

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

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(43) Date de la publication internationale
16 août 2012 (16.08.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/107369 A1

- (51) Classification internationale des brevets :
H04L 29/06 (2006.01)
- (21) Numéro de la demande internationale :
PCT/EP2012/051896
- (22) Date de dépôt international :
3 février 2012 (03.02.2012)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
11/50977 8 février 2011 (08.02.2011) FR
- (71) Déposant (*pour tous les États désignés sauf US*) : **MORPHO** [FR/FR]; 27 rue Leblanc, F-75015 Paris (FR).
- (72) Inventeurs; et
- (75) Inventeurs/Déposants (*pour US seulement*) : **PEPIN, Cyrille** [FR/FR]; Morpho, 27 rue Leblanc, F-75015 Paris (FR). **LECOCQ, François** [FR/FR]; Morpho, 27 rue Leblanc, F-75015 Paris (FR).
- (74) Mandataire : **MAILLET, Alain**; B.P 70250, 5 place Newquay, B.P 70250, F-35802 Dinard Cedex (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, CL, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, 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, RS, SE, SI, SK,

[Suite sur la page suivante]

(54) Title : METHOD AND DEVICE FOR CONNECTING TO A REMOTE SERVICE FROM A HOST DEVICE

(54) Titre : PROCEDE ET DISPOSITIF DE CONNEXION A UN SERVICE DISTANT DEPUIS UN DISPOSITIF HOTE

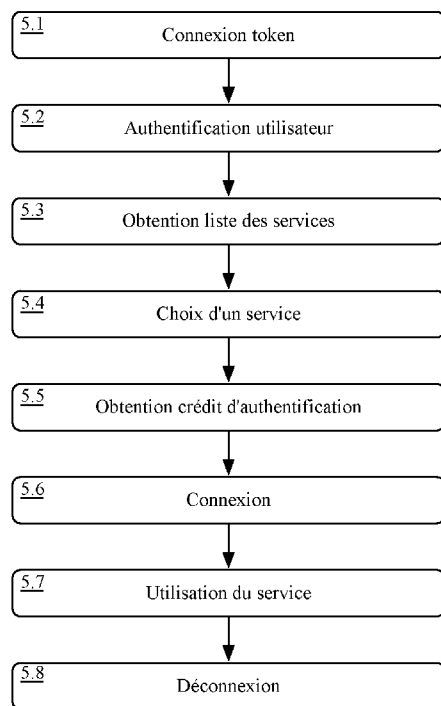


Fig. 5

(57) Abstract : The invention pertains to the field of computer security, and specifically, to the protection of confidential personal data so as to enable the encrypted access to a remote service, wherein said invention relates to a security device that can be connected to a host device. The security device handles the transaction security. The device advantageously uses a smartcard component for storing the list of accessible services as well as the associated authentication credits. The browser used for connecting to the remote service obtains the list of services and the authentication credit corresponding to a selected service. The connection to the device is then made using the authentication credit provided by the security device.

(57) Abrégé : Dans le domaine de la sécurité informatique et plus précisément le domaine de la protection des informations personnelles confidentielles permettant l'accès chiffré à un service distant est décrit un dispositif de sécurité connectable au dispositif hôte. Ce dispositif de sécurité est en charge de la sécurité de la transaction. Il repose avantageusement sur un composant de carte à puce qui stocke la liste des services accessibles ainsi que les crédits d'authentification associés. Le navigateur servant à la connexion avec le service distant obtient la liste des services puis le crédit d'authentification correspondant à un service choisi. La connexion au service se fait alors en utilisant le crédit d'authentification fourni par le dispositif de sécurité.

WO 2012/107369 A1



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). **Publiée :**

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

Procédé et dispositif de connexion à un service distant depuis un dispositif hôte

La présente invention concerne le domaine de la sécurité informatique et plus précisément le domaine de la protection des informations personnelles confidentielles permettant l'accès chiffré à un service distant.

Aujourd'hui, grâce au développement important du réseau Internet, l'utilisateur peut accéder à un nombre grandissant de services dits « en ligne ». La plupart de ces services nécessitent une authentification de l'utilisateur pour lui permettre l'accès à des données qui le concernent. On peut citer comme exemple de tels services, l'accès aux données de son compte bancaire, le suivi de ses opérations de remboursement de prestations médicales ou encore la déclaration d'impôts en ligne.

La Fig. 1 illustre l'architecture du réseau. L'utilisateur utilise typiquement un dispositif hôte 1.1 tel qu'un ordinateur personnel ou tout dispositif similaire tel qu'un assistant personnel ou un téléphone intelligent (*smartphone* en anglais). Ce dispositif hôte est connecté à un réseau d'échange d'informations 1.2, typiquement le réseau Internet. Sur ce réseau sont également connectés des serveurs 1.3 hébergeant les services distants. L'utilisateur peut donc accéder depuis son dispositif hôte aux

services hébergés sur les serveurs 1.3 par l'intermédiaire du réseau d'échange d'informations 1.2.

Nombre de ces services traitent d'informations confidentielles et il est important de sécuriser l'accès à ces services. Cette sécurisation passe généralement par la mise à disposition de l'utilisateur d'informations de connexion secrètes qu'il doit produire pour établir la connexion au service. Typiquement il s'agit d'un nom d'utilisateur et d'un mot de passe associé. Lors de la connexion, l'utilisateur se voit demander d'entrer ce nom et ce mot de passe qui servent à l'authentification et à l'établissement d'une connexion chiffrée permettant d'assurer la confidentialité des échanges d'informations entre l'utilisateur et le service distant. Il est courant de sécuriser ces échanges d'informations de connexion pour éviter qu'elles puissent être dérobées lors de leur transport entre le dispositif hôte et le serveur. Cette sécurisation se fait typiquement par la création d'une connexion chiffrée ou d'un tunnel chiffré entre le dispositif hôte et le serveur. Cette connexion chiffrée ou tunnel peut, par exemple, être créé en utilisant le protocole *SSL* (*Secure Socket Layer* en anglais), ou son successeur *TLS* (*Transport Layer Security* en anglais). La Fig. 2 illustre l'utilisation de ces techniques. Le dispositif hôte envoie une requête en connexion 2.1, généralement à l'aide de son navigateur Internet au serveur hébergeant le service. Cette requête n'est pas chiffrée. Elle est interprétée par le serveur lors d'une étape 2.2 qui répond par le message 2.3 comportant une clé publique correspondant au certificat identifiant le serveur ou le service. Le dispositif hôte détermine une clé symétrique pseudo aléatoire lors d'une étape 2.4. Il la chiffre à l'aide de la clé publique du serveur reçue dans le message 2.3 et il l'envoie au serveur dans le message 2.5. Seul le serveur est à même de déchiffrer cette clé symétrique à l'aide de sa clé privée associée à sa clé publique. Il effectue ce déchiffrement lors de l'étape 2.6. A ce moment, le dispositif hôte et le serveur partagent une même clé secrète, la clé symétrique et sont donc à même d'établir une connexion chiffrée 2.7 à l'aide de cette clé partagée. Cette connexion chiffrée permet ensuite l'échange d'informations entre le dispositif hôte et le serveur de manière sécurisée. Toutes les données échangées sont chiffrées à l'aide de la clé secrète partagée et ne sont donc déchiffrables que par les deux extrémités de la connexion chiffrée, le dispositif hôte et le serveur, qui partagent le même secret.

On voit que ce procédé permet de sécuriser les échanges entre le dispositif hôte et le serveur. Par contre, les données échangées sont manipulées en clair par le serveur

et le terminal. On suppose *a priori* que le serveur est sûr du fait d'une gestion par des professionnels. Par contre, la sécurité du dispositif hôte pose problème.

En effet, les utilisateurs sont rarement au fait des techniques permettant d'assurer la sécurité d'un poste de traitement de l'information. De plus, il est
5 extrêmement difficile d'obtenir de leur part un strict respect des règles de sécurité. Il n'est pas rare que le dispositif hôte de l'utilisateur soit infecté par des virus, des logiciels espions ou tout type de logiciels malicieux (*malware* en anglais). Ces logiciels malicieux sont susceptibles de découvrir les informations confidentielles manipulées par le dispositif hôte et de les envoyer à des tiers pouvant en faire un
10 mauvais usage. Et ceci, même lorsque des techniques de sécurité comme celles précédemment décrites sécurisent le lien entre le dispositif hôte et le serveur. Il s'avère que le point faible du système, en ce qui concerne la sécurité, est le dispositif hôte de l'utilisateur. L'utilisateur peut également être vu comme un point faible de sécurité du fait, par exemple, d'un choix de mot de passe simple, peu robuste ou d'une
15 communication volontaire ou non de celui-ci à une personne malveillante.

Ces problèmes de sécurité posent un réel problème au développement des services en ligne. Ils provoquent des préjudices importants pour les acteurs économiques de ce secteur et pour les utilisateurs.

L'invention vise à résoudre les problèmes précédents à l'aide d'un dispositif de
20 sécurité connectable au dispositif hôte. Ce dispositif de sécurité est en charge de la sécurité de la transaction. Il repose avantageusement sur un composant de carte à puce qui stocke la liste des services accessibles ainsi que les crédits d'authentification associés. Le navigateur servant à la connexion avec le service distant obtient la liste des services puis le crédit d'authentification correspondant à un service choisi. La
25 connexion au service se fait alors en utilisant le crédit d'authentification fourni par le dispositif de sécurité.

L'invention concerne un procédé de connexion à un service distant depuis un dispositif hôte qui comprend une étape d'authentification de l'utilisateur auprès d'un
dispositif de sécurité connecté sur le dispositif hôte ; une étape d'obtention d'une liste
30 de services distants auprès dudit dispositif de sécurité ; une étape de choix d'un service parmi la liste de services distants obtenue ; une étape de connexion et d'authentification de l'utilisateur auprès du service distant choisi à l'aide d'un crédit d'authentification stocké dans ledit dispositif de sécurité.

Selon un mode particulier de réalisation de l'invention, le procédé comprend en outre une étape de chargement d'une page d'authentification disponible sur ledit dispositif de sécurité dans un navigateur lancé sur le dispositif hôte ; une étape d'entrée de paramètres d'authentification dans ladite page d'authentification ; une
5 étape de validation desdits paramètres d'authentification par ledit dispositif de sécurité.

Selon un mode particulier de réalisation de l'invention, l'authentification de l'utilisateur auprès dudit dispositif de sécurité comprend une étape d'authentification d'un paramètre biométrique de l'utilisateur par un capteur biométrique intégré audit
10 dispositif de sécurité.

Selon un mode particulier de réalisation de l'invention, l'étape d'obtention d'une liste de services distants comprend une étape de chargement dans un navigateur lancé sur le dispositif hôte d'une page disponible sur ledit dispositif de sécurité, ladite page comprenant une liste de liens sur lesdits services distants.

15 Selon un mode particulier de réalisation de l'invention, l'étape de connexion et d'authentification de l'utilisateur auprès du service distant choisi comprend au sein d'un navigateur :

- une étape de connexion avec ledit dispositif de sécurité;
- une étape de connexion au service distant ;
- 20 - une étape de communication au service distant de crédit d'authentification obtenu dudit dispositif de sécurité ;

Selon un mode particulier de réalisation de l'invention, l'étape de connexion au service distant comprend une étape de chargement d'une page disponible dans ledit dispositif de sécurité, ladite page comprenant un premier cadre dédié à la
25 communication avec le service distant et un second cadre dédié à la communication avec ledit dispositif de sécurité lorsque ladite page est chargée dans un navigateur lancé sur le dispositif hôte.

Selon un mode particulier de réalisation de l'invention, l'étape de connexion et de communication avec ledit dispositif de sécurité est faite selon un protocole
30 particulier implémenté au sein du navigateur et du dispositif.

Selon un mode particulier de réalisation de l'invention, le crédit d'authentification est transmis du dispositif de sécurité au navigateur sous la forme d'une page de données.

Selon un mode particulier de réalisation de l'invention, le crédit d'authentification est transmis du dispositif de sécurité au navigateur sous la forme d'une séquence de codes simulant l'appui sur les touches d'un clavier.

5 Selon un mode particulier de réalisation de l'invention, le procédé comprend en outre une étape préalable de chargement du navigateur utilisé pour la connexion depuis une mémoire de stockage dudit dispositif de sécurité.

Selon un mode particulier de réalisation de l'invention, le procédé comprend en outre une étape de chiffrement/déchiffrement d'au moins une partie des données échangées entre le navigateur et le service distant faite par ledit dispositif de sécurité.

10 L'invention concerne également un dispositif de sécurité connectable à un dispositif hôte pour la connexion sécurisée à un service distant, qui comprend un composant de carte à puce pour le stockage sécurisé de crédits d'authentification et les calculs cryptographiques; une pile de protocoles de communication pour communiquer avec le dispositif hôte ; une liste de services distants avec les adresses
15 de ces services et des crédits d'authentification de l'utilisateur auprès de ces services ;
- des moyens d'authentifier un utilisateur ; des moyens de transmettre au dispositif hôte la liste des services distants ; des moyens de transmettre au dispositif hôte le crédit d'authentification d'un service choisi.

20 Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre une page d'authentification qu'il rend disponible auprès d'un navigateur lancé sur le dispositif hôte et des moyens de valider des paramètres d'authentification entrés par un utilisateur à l'aide de ladite page d'authentification.

Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre un capteur biométrique pour l'authentification de l'utilisateur.

25 Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre une page disponible sur ledit dispositif de sécurité, ladite page comprenant une liste de liens sur lesdits services distants.

30 Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre une page disponible dans ledit dispositif de sécurité, ladite page comprenant un premier cadre dédié à la communication avec le service distant et un second cadre dédié à la communication avec ledit dispositif de sécurité lorsque ladite page est chargée dans un navigateur lancé sur le dispositif hôte.

Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre des moyens pour communiquer avec le dispositif hôte selon un protocole particulier.

5 Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre des moyens de transmettre au dispositif hôte une séquence de codes simulant l'appui sur les touches d'un clavier.

Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre une mémoire de stockage pour mémoriser le navigateur destiné à être utilisé pour la connexion au service distant depuis le dispositif hôte.

10 Selon un mode particulier de réalisation de l'invention, le dispositif comprend en outre des moyens de chiffrer/déchiffrer au moins une partie des données échangées entre le service distant et le navigateur.

Les caractéristiques de l'invention mentionnées ci-dessus, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un exemple de réalisation, ladite description étant faite en relation avec les dessins joints, parmi
15 lesquels :

La Fig. 1 illustre l'architecture du réseau.

La Fig. 2 illustre un exemple de connexion à un service sécurisé selon l'art antérieur.

20 La Fig. 3 illustre l'architecture de principe d'un exemple de réalisation de l'invention.

Les Fig. 4a et 4b illustrent l'architecture protocolaire de deux exemples de réalisation de l'invention.

25 La Fig. 5 illustre le processus d'utilisation d'un service sécurisé selon un exemple de réalisation de l'invention.

Dans l'architecture d'accès à un service sécurisé distant par un utilisateur, le point faible du point de vue de la sécurité est le terminal de l'utilisateur. En effet, l'utilisateur est rarement au fait des règles de sécurité permettant de se prémunir d'une contamination du poste par des logiciels malveillants. En particulier, il n'est pas rare
30 que le terminal des utilisateurs soit envahi par des logiciels tels que des virus informatiques ou des logiciels espions. Certains de ces logiciels malveillants, une fois opérationnels sur le terminal, sont à même d'espionner les actions de l'utilisateur et de prendre connaissance des informations potentiellement confidentielles de celui-ci. Parmi les informations confidentielles sensibles, on peut citer les informations

permettant à l'utilisateur de se connecter à des services distants sécurisés tels que le site de sa banque, des sites de commerces électroniques ou autres. Une fois en possession de ces données sensibles, ces logiciels malveillants sont susceptibles d'utiliser la connexion réseau du poste pour expédier ces informations sensibles à des tiers pouvant en faire un usage frauduleux.

Outre le préjudice direct dû à ces actes de piraterie, l'existence même de la menace est un frein considérable à l'essor des services en ligne dû à la perte de confiance de l'utilisateur. Il est donc particulièrement important de fournir à l'utilisateur le moyen d'accéder de manière sécurisée à des services distants.

La Fig. 3 illustre l'architecture d'un exemple de réalisation de l'invention. Cet exemple montre un dispositif hôte 3.1. Ce dispositif hôte est typiquement un ordinateur personnel ou encore tout type de système de traitement de l'information tel qu'un organiseur personnel (*PDA* en anglais), téléphone intelligent (*smartphone* en anglais), ou autre. Ce dispositif hôte est doté de capacités de communication avec un réseau de communication de données, typiquement Internet. Ce réseau lui permet de se connecter à l'aide d'un logiciel de navigation ou navigateur 3.2 à un service distant 3.3. Selon l'exemple de réalisation de l'invention, un dispositif de sécurité 3.4 est connecté au dispositif hôte. Cette connexion peut se faire selon divers protocoles de communication. L'exemple de réalisation est basé sur une connexion de type USB (*Universal Serial Bus* en anglais). Le dispositif de sécurité se présente alors comme une clé USB connectable au dispositif hôte.

Toutefois, le dispositif de sécurité renferme des fonctionnalités allant bien au-delà d'une simple clé USB. Elle renferme des moyens 3.5 de stocker de manière sécurisée des crédits d'authentification pour la connexion à au moins un service distant. Nous appelons crédit d'authentification un jeu de données permettant l'authentification d'un utilisateur auprès d'un service distant. Ce jeu de données peut consister par exemple en un couple nom de connexion et mot de passe, solution largement utilisée pour l'authentification à des services distants. Toute autre solution peut également être utilisée ici, comme un certificat numérique offrant plus de sécurité qu'un nom et un mot de passe. Avantagusement, ces crédits d'authentification sont stockés dans un composant de carte à puce qui offre l'avantage d'offrir un composant dont la sécurité est éprouvée. De plus, un composant de carte à puce dispose également de moyens de chiffrement et de déchiffrement pouvant être également

utilisés pour les calculs cryptographiques lors des communications entre le dispositif hôte et le service distant si nécessaire.

Le dispositif peut également avantageusement disposer d'une mémoire de masse 3.6. Cette mémoire de masse peut alors servir à stocker par exemple une version du navigateur 3.2 dédiée à la communication avec le service distant. Ce navigateur sera
5 alors typiquement adapté pour intégrer des protocoles de communication avec le dispositif de sécurité lorsqu'il sera exécuté par le dispositif hôte.

Le dispositif peut également avantageusement disposer d'un module 3.7 simulant le fonctionnement d'un clavier lorsqu'il est connecté au dispositif hôte. Dans
10 l'exemple de réalisation, ce module simule un clavier compatible USB et est donc conforme au protocole HID (*Human Interface Device* en anglais) qui normalise le fonctionnement des dispositifs d'entrée sortie USB. Ce module permet l'envoi de séquences de codes simulant l'entrée au clavier d'un nom et d'un mot de passe dans certains modes de réalisation de l'invention.

Selon les modes de réalisation de l'invention, le dispositif de sécurité, lorsqu'il est connecté à un dispositif hôte, apparaît à celui-ci comme un périphérique triple. D'une part, il apparaît comme un dispositif de stockage de masse, tel une clé USB standard grâce au module de mémoire de masse 3.6. D'autre part, il apparaît comme un module de sécurité 3.5 avec lequel le dispositif hôte peut communiquer. Et
20 finalement, il apparaît comme un clavier connecté grâce au module de simulation de clavier 3.7.

Le module de sécurité 3.5 communique avec le dispositif hôte tel un hôte indépendant accessible sur le réseau local du dispositif hôte. Pour cela, il implémente une pile 4.1 de protocoles de communication complète telle la pile illustrée par la Fig.
25 4a. Selon cet exemple de réalisation, le protocole RNDIS 4.6 (*Remote Network Driver Interface Specification* en anglais) est utilisé pour produire un lien Ethernet virtuel au dessus de la couche USB 4.7. Le protocole IP 4.5 est porté sur RNDIS. Il supporte la couche de contrôle TCP 4.4. Les connexions TCP peuvent être sécurisées par la couche TLS (*Transport Layer Security* en anglais) pour, entre autres, permettre
30 l'établissement de requêtes HTTP (*Hyper Text Transport Protocol* en anglais). En particulier, il est avantageux de disposer d'un serveur HTTP implémenté dans le dispositif de sécurité qui va être en mesure de servir des requêtes en authentification ainsi que de fournir des informations comme la liste des services distants disponibles. Selon l'exemple de réalisation, le dispositif de sécurité est donc vu pour ce qui est du

module de sécurité comme un serveur WEB accessible sur le réseau local du dispositif hôte. Alternativement, les couches IP à HTTP peuvent être remplacées par un protocole propriétaire ayant la même fonction, voir Fig. 4b.

La Fig. 5 illustre le fonctionnement typique d'une connexion selon l'invention.

- 5 Lors d'une étape 5.1, l'utilisateur connecte le dispositif de sécurité au dispositif hôte. Il doit alors lancer le navigateur pour accéder d'une part à la liste des services et ensuite aux services eux-mêmes. Selon un premier mode de réalisation, il lance le navigateur disponible sur le dispositif hôte. Ceci pose le problème que ce navigateur n'est pas sûr, il peut avoir été infecté par des logiciels espions ou autres.
- 10 Avantageusement, lors de la connexion du dispositif de sécurité, le module mémoire de masse 3.6 est vu par le système d'exploitation de l'hôte comme une clé USB. Avantageusement, cette mémoire est en lecture seule et propose alors une version du navigateur à l'utilisateur. C'est alors ce navigateur sauvegardé dans un espace protégé en écriture qui est lancé par l'utilisateur.
- 15 Lors d'une étape 5.2, l'utilisateur est invité à s'authentifier auprès du dispositif de sécurité. Cette authentification vise à éviter l'utilisation du dispositif par une personne non autorisée. Typiquement, ce dispositif est utilisé pour sécuriser l'accès à un ensemble de services pour un utilisateur et ne doit donc pouvoir être utilisé que par celui-ci. Cette authentification peut se faire par différents moyens. Un premier mode
- 20 de réalisation utilise une authentification par nom de connexion et mot de passe. L'utilisateur se connecte sur le serveur WEB hébergé par le dispositif de sécurité et charge une page d'authentification. Il entre son nom de connexion et son mot de passe. Le dispositif valide l'authentification et, si celle-ci est valide, il déverrouille le dispositif de sécurité pour en autoriser l'utilisation. Dans un second mode de
- 25 réalisation, le dispositif intègre un capteur biométrique, par exemple un lecteur d'empreinte digitale, mais tout autre capteur peut être utilisé comme un lecteur d'iris ou autre. L'authentification de l'utilisateur est alors faite à l'aide de ce capteur biométrique. Dans d'autres modes de réalisation, le dispositif de sécurité implémente des protocoles d'authentification tels que TLS ou RADIUS (*Remote Authentication*
- 30 *Dial In User Service* en anglais).

Lors d'une étape 5.3, l'utilisateur obtient la liste des services disponibles offerts par le dispositif de sécurité. Cette liste peut être réduite à un seul service. Avantageusement cette liste est fournie sous la forme d'une page WEB servie par le serveur WEB embarqué sur le dispositif de sécurité. Un autre protocole peut être

utilisé pour transmettre cette liste du dispositif de sécurité au dispositif hôte. Associé au nom du service est également transmis un lien d'accès au service, typiquement une adresse WEB.

5 Cette liste est soumise à l'utilisateur qui peut alors choisir l'un des services parmi la liste lors d'une étape 5.4. Ce choix provoque l'initialisation d'un processus de connexion au service sélectionné. Ces services étant typiquement sécurisés, l'initialisation débute par une étape d'authentification de l'utilisateur auprès du service choisi.

10 Pour réaliser cette authentification, l'utilisateur doit obtenir du dispositif de sécurité le crédit d'authentification associé au service. Ce crédit lui est typiquement associé. Il est stocké dans le dispositif au sein du module de sécurité, typiquement un composant de carte à puce.

15 D'une manière générale, c'est donc le navigateur qui va requérir et obtenir le crédit associé au service auprès du dispositif de sécurité lors de l'étape 5.5. La communication entre le navigateur et le dispositif peut être implémentée de plusieurs manières.

20 Selon un premier mode de réalisation, le navigateur est un navigateur standard qui peut être le navigateur usuel de l'utilisateur sur le dispositif de sécurité. Dans ce mode, une page est rendue disponible sur le dispositif de sécurité pour l'accès au service. Cette page comprend deux cadres (*frames* en anglais). Un premier cadre est appelé cadre de service et sert à la connexion entre le navigateur et le service distant. C'est ce cadre qui est visible pour l'utilisateur. Ce cadre correspond à la fenêtre habituelle d'accès à un service distant. Un second cadre, dit cadre de sécurité, sert à la communication entre le navigateur et le dispositif de sécurité. Ce cadre implémente un script de communication avec le dispositif. Il n'est typiquement pas visible dans la fenêtre de navigation. La communication entre le cadre de sécurité et le dispositif de sécurité peut être faite par exemple en HTTP avec le serveur WEB du dispositif. Avantageusement la communication est chiffrée, par exemple en utilisant le protocole HTTPS ou par un protocole propriétaire. Ce cadre de sécurité communique également avec le cadre de service.

30 Lors de la connexion au service distant, le cadre de service charge la page d'authentification au service distant. Lorsque ce chargement est terminé, il prévient le cadre de sécurité. Ce dernier requiert alors le crédit d'authentification auprès du dispositif de sécurité, typiquement un nom de connexion et un mot de passe. Lorsqu'il

les a reçus, il remplit les champs idoines du cadre de service avec les informations transmises. L'utilisateur valide ces champs et l'authentification peut alors avoir lieu de manière habituelle.

Selon un mode particulier de réalisation, la transmission des crédits
5 d'authentification du dispositif de sécurité vers le dispositif hôte est faite par le module 3.7 de simulation d'un clavier. Le nom de connexion et le mot de passe sont alors envoyés vers le cadre de service sous la forme d'une séquence de codes simulant l'appui sur les touches correspondantes du clavier. Il est à noter ici que le type de système d'exploitation est détecté par le dispositif de sécurité grâce aux en-têtes
10 HTTP des requêtes faites par le navigateur au dispositif de sécurité. En effet, les séquences de codes sont dépendantes du système d'exploitation du dispositif hôte. Avantageusement, selon ce mode de réalisation, il est fait usage de mots de passe à usage unique générés par le token. L'utilisation du module de simulation de clavier donne un certain contrôle à l'utilisateur sur ce que fait le dispositif de sécurité. De
15 plus, si la fonction de génération de mots de passe à usage unique peut être déclenchée par l'appui sur un bouton sur le dispositif de sécurité, il est alors possible pour l'utilisateur de générer ce type de mot de passe lorsqu'il le désire. Il peut également être utilisé pour éviter l'expiration d'une page du service distant en simulant une activité sous la forme d'un appui sur une touche. Il peut encore servir à fermer une
20 session ou redémarrer l'ordinateur hôte au besoin.

Ce mode de réalisation offre l'avantage de permettre l'usage d'un navigateur non modifié au prix d'une page intégrant les deux cadres programmés de manière appropriée disponible sur le dispositif de sécurité.

Selon un autre mode de réalisation, le navigateur est modifié pour intégrer
25 nativement dans son code un module de communication avec le dispositif de sécurité. Dans ce mode de réalisation, le choix des protocoles entre le navigateur et le dispositif de sécurité est libre. Il est alors permis de sécuriser ce protocole. On peut aussi alléger la communication en développant une pile de protocoles de communication plus légère du fait que l'on a le contrôle des deux interlocuteurs. Par contre, il n'est plus
30 possible d'utiliser un navigateur non modifié. Il faut donc que le navigateur modifié soit accessible à l'utilisateur. Avantageusement, il est rendu disponible dans le module de mémoire du dispositif de sécurité. Ce mode de réalisation est lié à la pile de protocoles dans le dispositif illustré à la Fig. 4b.

Quel que soit le mode de réalisation utilisé pour transmettre le crédit d'authentification au navigateur, lorsqu'il en dispose, il peut réaliser l'étape 5.6 de connexion au service. La communication se réalise alors de manière classique entre le service distant et le navigateur. Seule l'authentification ayant été sécurisée par le
5 dispositif de sécurité. L'utilisateur peut utiliser le service, étape 5.7.

Selon une variante de réalisation, tout ou partie de la communication entre le service distant et le navigateur est chiffré. Il peut s'agir d'un chiffrement partiel des données les plus sensibles ou du chiffrement total de la communication, on parle alors de tunnel sécurisé entre le navigateur et le service. Avantageusement, ce chiffrement
10 est effectué par le dispositif de sécurité à l'aide de crédits de chiffrement qui resteront stockés au sein du module de sécurité dudit dispositif de sécurité. L'échange des données à chiffrer ou à déchiffrer par le dispositif de sécurité est alors pris en charge soit par le cadre de sécurité soit par le module qui gère la communication avec le dispositif de sécurité selon le mode de réalisation adopté.

15 Lorsque l'utilisateur a terminé d'utiliser le service, intervient une étape de déconnexion 5.8. Cette étape peut être déclenchée par l'utilisateur au travers de l'interface du navigateur ou par déconnexion du dispositif de sécurité du dispositif hôte.

REVENDICATIONS

1/ Procédé de connexion à un service distant depuis un dispositif hôte caractérisé en ce qu'il comprend les étapes suivantes :

- 5 - une étape d'authentification de l'utilisateur auprès d'un dispositif de sécurité connecté sur le dispositif hôte ;
- une étape d'obtention d'une liste de services distants auprès dudit dispositif de sécurité ;
- une étape de choix d'un service parmi la liste de services distants obtenue ;
- 10 - une étape par ledit dispositif hôte de connexion et d'authentification de l'utilisateur auprès du service distant choisi à l'aide d'un crédit d'authentification stocké dans ledit dispositif de sécurité ;
- une étape de transmission du crédit d'authentification depuis le dispositif de sécurité au navigateur sous la forme d'une séquence de codes simulant l'appui sur les
- 15 touches d'un clavier.

2/ Procédé de connexion selon la revendication 1, caractérisé en ce que l'authentification de l'utilisateur auprès dudit dispositif de sécurité comprend les étapes suivantes :

- 20 - une étape de chargement d'une page d'authentification disponible sur ledit dispositif de sécurité dans un navigateur lancé sur le dispositif hôte ;
- une étape d'entrée de paramètres d'authentification dans ladite page d'authentification ;
- une étape de validation desdits paramètres d'authentification par ledit
- 25 dispositif de sécurité.

3/ Procédé de connexion selon la revendication 1, caractérisé en ce que l'authentification de l'utilisateur auprès dudit dispositif de sécurité comprend une étape d'authentification d'un paramètre biométrique de l'utilisateur par un capteur

30 biométrique intégré audit dispositif de sécurité.

4/ Procédé de connexion selon l'une des revendications 1 à 3, caractérisé en ce que l'étape d'obtention d'une liste de services distants comprend une étape de chargement dans un navigateur lancé sur le dispositif hôte d'une page disponible sur

ledit dispositif de sécurité, ladite page comprenant une liste de liens sur lesdits services distants.

5/ Procédé de connexion selon l'une des revendications 1 à 4, caractérisé en ce que l'étape de connexion et d'authentification de l'utilisateur auprès du service distant choisi comprend au sein d'un navigateur :

- une étape de connexion avec ledit dispositif de sécurité;
- une étape de connexion au service distant ;
- une étape de communication au service distant de crédit d'authentification obtenu dudit dispositif de sécurité ;

6/ Procédé de connexion selon la revendication 5, caractérisé en ce que l'étape de connexion au service distant comprend une étape de chargement d'une page disponible dans ledit dispositif de sécurité, ladite page comprenant un premier cadre dédié à la communication avec le service distant et un second cadre dédié à la communication avec ledit dispositif de sécurité lorsque ladite page est chargée dans un navigateur lancé sur le dispositif hôte.

7/ Procédé de connexion selon la revendication 5, caractérisé en ce que l'étape de connexion et de communication avec ledit dispositif de sécurité est faite selon un protocole particulier implémenté au sein du navigateur et du dispositif.

8/ Procédé de connexion selon l'une des revendications 6 ou 7, caractérisé en ce que le crédit d'authentification est transmis du dispositif de sécurité au navigateur sous la forme d'une page de données.

9/ Procédé de connexion selon l'une des revendications 1 à 8, caractérisé en ce qu'il comprend une étape préalable de chargement du navigateur utilisé pour la connexion depuis une mémoire de stockage dudit dispositif de sécurité.

10/ Procédé de connexion selon la revendication 9, caractérisé en ce qu'il comprend en outre une étape de chiffrement/déchiffrement d'au moins une partie des données échangées entre le navigateur et le service distant faite par ledit dispositif de sécurité.

11/ Dispositif de sécurité connectable à un dispositif hôte pour la connexion sécurisée à un service distant, caractérisé en ce qu'il comprend :

- 5 - un composant de carte à puce pour le stockage sécurisé de crédits d'authentification et les calculs cryptographiques ;
- une pile de protocoles de communication pour communiquer avec le dispositif hôte ;
- une liste de services distants avec les adresses de ces services et des crédits d'authentification de l'utilisateur auprès de ces services ;
- 10 - des moyens d'authentifier un utilisateur ;
- des moyens de transmettre au dispositif hôte la liste des services distants ;
- des moyens de transmettre au dispositif hôte le crédit d'authentification d'un service choisi sous la forme d'une séquence de codes simulant l'appui sur les touches d'un clavier.

15

12/ Dispositif de sécurité selon la revendication 11, caractérisé en ce qu'il comporte en outre une page d'authentification qu'il rend disponible auprès d'un navigateur lancé sur le dispositif hôte et des moyens de valider des paramètres d'authentification entrés par un utilisateur à l'aide de ladite page d'authentification.

20

13/ Dispositif de sécurité selon la revendication 11, caractérisé en ce qu'il comporte en outre un capteur biométrique pour l'authentification de l'utilisateur.

14 / Dispositif de sécurité selon l'une des revendications 11 à 13, caractérisé en ce qu'il comporte en outre une page disponible sur ledit dispositif de sécurité, ladite page comprenant une liste de liens sur lesdits services distants.

25

15/ Dispositif de sécurité selon l'une des revendications 11 à 14, caractérisé en ce qu'il comporte en outre une page disponible dans ledit dispositif de sécurité, ladite page comprenant un premier cadre dédié à la communication avec le service distant et un second cadre dédié à la communication avec ledit dispositif de sécurité lorsque ladite page est chargée dans un navigateur lancé sur le dispositif hôte.

30

16 / Dispositif de sécurité selon l'une des revendications 11 à 14, caractérisé en ce qu'il comporte des moyens pour communiquer avec le dispositif hôte selon un protocole particulier.

- 5 17/ Dispositif de sécurité selon l'une des revendications 11 à 16, caractérisé en ce qu'il comporte une mémoire de stockage pour mémoriser le navigateur destiné à être utilisé pour la connexion au service distant depuis le dispositif hôte.

- 10 18/ Dispositif de sécurité selon la revendication 17, caractérisé en ce qu'il comporte en outre des moyens de chiffrer/déchiffrer au moins une partie des données échangées entre le service distant et le navigateur.

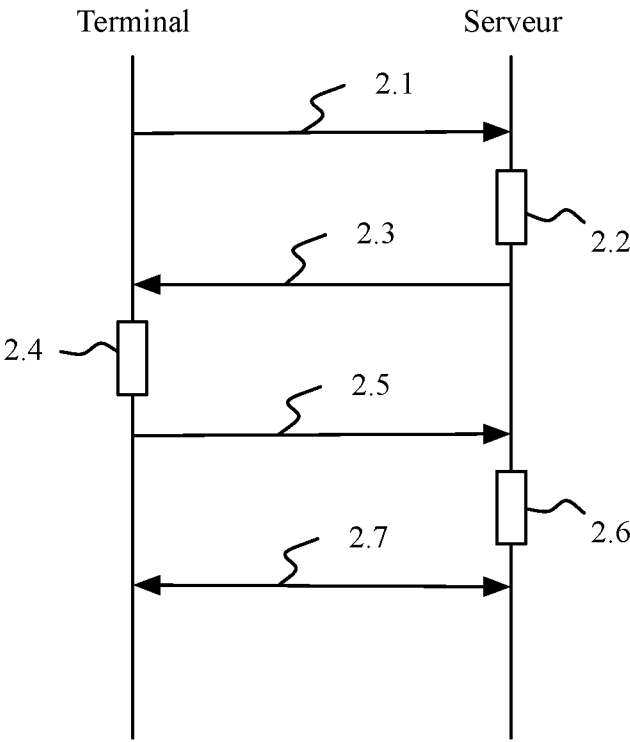
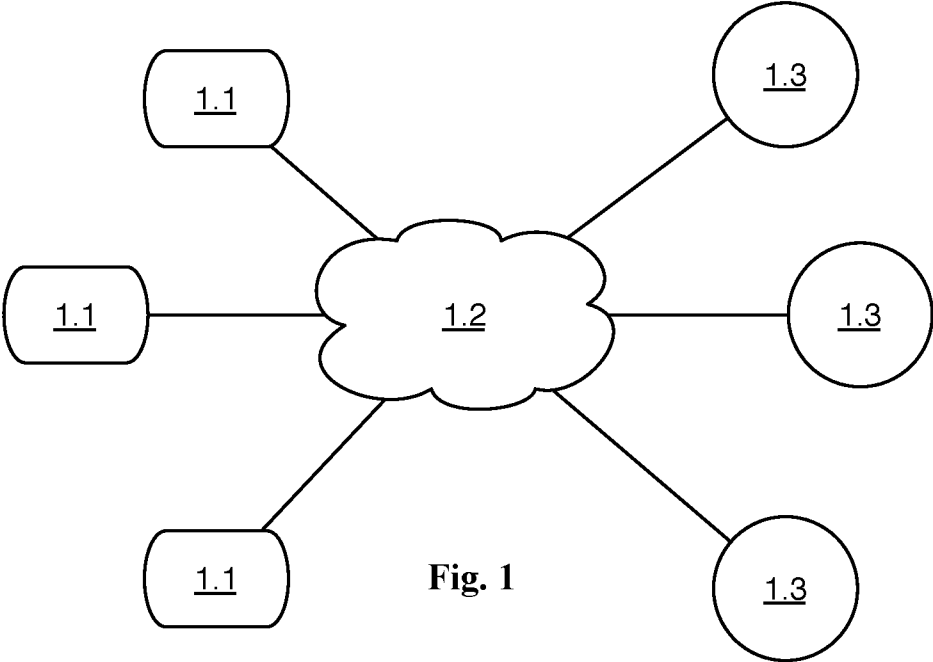


Fig. 2

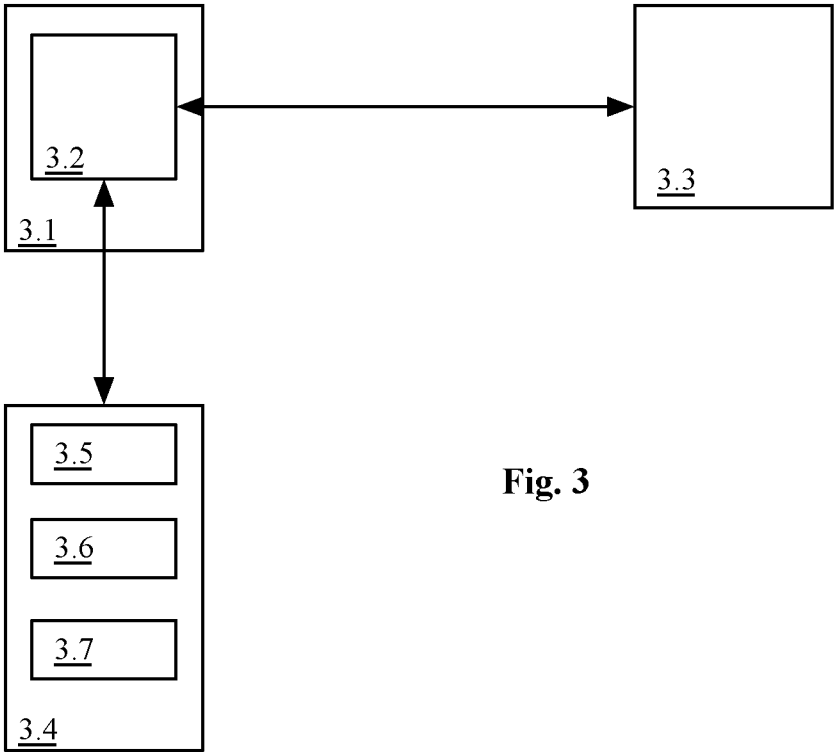


Fig. 3

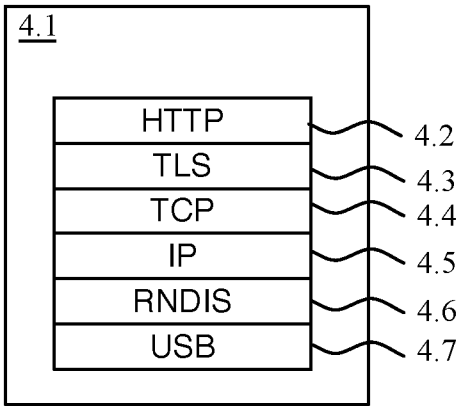


Fig. 4a

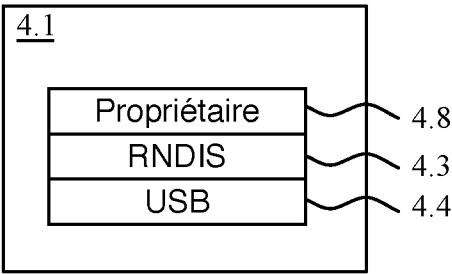
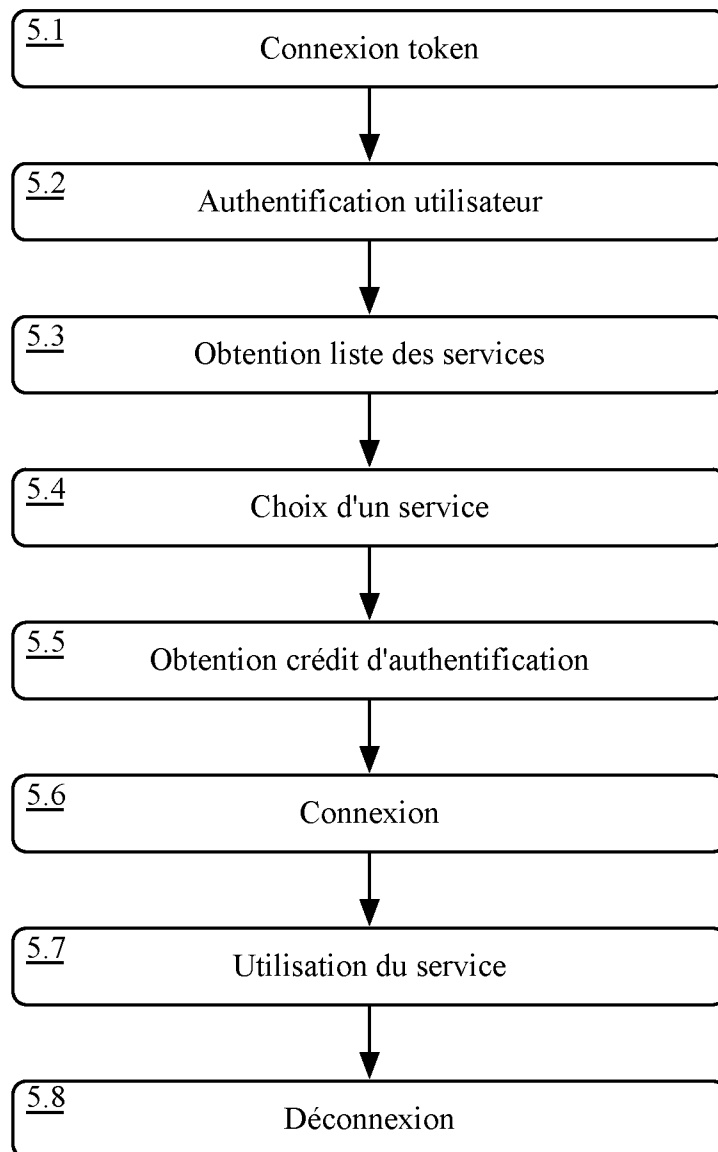


Fig. 4b

3/3

**Fig. 5**

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/051896

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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)
H04L

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)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2006/131897 A1 (AXALTO SA [FR]; MONTGOMERY MICHAEL A [FR]; ASAD MAHBOOB ALI [FR]) 14 December 2006 (2006-12-14) abstract; figure 1 page 5 page 7, line 19 - page 10, line 22 page 16, line 24 - page 18, line 21 -----	1-18
Y	WO 2007/122224 A1 (CYPAK AB [SE]; EHRENSVAERD JAKOB [SE]; EHRENSVAERD STINA [SE]) 1 November 2007 (2007-11-01) abstract page 3, line 17 - page 13, line 12 ----- -/--	1-18

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

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

16 April 2012

Date of mailing of the international search report

27/04/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Lebas, Yves

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/051896

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	GB 2 444 650 A (VISIBLE COMPUTING LTD [GB]) 11 June 2008 (2008-06-11) abstract page 11, line 31 - page 23, line 24 page 62, line 12 - page 66, last line -----	1-18
A	US 2005/071282 A1 (LU HONGQIAN KAREN [US] ET AL) 31 March 2005 (2005-03-31) abstract; figure 1a paragraph [0027] - paragraph [0055] paragraph [0069] - paragraph [0095] paragraph [0131] -----	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2012/051896

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006131897 A1	14-12-2006	US 2006282678 A1 WO 2006131897 A1	14-12-2006 14-12-2006
WO 2007122224 A1	01-11-2007	EP 2011052 A1 JP 2009534768 A US 2010199334 A1 WO 2007122224 A1	07-01-2009 24-09-2009 05-08-2010 01-11-2007
GB 2444650 A	11-06-2008	GB 2444650 A WO 2008068514 A1	11-06-2008 12-06-2008
US 2005071282 A1	31-03-2005	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2012/051896

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06
ADD.

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)
H04L

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, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 2006/131897 A1 (AXALTO SA [FR]; MONTGOMERY MICHAEL A [FR]; ASAD MAHBOOB ALI [FR]) 14 décembre 2006 (2006-12-14) abrégé; figure 1 page 5 page 7, ligne 19 - page 10, ligne 22 page 16, ligne 24 - page 18, ligne 21 -----	1-18
Y	WO 2007/122224 A1 (CYPACK AB [SE]; EHRENSVAERD JAKOB [SE]; EHRENSVAERD STINA [SE]) 1 novembre 2007 (2007-11-01) abrégé page 3, ligne 17 - page 13, ligne 12 ----- -/--	1-18

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

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

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

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

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

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

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

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant 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

16 avril 2012

Date d'expédition du présent rapport de recherche internationale

27/04/2012

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Lebas, Yves

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2012/051896

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	GB 2 444 650 A (VISIBLE COMPUTING LTD [GB]) 11 juin 2008 (2008-06-11) abrégé page 11, ligne 31 - page 23, ligne 24 page 62, ligne 12 - page 66, dernière ligne	1-18
A	----- US 2005/071282 A1 (LU HONGQIAN KAREN [US] ET AL) 31 mars 2005 (2005-03-31) abrégé; figure 1a alinéa [0027] - alinéa [0055] alinéa [0069] - alinéa [0095] alinéa [0131] -----	1-18

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2012/051896

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2006131897 A1	14-12-2006	US 2006282678 A1	14-12-2006
		WO 2006131897 A1	14-12-2006
-----		-----	
WO 2007122224 A1	01-11-2007	EP 2011052 A1	07-01-2009
		JP 2009534768 A	24-09-2009
		US 2010199334 A1	05-08-2010
		WO 2007122224 A1	01-11-2007
-----		-----	
GB 2444650 A	11-06-2008	GB 2444650 A	11-06-2008
		WO 2008068514 A1	12-06-2008
-----		-----	
US 2005071282 A1	31-03-2005	AUCUN	
-----		-----	