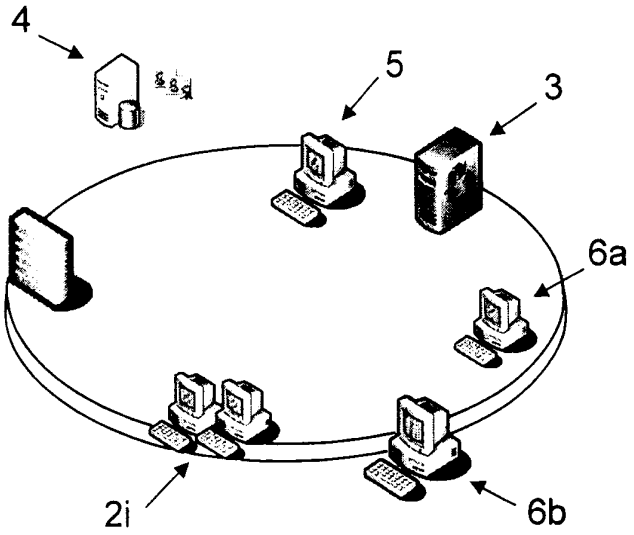


FIG.1

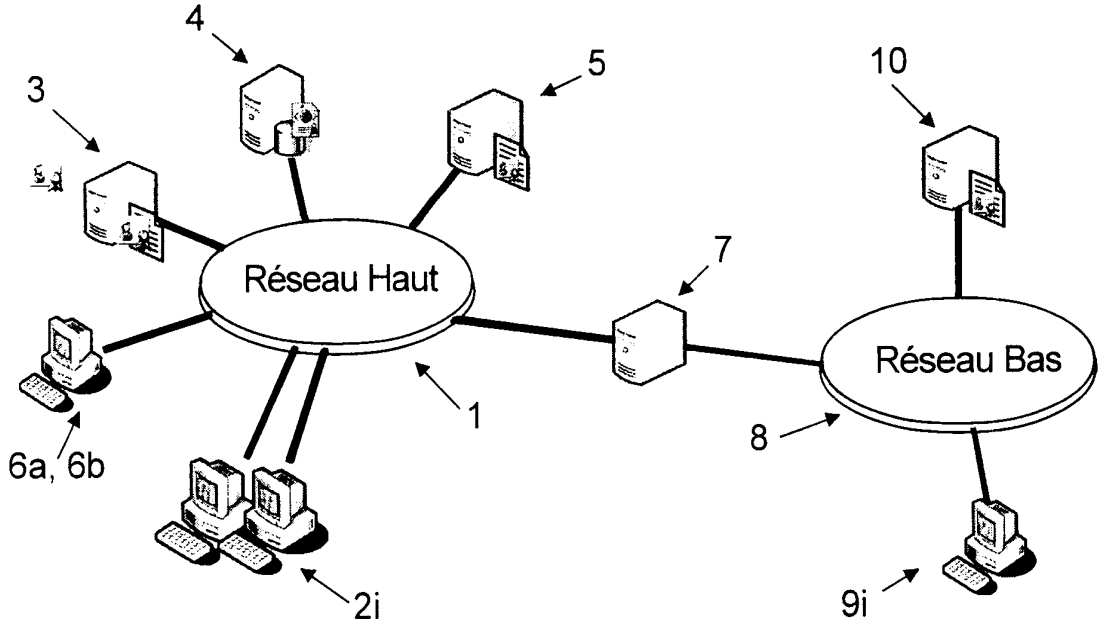


FIG.2

RÉPUBLIQUE FRANÇAISE

2895611

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 676810
FR 0513220

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 2004/196843 A1 (ZININ ALEXEY D [US]) 7 octobre 2004 (2004-10-07) * abrégé * * figure 1 * * alinéa [0024] - alinéa [0029] * -----	1-4	
A	CHAPMAN AND ZWICKY: "Building Internet Firewalls" 1995, O'REILLY & ASSOCIATES , USA , XP002406306 * page 4 - page 5 * * page 131 - page 134 * * page 168 - page 171 * * page 379 - page 381 * -----	1-4	
A	US 6 480 963 B1 (TACHIBANA HIROTAKA [JP] ET AL) 12 novembre 2002 (2002-11-12) * abrégé * -----	1-4	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L

Date d'achèvement de la recherche	Examinateur
9 novembre 2006	SAN MILLAN MAESO, J

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 0513220 FA 676810

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 09-11-2006
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 2004196843 A1	07-10-2004	AUCUN	
US 6480963 B1	12-11-2002	JP 2000004225 A	07-01-2000

EPO FORM P0465