(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 140 688**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 10381**

(51) Int Cl[8] : ***G 06 F 21/34*** *(2023.01), H 04 W 12/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 11.10.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 12.04.24 Bulletin 24/15.

(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 :**

( ) **Demande(s) d'extension :**

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

(72) **Inventeur(s) :** MONCOMBLE Ghislain.

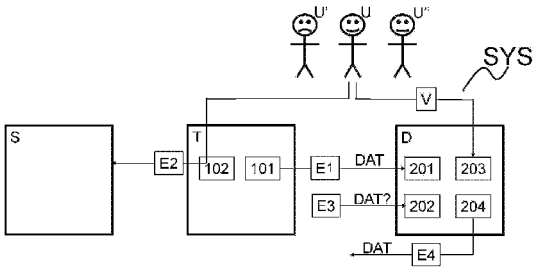
(73) **Titulaire(s) :** ORANGE Société anonyme.

(54) **Procédé de gestion de données d'authentification permettant l'accès à un service d'un utilisateur depuis un terminal.**

(57) Procédé de gestion de données d'authentification permettant l'accès à un service d'un utilisateur depuis un terminal
L'invention se rapporte à un procédé de gestion de données d'authentification (DAT) permettant l'accès à un service (S) d'un utilisateur (U) depuis un terminal (T), l'accès d'un utilisateur (U) requérant une fourniture au service (S) de données d'authentification (DAT), procédé qui comprend les étapes suivantes :

Une étape préalable de demande par ledit terminal (T) à un dispositif (D) distinct du terminal (T) de mémorisation (E1) de données d'authentification (DAT) d'un utilisateur (U) pour le service (S) ;Suite à une demande (E2) d'accès au service (S) par un utilisateur (U) donné depuis ledit terminal (T), une étape de réception (E3) par le dispositif (D) d'une requête d'obtention des données d'authentification (DAT) ;Une étape de validation (V) effectuée par l'utilisateur (U) sur le dispositif (D) ;En cas de réussite de l'étape de validation (V), une étape de fourniture (E4) par le dispositif (D) des données d'authentification (DAT).

Figure 1



FR 3 140 688 - A1

Description

Titre de l'invention : Procédé de gestion de données d'authentification permettant l'accès à un service d'un utilisateur depuis un terminal

Domaine technique

[0001] Le domaine technique est celui de l'authentification des utilisateurs d'un service.

[0002] Plus précisément, l'invention se rapporte à un procédé de gestion de données d'authentification permettant l'accès à un service d'un utilisateur depuis un terminal. Un tel procédé pourra être utilisé pour gérer les données d'authentification de plusieurs utilisateurs qui souhaitent accéder à des services distincts les uns des autres. Cependant, une caractéristique de l'invention est que le terminal permettant l'accès des utilisateurs aux services est apte à être partagé entre plusieurs utilisateurs.

[0003] Les services dont il est question sont par exemple des services Web, qu'il s'agisse de services à l'intention de particuliers ou de professionnels. Les données d'authentification dont il est question vont alors être dans la majorité des cas des identifiants et des mots de passe, mais peuvent également être des données biométriques, selon le mode d'authentification aux services, ou toute autre donnée utile à l'authentification, comme par exemple des jetons d'authentification (de l'anglais *authentication tokens*). D'autres modes de connexion des utilisateurs aux services sont possibles en sus d'une connexion selon le protocole http. On ne parlera pas alors de services Web, mais l'authentification au service se fera toujours depuis le terminal, en soumettant au service des données d'authentification propres à l'utilisateur du service, telles qu'une paire composée d'un identifiant et d'un mot de passe.

[0004] Les utilisateurs vont s'authentifier au service depuis un terminal. Il s'agit par exemple d'un ordinateur que celui-ci soit portable, ou bien fixe, mais cela peut également être une tablette ou bien un ordiphone (traduction de l'anglais *smartphone*). L'authentification de l'utilisateur à un service se fait alors en soumettant un identifiant puis un mot de passe. En général, les utilisateurs peuvent souhaiter se connecter à différents services depuis un même terminal. Il existera donc des données d'authentification différentes selon les services pour un même utilisateur.

[0005] Comme un utilisateur peut vouloir se connecter à de nombreux services, il existe un besoin de gestion des données d'authentification, afin que celle-ci ne repose pas entièrement sur la mémoire de l'utilisateur. Par ailleurs, les données d'authentification permettant de se connecter à un service qui peut donner accès à des données ou des fonctions confidentielles, la gestion de ces données d'authentification doit être sécurisée.

Etat de la technique

[0006] Une méthode bien établie de gestion des données d'authentification est la réalisation d'un coffre-fort à mots de passe. Un tel coffre-fort est une application logicielle qui va enregistrer dans un terminal un ensemble de données d'authentification, sous la forme de paires identifiant-mot de passe. D'autres données peuvent être éventuellement enregistrées. On peut également enregistrer des données d'authentification dans un fichier ou dans un espace disque d'un ordinateur, et en protéger l'accès par un mot de passe. Les jetons d'authentification sont également enregistrés dans des zones mémoire sécurisées.

[0007] Un tel coffre-fort va être typiquement développé en tant que module d'un navigateur Web. De cette manière, quand un utilisateur crée un compte sur un service et les données d'authentification associées par l'intermédiaire du navigateur Web, le module dédié à la gestion des données d'authentification pourra enregistrer celles-ci dans le terminal dans lequel s'exécute le navigateur Web. Cet enregistrement dans le terminal pourra se faire en utilisant des techniques de cryptographie pour assurer la protection des données d'authentification et assurer une gestion sécurisée de celles-ci. Quand un utilisateur va chercher à s'authentifier sur un service Web par l'intermédiaire du navigateur, service pour lequel les données d'authentification sont déjà enregistrées, le module du navigateur dédié à la gestion des données d'authentification pourra fournir le mot de passe enregistré dans le terminal afin de faciliter l'authentification de l'utilisateur. Cette fourniture se fera éventuellement après déchiffrement si celui-ci a été enregistré dans le terminal sous forme chiffrée pour assurer la sécurisation des données d'authentification.

[0008] Cette technologie est maintenant bien établie mais présente un inconvénient majeur quand plusieurs utilisateurs partagent un même terminal pour assurer leurs connexions à un ou plusieurs services. Cette situation peut se produire dans plusieurs contextes. Par exemple, dans un contexte familial, un seul ordinateur, ou tablette, voire même un seul ordiphone, peut être utilisé par tous les membres d'une famille pour leur connexion à des services sur lesquels ils doivent s'authentifier, comme des réseaux sociaux ou des sites marchands. Ou bien, dans un contexte professionnel, plusieurs employés situés dans un même local professionnel, par exemple des vendeurs dans une boutique, ou bien des mécaniciens dans un atelier, peuvent partager un ordinateur unique attaché au local pour accéder à des applications professionnelles sur lesquelles ils doivent s'authentifier. Comme il est impossible de garantir que chaque utilisateur effectue une sortie de session après son interaction avec le terminal partagé, un autre utilisateur peut accéder aux données qui permettent l'authentification aux services.

[0009] Dans ces deux contextes familial et professionnel, l'accès aux services implique un

besoin de confidentialité. Un utilisateur ne doit pas pouvoir connaître les données d'authentification d'un autre utilisateur, ou bien ne doit pas pouvoir utiliser les données d'un autre utilisateur pour se connecter à un service en usurpant son identité. Or, un module du navigateur Web qui remplit le rôle de coffre-fort à mots de passe ne satisfait pas cette exigence, car il est impossible de garantir que chaque utilisateur quittera sa session après avoir utilisé un terminal partagé. En effet, rien n'empêche un utilisateur de consulter les données d'authentification de tous les utilisateurs, données enregistrées par le navigateur Web du terminal partagé par les différents utilisateurs. Ces données d'authentification peuvent être ou bien consultées ou bien même utilisées directement pour effectuer l'authentification. Dans ce cas, un utilisateur peut usurper l'identité de n'importe quel utilisateur qui partage le terminal, et donc qui partage le navigateur et le module de celui-ci qui sert de coffre-fort à mots de passe.

[0010] Un autre inconvénient de la technologie existante est qu'elle n'est pas adaptée quand un utilisateur dispose de plusieurs terminaux. Quand les données d'authentification d'un utilisateur sont enregistrées dans un coffre-fort à mots de passe ou dans un fichier ou espace disque dédié, ces données ne sont présentes que dans un seul terminal. Quand l'utilisateur change de terminal, il ne peut pas a priori accéder aux données d'authentification enregistrées dans un autre terminal.

[0011] L'invention vient améliorer la situation.

L'invention

[0012] Selon un premier aspect fonctionnel, l'invention a trait à un procédé de gestion de données d'authentification permettant l'accès à un service d'un utilisateur depuis un terminal, l'accès d'un utilisateur donné à un service requérant une fourniture au service de données d'authentification relatives audit utilisateur, procédé caractérisé en ce qu'il comprend les étapes suivantes :

- Une étape préalable de demande par ledit terminal à un dispositif distinct du terminal de mémorisation de données d'authentification d'un utilisateur pour le service ;
- Suite à une demande d'accès au service par un utilisateur donné depuis ledit terminal, une étape de réception par le dispositif d'une requête d'obtention des données d'authentification de l'utilisateur donné pour le service ;
- Une étape de validation effectuée par l'utilisateur sur le dispositif ;
- En cas de réussite de l'étape de validation, une étape de fourniture par le dispositif des données d'authentification de l'utilisateur donné pour le service.

[0013] Grâce à l'invention, l'utilisateur ne doit plus mémoriser les données d'authentification qui lui permettent d'accéder au service. Celles-ci, à la suite d'une demande du terminal, sont mémorisées par un dispositif distinct du terminal. Ces données seront ensuite fournies, après une étape de validation effectuée par

l'utilisateur, ce qui permettra l'accès de l'utilisateur au service depuis le terminal.

[0014] Le dispositif qui mémorise les données d'authentification est distinct du terminal. Ce point donne un deuxième avantage au procédé. Le terminal peut être partagé entre plusieurs utilisateurs pour permettre l'accès au service. Mais les données d'authentification ne sont pas mémorisées dans le terminal mais dans un dispositif distinct. Dans une situation privilégiée, un utilisateur disposera d'un dispositif personnel, comme on le verra ultérieurement. Dans ce cas, qui sera le standard d'utilisation du procédé, les données d'authentification d'un utilisateur seront mémorisées dans le dispositif personnel de l'utilisateur et ne pourront pas être vues ou utilisées par les utilisateurs qui partagent le terminal pour accéder au service.

[0015] Un autre avantage du procédé est que les données d'authentification présentes dans le dispositif pourront être utilisées dans plusieurs terminaux. Un utilisateur pourra donc changer de terminal et il lui sera possible de retrouver ses données d'authentification en utilisant un dispositif dans lequel elles auront été mémorisées.

[0016] L'étape de validation donne un autre avantage au procédé, à savoir que l'utilisateur va pouvoir contrôler l'utilisation des données d'authentification qui lui sont propres et qui lui permettent d'accéder à un service. Le fait que celles-ci soient mémorisées dans un dispositif, qui peut être lui aussi propre à l'utilisateur, n'assure pas une protection suffisante en l'absence d'un contrôle de l'usage de ses données par l'utilisateur. En effet, d'autres utilisateurs qui auraient accès au dispositif pourraient en extraire des données d'authentification pour les utiliser pour accéder au service en usurpant l'identité de l'utilisateur légitime. Pour éviter cela, une phase de validation est demandée à l'utilisateur, qui permettra d'extraire les données d'authentification de l'utilisateur du dispositif, pour que l'utilisateur accède bien au service.

[0017] Selon un premier mode de mise en œuvre particulier de l'invention, l'étape de validation comprend une étape préalable de mémorisation d'une base de correspondances entre des identifiants d'utilisateur et des données d'identification respectives, et en ce que l'étape de validation réussit, ce qui permet la fourniture par le dispositif des données d'authentification d'un utilisateur donné, après l'exécution des étapes suivantes :

- Obtention d'une donnée d'identification par le dispositif ;
- Détermination d'un identifiant d'utilisateur correspondant dans la base mémorisée à la donnée d'identification obtenue ;
- Vérification que l'identifiant d'utilisateur déterminé correspond bien à l'utilisateur donné.

[0018] Grâce à ce premier mode, l'étape de validation réalise bien un contrôle de l'identité de l'utilisateur afin de garantir que la fourniture par le dispositif des données d'authentification d'un utilisateur donné ne se produit qu'après une validation

effectuée par ledit utilisateur. C'est donc bien l'utilisateur légitime qui valide l'utilisation de ses données d'authentification et leur fourniture par le dispositif externe. Si jamais un utilisateur malveillant met la main sur le dispositif d'un utilisateur donné, la phase de validation telle que précisée dans ce mode de réalisation va empêcher l'utilisateur malveillant d'accéder aux données d'authentification auxquelles il n'a pas droit.

[0019] Il est également possible grâce à ce mode de réalisation d'envisager un fonctionnement dans lequel un dispositif distinct est partagé entre plusieurs utilisateurs. Dans ce cas, la phase de validation permettra d'attribuer à un utilisateur donné les données d'authentification mémorisées par le dispositif qui lui sont propres afin d'éviter de mauvaises attributions ou des usurpations de données. Dans ce mode de réalisation, un dispositif distinct du terminal est à la disposition de plusieurs utilisateurs, et les données d'authentification d'un utilisateur donné sont mémorisées dans une zone de mémoire déterminée du dispositif, zone de mémoire cloisonnée vis-à-vis des autres zones de mémoire du dispositif, ladite zone de mémoire déterminée comprenant les données d'authentification dudit utilisateur. De cette manière, un accès à une zone du dispositif partagé par plusieurs utilisateurs ne permet pas d'accéder aux données d'autres utilisateurs, données mémorisées dans d'autres zones.

[0020] Selon un deuxième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec le premier mode, l'étape de validation comprend une étape préalable de mémorisation d'une base de correspondances entre des identifiants de terminal et des données d'identification respectives, et en ce que l'étape de validation réussit, ce qui permet la fourniture par le dispositif des données d'authentification d'un utilisateur donné, après l'exécution des étapes suivantes :

- Obtention d'une donnée d'identification par le dispositif ;
- Détermination d'un identifiant de terminal correspondant dans la base mémorisée à la donnée d'identification obtenue ;
- Vérification que l'identifiant de terminal déterminé correspond bien à l'utilisateur donné

[0021] Dans ce mode de réalisation, l'étape de validation consiste pour le dispositif à vérifier qu'il interagit bien avec le terminal attendu. L'étape préalable de mémorisation d'identifiants de terminal peut être réalisée par exemple par un processus d'appairage du terminal et du dispositif. Dans tous les cas, l'étape de validation va être effectuée par l'utilisateur sur le dispositif ; l'étape de validation peut consister juste en le branchement par l'utilisateur du dispositif sur le terminal, le dispositif vérifiant alors qu'il interagit avec le terminal attendu.

[0022] L'avantage de ce mode de réalisation peut être de simplifier l'étape de validation. Après une étape préalable d'appairage, le dispositif pourra fournir les données

d'authentification uniquement après présentation du dispositif au terminal. De cette manière, la fourniture des données d'authentification est accélérée tout en restant contrôlée par l'utilisateur qui choisit bien le terminal auquel il connecte le dispositif.

[0023] Les deux modes de réalisation précédents peuvent être combinés. Dans ce cas, la validation consiste à la fois en une identification de l'utilisateur et du terminal par le dispositif avant de fournir les données d'authentification. De cette manière, la sécurité est améliorée pour ces données.

[0024] Selon un troisième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec les deux premiers modes, la requête d'obtention des données d'authentification d'un utilisateur reçue par le dispositif est en provenance du terminal ; et la fourniture par le dispositif des données d'authentification d'un utilisateur est à destination du terminal.

[0025] Grâce à ce mode de mise en œuvre particulier de l'invention, quand l'utilisateur va vouloir accéder au service depuis le terminal, celui-ci va requêter le dispositif distinct dans lequel les données d'authentification nécessaires pour que l'utilisateur accède au service sont mémorisées, et le dispositif va fournir ces données au terminal après qu'ait eu lieu l'étape de validation effectuée par l'utilisateur sur le dispositif. Le terminal pourra ensuite soumettre ces données d'authentification au service, et si elles sont correctes, l'utilisateur va bien pouvoir accéder au service depuis le terminal.

[0026] Selon un quatrième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec les deux premiers modes, la requête d'obtention des données d'authentification d'un utilisateur reçue par le dispositif est en provenance du terminal ; et la fourniture par le dispositif des données d'authentification d'un utilisateur est à destination du service.

[0027] Grâce à ce mode de mise en œuvre, quand un utilisateur souhaite accéder au service depuis le terminal, celui-ci va demander au dispositif de fournir les données d'authentification de l'utilisateur et le dispositif, après une étape de validation par l'utilisateur, va adresser directement au service les données d'authentification nécessaires pour que l'utilisateur puisse accéder au service. Cette fourniture se fait directement depuis le dispositif au service, sans passer par l'intermédiaire du terminal. Ceci permet d'assurer une plus grande protection des données d'authentification vis-à-vis du terminal. Ces données ne transitent pas par le terminal, qui peut être partagé entre plusieurs utilisateurs, pour être soumises au service, ce qui permet d'éviter que des logiciels malveillants qui pourraient être installés sur le terminal puissent accéder à ces données d'authentification pour les transmettre à des utilisateurs malveillants.

[0028] Selon un cinquième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec les deux premiers modes, la requête d'obtention des données d'authentification d'un utilisateur reçue par le dispositif est en provenance

du service ; et la fourniture par le dispositif des données d'authentification d'un utilisateur est à destination du service.

[0029] Dans ce mode de mise en œuvre, lorsqu'un utilisateur essaie d'accéder au service depuis le terminal, le service va directement solliciter le dispositif et celui-ci va lui fournir directement les données d'authentification nécessaires à l'accès de l'utilisateur au service. Ce mode de mise en œuvre permet de complètement contourner le terminal pour la fourniture de données d'authentification au service, ce qui sécurise encore davantage celles-ci. En effet, le terminal pouvant être partagé entre plusieurs utilisateurs, on peut estimer que des logiciels malveillants peuvent être installés sur celui-ci et permettre d'accéder à ces données d'authentification pour les transmettre à des utilisateurs malveillants. Ce mode de réalisation qui contourne le terminal évite ce risque. Une fois les données d'authentification fournies au service, l'utilisateur accèdera bien au service et interagira avec celui-ci depuis le terminal.

[0030] Selon un sixième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec les deux premiers modes, la requête d'obtention des données d'authentification d'un utilisateur reçue par le dispositif est en provenance du service ; et la fourniture par le dispositif des données d'authentification d'un utilisateur est à destination du terminal.

[0031] Grâce à ce mode de mise en œuvre, le service va requêter directement le dispositif pour qu'il fournisse les données d'authentification de l'utilisateur, mais ces données transiteront par le terminal avant d'être adressées au service. De cette manière, l'accès de l'utilisateur au service se fait plus directement via le terminal. Cependant, la requête directe depuis le service permet d'accélérer la fourniture des données d'authentification par le dispositif.

[0032] Selon un septième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec le troisième ou le sixième mode, après la fourniture par le dispositif des données d'authentification à destination du terminal, le terminal utilise les données d'authentification pour compléter l'accès demandé au service par un utilisateur depuis le terminal, puis le terminal efface lesdites données d'authentification de l'ensemble des zones mémoire du terminal.

[0033] Grâce à ce mode de mise en œuvre, le procédé de gestion permet d'assurer la connexion de l'utilisateur au service depuis le terminal et assure en même temps que les données d'authentification ne sont pas mémorisées dans le terminal. Les données d'authentification, dans ce mode, ne font que transiter depuis le dispositif par le terminal vers le service, et ne sont pas conservées en mémoire dans le terminal. De cette façon, le risque de détournement des données d'authentification depuis le terminal est limité et la sécurité des données d'authentification est améliorée.

[0034] Selon un huitième mode de mise en œuvre particulier de l'invention, qui pourra être

mis en œuvre cumulativement avec les deux premiers modes, l'étape de fourniture par le dispositif des données d'authentification d'un utilisateur donné consiste en l'affichage par le dispositif des données.

[0035] Grâce à ce mode de réalisation, le dispositif affiche les données d'authentification, à charge pour l'utilisateur de les mémoriser et les transcrire ensuite pour réaliser son accès au service. L'intérêt de ce mode de réalisation est de garantir que les données d'authentification ne sont jamais exportées en dehors du dispositif et restent ainsi protégées d'éventuels attaquants.

[0036] Selon un neuvième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec les modes précédents, l'étape préalable de mémorisation de données d'authentification d'un utilisateur pour le service est déclenchée par une interaction directe de l'utilisateur avec le dispositif.

[0037] Grâce à ce mode de réalisation, les données d'authentification sont entrées directement par l'utilisateur dans le dispositif. Un avantage de ce mode de réalisation est là encore d'assurer que les données d'authentification ne sont jamais accessibles en dehors du dispositif. Ces données sont entrées directement par l'utilisateur dans le dispositif, ce qui assure leur confidentialité et leur protection contre d'éventuels attaquants.

[0038] Selon un dixième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre cumulativement avec les modes précédents, l'étape de fourniture par le dispositif des données d'authentification de l'utilisateur consiste en un transfert d'informations relatives aux données d'authentification de l'utilisateur pour différents services vers le terminal.

[0039] Grâce à ce mode de réalisation, il va être possible à l'utilisateur d'exporter tout un ensemble d'informations relatives aux données d'authentification dans un terminal. Ces informations peuvent comprendre des données d'authentification, mais seront en général limitées aux identifiants de service dont les données d'authentification sont mémorisées dans le dispositif. De cette manière, il sera possible à un utilisateur d'utiliser plusieurs terminaux pour accéder à des services et de centraliser la gestion des données d'authentification dans un seul dispositif. L'exportation des informations relatives aux données d'authentification permet ainsi à un utilisateur de changer de terminal tout en conservant ses données d'authentification puisque celles-ci restent centralisées dans le dispositif. Le dispositif peut gérer l'export d'informations relatives aux données d'authentification en catégorisant les terminaux en plusieurs types distincts (ordinateurs, tablettes, ordiphones), ce qui permet par exemple de disposer de données d'authentification dédiées à un type de terminal. L'utilisateur peut ainsi sélectionner des services pour lesquels il ne souhaite pas que les données d'authentification puissent transiter par le terminal.

[0040] Dans les modes présentés précédemment, l'étape de fourniture par le dispositif des données d'authentification a lieu après la réussite de l'étape de validation. Selon les deux premiers modes présentés, cette étape de validation peut comprendre l'identification de l'utilisateur, ou bien du terminal, ou bien des deux.

[0041] Selon un premier aspect matériel, l'invention a trait à un système comprenant un terminal apte à accéder à un service, l'accès au service d'un utilisateur donné requérant une fourniture au service de données d'authentification relatives audit utilisateur, caractérisé en ce que le système comprend en outre un dispositif distinct du terminal, et en ce que le terminal comprend les modules suivants :

- Un module de demande au dispositif de mémorisation de données d'authentification d'un utilisateur pour le service ;
- Un module de demande d'accès au service par un utilisateur ; et en ce que le dispositif comprend les modules suivants :
- Un module de mémorisation de données d'authentification ;
- Un module de réception d'une requête d'obtention de données d'authentification d'un utilisateur donné pour le service ;
- Un module de validation par un utilisateur de la fourniture de données d'authentification ;
- Un module de fourniture de données d'authentification.

[0042] Grâce à cet aspect matériel, des utilisateurs peuvent accéder à un service via un terminal apte à être partagé entre plusieurs utilisateurs, mais comme le terminal demande que les données d'authentification des utilisateurs soient mémorisées dans des dispositifs distincts, les accès non autorisés des utilisateurs à d'autres données d'authentification que les leurs sur le terminal ne sont pas possibles. Les données d'authentification personnelles des utilisateurs sont mémorisées par des dispositifs distincts du terminal apte à être partagé entre les utilisateurs, et la confidentialité des données d'authentification ne pourra donc pas être compromise du fait du partage du terminal d'accès au service entre plusieurs utilisateurs.

[0043] De plus, le dispositif peut être personnel et dédié à un utilisateur donné, ce qui lui permet d'utiliser plusieurs terminaux mais de gérer les données d'authentification en utilisant uniquement un dispositif personnel et en exportant les données d'authentification vers différents terminaux selon leur type et selon ses besoins.

[0044] Selon un autre aspect matériel, l'invention a trait à un programme d'ordinateur apte à être mis en œuvre par un terminal, le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur, réalise les étapes effectuées par le terminal du procédé de gestion défini ci-dessus.

[0045] Selon un autre aspect matériel, l'invention a trait à un programme d'ordinateur apte à être mis en œuvre par un dispositif, le programme comprenant des instructions de code

qui, lorsqu'il est exécuté par un processeur, réalise les étapes effectuées par le dispositif du procédé de gestion défini ci-dessus.

[0046] Enfin, selon un autre aspect matériel, l'invention a trait à des supports de données sur lesquels sont enregistrés des programmes d'ordinateurs comprenant des séquences d'instructions pour la mise en œuvre des procédés d'accès et de gestion définis ci-dessus.

[0047] Les supports de données peuvent être n'importe quelle entité ou dispositif capable de stocker les programmes. Par exemple, les supports peuvent comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit micro-électronique, ou encore un moyen d'enregistrement magnétique tel qu'un un disque dur. D'autre part, les supports peuvent être des supports transmissibles tels qu'un signal électrique ou optique, qui peuvent être acheminés via un câble électrique ou optique, par radio ou par d'autres moyens. Les programmes selon l'invention peuvent être en particulier téléchargés sur un réseau de type Internet. Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

[0048] Il est important de préciser que la présentation de l'invention a été faite ici en parlant de l'accès des utilisateurs à un service depuis un terminal, mais l'invention peut bien sûr s'appliquer également dans une situation où un terminal permet à des utilisateurs d'accéder à plusieurs services. Dans ce cas, les données d'authentification doivent être attribuées comme permettant l'accès d'un utilisateur donné à un service donné, afin que les dispositifs distincts fournissent les données appropriées permettant l'accès d'un utilisateur donné à un service donné suite à une demande d'accès au service. Ces attributions de données d'authentification à différents services sont bien connues de l'état de l'art, par exemple dans les modules de gestion de mots de passe par les navigateurs Web et ne seront pas détaillées davantage ici.

[0049] De même, la présentation de l'invention a été faite ici en parlant d'un terminal apte à être partagé entre plusieurs utilisateurs. Il est clair que l'invention s'applique également quand plusieurs terminaux sont partagés entre plusieurs utilisateurs, sans avoir une identité de nombre entre les deux, comme on le verra plus loin dans la description. En particulier, l'invention peut également s'appliquer quand un utilisateur utilise plusieurs terminaux pour accéder à différents services. Grâce à l'invention, l'utilisateur peut disposer d'un dispositif dédié personnel avec lequel il pourra réaliser la gestion de ses données d'authentification à un endroit unique au lieu de devoir l'effectuer de façon séparée dans les différents terminaux qu'il utilise. De cette manière, les données d'authentification sont toujours à jour, protégées contre d'éventuels attaquants, et les informations relatives aux données d'authentification sont

facilement exportables vers un nouveau terminal quand l'utilisateur en utilise un nouveau.

[0050] L'invention sera mieux comprise à la lecture de la description qui suit, donnée à titre d'exemple, et faite en référence aux dessins annexées sur lesquels :

[0051] [Fig.1] représente un système comprenant un terminal permettant à des utilisateurs d'accéder à un service, ainsi qu'un dispositif distinct du terminal, l'ensemble illustrant un exemple de réalisation de l'invention.

[0052] [Fig.2] illustre un exemple d'étapes mises en œuvre dans le cadre d'un mode de réalisation de l'invention.

[0053] [Fig.3] illustre un autre exemple d'étapes mises en œuvre dans le cadre d'un autre mode de réalisation de l'invention.

[0054] [Fig.4] illustre un autre exemple d'étapes mises en œuvre dans le cadre d'un autre mode de réalisation de l'invention.

[0055] [Fig.5] illustre un autre exemple d'étapes mises en œuvre dans le cadre d'un autre mode de réalisation de l'invention.

[0056] [Fig.6] illustre un autre exemple d'étapes mises en œuvre dans le cadre d'un autre mode de réalisation de l'invention.

[0057] [Fig.7] illustre un autre exemple d'étapes mises en œuvre dans le cadre d'un autre mode de réalisation de l'invention.

[0058] [Fig.8] illustre un autre exemple d'étapes mises en œuvre dans le cadre d'un autre mode de réalisation de l'invention.

[0059] La [Fig.1] représente un système informatique SYS comprenant un terminal T et un dispositif D distinct du terminal T. Le terminal T est apte à être partagé entre plusieurs utilisateurs U, U', U'' afin de leur permettre d'accéder à un service S.

[0060] Le service S est un service informatique. Il est rendu par un serveur (non représenté sur la figure). Il peut s'agir par exemple d'un service Web et sera alors accédé par des requêtes du protocole http, et fournira ses réponses par le même protocole. Le service S est accédé par des utilisateurs U, U', U'' et doit procéder à une authentification des utilisateurs U, U', U'' pour fournir les informations et perpétrer les actions adaptées à un utilisateur U donné. L'authentification d'un utilisateur U donné se fait grâce à la fourniture au service de données d'authentification DAT propres à un utilisateur U donné. Ces données d'authentification DAT seront en général constituées par une paire comprenant d'une part un identifiant de l'utilisateur U donné et d'autre part un mot de passe connu de l'utilisateur U. Le service S vérifiera alors que le mot de passe fourni dans les données d'authentification DAT est bien celui attendu pour l'utilisateur U donné et permettra alors l'accès de l'utilisateur U au service S. D'autres données d'authentification DAT peuvent être par exemple des données relatives à une identification biométrique. Le service S, plutôt que d'être accessible par un navigateur Web,

pourra être accessible depuis un terminal de type ordiphone via une application mobile qui interroge le service S hébergé par un serveur distant. L'application mobile devra alors fournir un mot de passe, ce mot de passe étant soit mémorisé par l'application, soit fourni par l'utilisateur U suivant les cas. Dans le cas où le service S est un service Web, ou bien est accessible par une application mobile, les données d'authentification DAT peuvent plutôt comprendre un ou plusieurs jetons d'authentification (en anglais, *authentication tokens*) qui enregistrent une connexion passée de l'utilisateur U sur le service S et l'autorisation donnée de se connecter au service S uniquement en présentant le jeton d'authentification sans fournir de nouveau le mot de passe. Le service S peut aussi être un service tel que la fourniture d'une API (acronyme pour l'anglais *Application Programming Interface*) et les données d'authentification pourront alors être des données telles que des mots de passe ou des clés de chiffrement demandées par l'API pour pouvoir y accéder et effectuer des requêtes sur cette interface, ou bien encore des jetons d'authentification. Ces notions sont bien connues de l'état de l'art et nous ne détaillerons pas davantage la nature du service S ni celle des données d'authentification DAT.

[0061] Le terminal T sera en général un ordinateur. Il pourra également être une tablette ou un ordiphone, mais dans tous les cas, le terminal T présente l'architecture matérielle d'un ordinateur conventionnel. Il comporte notamment un processeur, une mémoire vive de type RAM et une mémoire morte telle qu'une mémoire de type Flash, ROM, (non représentés sur la figure) ainsi que des dispositifs d'entrée-sortie tels que claviers et/ou écrans (non représentés sur la figure).

[0062] Le terminal T permet aux utilisateurs U, U', U'' d'accéder au service S. Pour cela, le terminal T va d'abord permettre aux utilisateurs U, U', U'' de gérer leurs données d'authentification DAT respectives.

[0063] Comme on l'a déjà vu, dans l'état de l'art, le terminal T sera par exemple un ordinateur qui permet d'accéder au service via un navigateur Web, et la gestion des mots de passe se fait via un module dédié du navigateur. Dans la présente invention, certains éléments d'un tel module dédié peuvent être conservés, comme par exemple un élément de génération aléatoire de mots de passe ou bien de détection des interfaces de service demandant la fourniture de mots de passe. Ces éléments sont bien connus de l'état de l'art et ne sont pas détaillés plus avant.

[0064] Selon l'invention, le terminal T comprend un module 101 de demande au dispositif D de mémorisation E1 de données d'authentification DAT d'un utilisateur U donné. Ce module travaillera avec par exemple un module dédié de gestion de mots de passe présent dans le navigateur Web du terminal T. Quand un utilisateur U se connectera pour la première fois au service S, le navigateur Web du terminal T pourra détecter le mot de passe créé par l'utilisateur U, ou pourra lui en suggérer un. Mais selon

l'invention, la mémorisation du mot de passe de l'utilisateur U sera demandée E1 par le module 101 du terminal T au dispositif D distinct du terminal T. Ceci aura également lieu à chaque modification du mot de passe de l'utilisateur U pour le service S et en général à tout moment où il sera pertinent de mémoriser E1 des données d'authentification DAT.

[0065] De cette manière, l'invention permet de mémoriser les données d'authentification DAT en dehors du terminal T apte à être partagé par les utilisateurs U, U', U''. Grâce à cette mémorisation hors du terminal T, les données d'authentification DAT sont mieux protégées d'éventuels utilisateurs malveillants qui chercheraient à accéder au service S à la place d'un utilisateur U donné.

[0066] Dans des modes de réalisation, les données d'authentification DAT permettant l'accès d'un utilisateur U au service S depuis un terminal T comprennent des éléments permettant d'identifier le service S. Ces éléments permettront par exemple d'identifier automatiquement un service S afin que, lorsqu'une requête des données d'authentification DAT est faite au dispositif D, seules celles concernant l'accès au service S sont fournies.

[0067] Dans des modes de réalisation, les données d'authentification DAT permettant l'accès d'un utilisateur U au service S depuis un terminal T comprennent des éléments permettant d'identifier le terminal T. Ces éléments peuvent être par exemple une adresse MAC (acronyme pour l'anglais *Media Access Control*) ou bien un numéro IMEI (acronyme pour l'anglais *International Mobile Equipment Identity*). L'identifiant du terminal T ajouté aux données d'authentification DAT permettra là aussi au dispositif de filtrer les données d'authentification DAT fournies selon le terminal T qu'elles concernent. Des catégories de terminaux T peuvent également être identifiées afin de classer les données d'authentification DAT selon les types de terminaux T pour lesquels elles sont demandées.

[0068] Le terminal T comprend également un module 102 de demande E2 d'accès au service S par un utilisateur U. Le module 102 peut être par exemple un composant d'un navigateur Web grâce auquel l'utilisateur U va accéder au service S.

[0069] Le système SYS comprend également un dispositif D distinct du terminal T.

[0070] Le dispositif D comprend des éléments, non représentés sur la [Fig.1], tels qu'un processeur, une mémoire vive de type RAM et une mémoire morte telle qu'une mémoire de type Flash, ROM, (non représentés sur la figure), afin de pouvoir effectuer les opérations selon l'invention.

[0071] Le dispositif D pourrait par exemple être un ordinateur distinct du terminal T, ou bien un ordiphone. Cependant, bien d'autres modes de réalisation sont également possibles. Par exemple, le dispositif D pourrait être un dispositif dédié attribué à un utilisateur U donné. Ce dispositif D pourrait être uniquement dédié à remplir les

opérations selon l'invention, à savoir la mémorisation E1 de données d'authentification DAT et leur fourniture E4 en temps voulu après une validation V. Le dispositif D pourrait également remplir certaines fonctions en sus de celles de l'invention. Par exemple, le dispositif D attribué à un utilisateur U donné pourrait être un dispositif de pointage tel qu'une souris que l'utilisateur U connectera au terminal T lorsqu'il voudra mettre en œuvre l'invention, et qui lui servira à la fois comme dispositif de pointage pour le terminal T et comme dispositif mettant en œuvre l'invention. Dans ce mode de réalisation de l'invention, le terminal T est partagé entre plusieurs utilisateurs U, U', U'' qui disposent chacun d'un dispositif D distinct qui leur est attribué.

[0072] Le dispositif D attribué à l'utilisateur U peut aussi être un dispositif du type clé USB (acronyme anglais de *Universal Serial Bus*) qui permet de mémoriser tous types de données.

[0073] Le dispositif D peut comprendre ou pas des composants tels que des claviers ou des écrans qui permettent à l'utilisateur U d'interagir directement avec le dispositif D. Certains modes de réalisation de l'invention imposent la présence de tels composants d'interaction et seront signalés comme tels par la suite.

[0074] Bien entendu, des utilisateurs peuvent ne pas disposer de dispositif D et devront donc gérer et mémoriser leurs données d'authentification DAT selon un des états de l'art antérieur.

[0075] Le dispositif D comprend un module 201 de mémorisation E1 de données d'authentification DAT d'un utilisateur U pour le service S.

[0076] Comme on a vu précédemment, le module 101 du terminal T va demander au dispositif D la mémorisation E1 de données d'authentification DAT, par exemple quand l'utilisateur U crée son mot de passe pour le service S, ou bien quand ce mot de passe est modifié, ou à tout moment où cette mémorisation E1 est pertinente. La mémorisation E1 peut être également demandée par le terminal T quand celui-ci reçoit un jeton d'authentification fourni par le service S comme permettant la connexion ultérieure de l'utilisateur U. C'est le module 201 du dispositif D distinct du terminal T qui effectue cette mémorisation E1. Sur la [Fig.1], l'opération E1 de mémorisation des données d'authentification DAT est représentée par une flèche entre le module 101 du terminal T qui demande cette mémorisation E1, la flèche étant étiquetée par E1 et portant la mention DAT.

[0077] Dans un mode de réalisation, l'étape préalable de mémorisation E1 de données d'authentification DAT d'un utilisateur U pour le service S est déclenchée par une interaction directe de l'utilisateur U avec le dispositif D. Dans ce mode, le dispositif D comprend des éléments, non représentés sur la [Fig.1], permettant une interaction avec l'utilisateur U tels qu'un clavier, un écran, ou un micro pour permettre une interaction vocale. L'écran peut être tactile, et dans ce cas offrir une possibilité de clavier virtuel.

Le dispositif D dans ce cas peut être par exemple un ordiphone, mais d'autres formes sont possibles pour un dispositif D dédié à l'invention. Le dispositif D peut avoir le format d'une carte de crédit et être muni en sus d'un clavier et d'un écran de taille limitée, permettant uniquement la saisie de données d'authentification DAT. Le dispositif D peut aussi remplir le rôle de dispositif de pointage (souris ou autre) et être également muni d'un écran et d'un clavier de tailles réduites, l'interface utilisateur étant limitée à la saisie de données d'authentification DAT.

[0078] Dans tous les cas, grâce à ce module 201, les données d'authentification DAT sont mémorisées en dehors du terminal T apte à être partagé entre plusieurs utilisateurs U, U', U'' ce qui améliore la protection de ces données.

[0079] Le dispositif D comprend également un module 202 de réception E3 d'une requête d'obtention des données d'authentification DAT de l'utilisateur U donné pour le service S. Sur la [Fig.1], la réception E3 d'une requête d'obtention des données d'authentification DAT est représentée par une flèche portant la mention DAT?, le point d'interrogation symbolisant la requête des données d'authentification DAT.

[0080] Le dispositif D comprend également un module 203 de validation V par un utilisateur U sur le dispositif D.

[0081] Cette étape V de validation survient à la suite d'une demande d'accès au service S par un utilisateur U donné. Cet accès va nécessiter la soumission au service S des données d'authentification DAT de l'utilisateur U pour le service S. Il y a donc besoin que soit réalisée une opération de validation V grâce au module 203 du dispositif D pour justifier la fourniture ultérieure des données d'authentification DAT.

[0082] Le dispositif D comprend également un module 204 de fourniture E4 de données d'authentification DAT.

[0083] Une fois l'opération de validation V effectuée, et réussie, le dispositif D va procéder à la fourniture E4 des données d'authentification de l'utilisateur U pour le service S.

[0084] Dans un mode de réalisation, l'étape de fourniture E4 par le dispositif D des données d'authentification DAT d'un utilisateur U donné consiste en l'affichage par le dispositif D des données DAT. Dans ce mode, le dispositif D comprend un moyen d'affichage, non représenté sur la [Fig.1], tel qu'un écran de plus ou moins grande taille. Quand le dispositif D est un ordiphone, l'écran utilisé pour fournir E4 par affichage les données d'authentification DAT est présent. Le dispositif D peut aussi être un dispositif dédié à l'invention du format d'une carte de crédit avec un écran de taille réduite qui pourra être utilisé pour la fourniture E4 par affichage des données d'authentification DAT. Cela peut également être le cas quand le dispositif D dédié prend également la forme d'un dispositif de pointage, ou d'une carte mémoire USB. Dans le cas où l'étape de fourniture E4 est réalisée par l'affichage des données d'authentification DAT, c'est l'utilisateur U qui va ensuite fournir les données

d'authentification DAT au service S par l'intermédiaire du terminal T pour compléter son accès au service S depuis le terminal T. Cette fourniture se fait par les moyens d'interaction du terminal T. L'avantage de ce mode de réalisation est que les données d'authentification DAT restent mémorisées dans le dispositif dédié D et restent donc protégées.

[0085] Pour réaliser les différentes étapes du procédé de gestion selon l'invention, des liaisons de communication doivent être établies d'une part entre les éléments du système SYS et le service S et d'autre part au sein du système SYS.

[0086] Le service S est un service informatique. Le service S est rendu par un serveur informatique, non représenté dans la [Fig.1]. La nature du serveur rendant le service S n'est pas pertinente pour l'invention. Celui-ci peut être un serveur présent dans un nuage informatique, ou bien un ordinateur dédié. Le service S est accédé par l'utilisateur U depuis le terminal T. Le service S peut être un service Web, et dans ce cas, les interactions avec le service S se font grâce au protocole http, à travers un navigateur Web exécuté dans le terminal T. La liaison entre le terminal T et le serveur rendant le service S doit dans ce cadre permettre de réaliser le protocole http entre le terminal T et le service S. Le service S peut être par exemple accédé via Internet, et le terminal T devra alors pouvoir accéder à Internet. Le service S peut également être hébergé dans un serveur et accédé à travers une application mobile hébergée dans un terminal T de type ordiphone. La liaison entre le terminal T et le serveur S utilisera alors dans ce cas majoritairement le protocole http mais pourrait aussi utiliser un protocole ad hoc passant par le réseau Internet. Dans certains contextes, le service S sera accessible via un réseau d'entreprise de type Intranet, et le terminal T appartiendra au même réseau de type Intranet.

[0087] Dans des contextes particuliers, on peut imaginer que le service S sera accédé via une liaison directe entre le terminal T et le service S. Par exemple, le service S ne peut être accédé que par le terminal T, et une liaison directe est établie entre le terminal T et le service S. Cette liaison peut être radio ou filaire suivant les cas. Les liaisons radio peuvent être établies grâce aux protocoles WiFi, Bluetooth ou bien grâce aux normes de téléphonie sans fil GSM, Edge, UMTS, 3G, 4G, 5G ou autres. Les liaisons filaires peuvent être par exemple une liaison série entre un terminal T et un serveur hébergeant le service S. Le protocole de communication entre le terminal T et le service S peut alors rester le protocole http ou bien être un protocole complètement ad hoc. Le service S peut être par exemple une API (acronyme pour l'anglais *Application Programming Interface*) et des protocoles tels que SOAP, JSON, CORBA (acronymes anglais pour respectivement *Simple Object Access Protocol, JavaScript Object Notation, Common Object Request Broker Architecture*) ou autres peuvent être utilisés dans des liaisons filaires ou sans fils pour échanger des données entre le terminal T et le service S.

[0088] Dans certains contextes, le service S sera un logiciel exécuté directement dans le terminal T. La liaison entre le terminal T et le service S dans ce cas est une liaison interne à un ordinateur, utilisant les différents composants du terminal T (bus de données, liaison entre clavier et processeurs).

[0089] Le dispositif D, quant à lui, est distinct du terminal T. La liaison entre le terminal T et le dispositif D peut se faire de plusieurs manières. Dans un mode de réalisation, le terminal T sera accessible par Internet et les liaisons entre le terminal T et le dispositif D se feront par des requêtes http ou autres pouvant être adressées sur Internet. Dans d'autres cas, le terminal T et le dispositif D appartiendront au même réseau d'entreprise Intranet, ou bien à un même réseau local de type LAN. Les communications pourront alors se faire via une liaison filaire telle que WiFi ou Bluetooth. Dans d'autres cas enfin, le dispositif D aura la forme d'un dispositif de pointage ou d'une clé USB et sera connecté physiquement au terminal T pour effectuer la liaison entre le terminal T et le dispositif D. La liaison sera alors assurée par le bus de communication du terminal T et utilisera le protocole USB.

[0090] Dans l'ensemble des modes de réalisation, les liaisons au sein du système SYS d'une part, et les liaisons entre le système SYS et le service S d'autre part, peuvent être réalisées en utilisant des protocoles de communication assurant le chiffrement des données échangées grâce aux dits protocoles de communication. De tels protocoles sont par exemple https, mais aussi FTPs, SSH ou bien SFTP (acronymes anglais pour respectivement *File Transfer Protocol Secure, Secure Shell, SSH File Transfer Protocol*). De cette manière, les données d'authentification DAT sont protégées contre des risques d'interception lors de leurs échanges pendant l'étape de mémorisation E1 et de fourniture E4.

[0091] Le procédé comprend une étape préalable de demande par le terminal T au dispositif D de mémorisation E1 de données d'authentification DAT. Cette mémorisation E1 peut se faire simplement en enregistrant les données d'authentification DAT dans une zone mémoire du dispositif D. Si le dispositif D enregistre les données d'authentification de plusieurs utilisateurs U, U', U'', une zone mémoire cloisonnée pourra être affectée par utilisateur pour améliorer la protection des données d'authentification DAT.

[0092] Dans un mode de réalisation, l'étape préalable de mémorisation E1 de données d'authentification DAT d'un utilisateur U pour le service S est déclenchée par une interaction directe de l'utilisateur U avec le dispositif D. Ce mode nécessite que le dispositif D comprenne des moyens d'interaction tels que clavier, écran ou micro pour permettre à l'utilisateur U d'interagir avec le dispositif D. Suivant la forme du dispositif D (ordiphone ou dispositif dédié remplissant éventuellement d'autres fonctions), les moyens d'interaction auront des tailles variables, en général réduites.

[0093] Dans certains modes de réalisation, le dispositif D va utiliser des outils cryptographiques pour protéger davantage les données d'authentification DAT mémorisées par le dispositif D. De cette manière, la protection des données d'authentification DAT sera améliorée.

[0094] Un mode possible de réalisation utilisant la cryptographie est d'avoir le dispositif D réaliser un chiffrement des données d'authentification DAT lors de l'étape de mémorisation E1 réalisée par le module 201. De cette façon, les données d'authentification DAT seront conservées de façon chiffrée, ce qui diminue le risque que ces données soient accédées par des utilisateurs non légitimes. Le chiffrement réalisé ici peut utiliser une clé symétrique, et le déchiffrement des données d'authentification DAT pourra alors être effectuée lors de l'étape de fourniture E4 réalisée par le module 204 du dispositif D. Dans ce cas de chiffrement et déchiffrement symétrique, le dispositif D utilisera une même clé de chiffrement symétrique pour les deux opérations. Si un dispositif D mémorise des données d'authentification de plusieurs utilisateurs U, U', U'', une précaution supplémentaire sera d'affecter une clé différente pour mémoriser les données d'authentification DAT d'utilisateurs différents. Cette précaution se combinera avec la précaution d'utiliser des zones mémoire cloisonnées entre elles attribuées aux différents utilisateurs U, U', U''.

[0095] D'autres modes de réalisation utilisant la cryptographie pourraient utiliser un chiffrement asymétrique utilisant une paire de clés dite publique et privée. Dans un de ces modes, le terminal T utilise une clé publique pour chiffrer les données d'authentification DAT de l'utilisateur U avant l'étape de demande de mémorisation E1 par le dispositif D. La clé privée correspondante pourrait alors être détenue par le dispositif D qui l'utiliserait pour procéder au déchiffrement des données d'authentification DAT lors de l'étape de fourniture E4. Comme précédemment, une paire de clés publique/privée peut être utilisée pour un opérateur U donné pour améliorer la protection des données d'authentification au cas où le dispositif D mémorise les données d'authentification DAT de plusieurs utilisateurs.

[0096] Dans certains modes de réalisation qui utilisent la cryptographie, le terminal T peut gérer entièrement le chiffrement et le déchiffrement des données d'authentification DAT des utilisateurs U, U', U''. Ces modes de réalisation peuvent utiliser des techniques de chiffrement symétrique ou bien asymétrique. Dans ces modes de réalisation, la protection supplémentaire des données d'authentification DAT apportées par le chiffrement est présente, et, de surcroît, le dispositif D n'a pas à effectuer d'opérations de chiffrement ou de déchiffrement. De cette manière, le dispositif D peut rester un dispositif le plus simple possible, avec des capacités de calcul limitées, qui n'ont pas à réaliser d'opérations de chiffrement/déchiffrement, mais réalisent les opérations de mémorisation E1 de données d'authentification DAT chiffrées et de

fourniture E4 de ces mêmes données chiffrées.

[0097] Une fois réalisée l'étape préalable de demande de mémorisation E1 de données d'authentification DAT, le procédé de gestion peut être mis en œuvre pour permettre l'accès au service S d'un utilisateur U depuis le terminal T.

[0098] Le procédé comprend une étape E2 de demande d'accès au service S par un utilisateur U donné. Cette demande peut être réalisée de plusieurs manières. Dans le cas où le service S est un service Web, l'utilisateur U interagira avec un navigateur Web exécuté par le terminal T, navigateur qui enverra des requêtes http au service S. Le service S peut être aussi une application informatique, et dans ce cas une interface homme-machine dédiée dans le terminal T permettra à l'utilisateur U de demander E2 l'accès au service S.

[0099] Pour compléter l'accès au service S, les données d'authentification DAT sont nécessaires. L'étape suivante du procédé est donc la réception E3 par le dispositif D d'une requête d'obtention des données d'authentification DAT de l'utilisateur U donné pour le service S.

[0100] Selon la nature du dispositif D, la réception E3 de la requête d'obtention des données d'authentification peut prendre plusieurs formes. Si le dispositif D est un ordiphone, la liaison avec le dispositif D pourra être une liaison sans fil et la réception E3 pourra être la réception d'une requête Web. D'autres protocoles peuvent être envisagés comme l'envoi d'un fichier JSON (acronyme pour l'anglais *JavaScript Object Notation*) à compléter par le dispositif D. Dans le cas où le dispositif D est un dispositif dédié au procédé (dispositif de pointage modifié, clé USB modifiée, dispositif sous la forme d'une carte de crédit), celui-ci pourra être connecté grâce à une liaison Bluetooth ou bien filaire comme vu précédemment. La réception E3 de la requête d'obtention pourra utiliser alors cette liaison Bluetooth ou filaire. Le protocole de communication utilisant la liaison pourra être un protocole de communication ad hoc.

[0101] Pour que le dispositif D fournisse E4 les données d'authentification DAT, une étape de validation V par l'utilisateur U est nécessaire. L'étape de validation V peut prendre plusieurs formes.

[0102] Dans un mode de réalisation, la validation V peut se limiter à une opération simple, comme cliquer sur un bouton d'une fenêtre dédiée, si le dispositif D comprend l'interface homme-machine permettant à l'utilisateur U de réaliser cette interaction, à savoir un écran et un dispositif de pointage. Dans un mode de réalisation, la validation V pourra consister en la soumission par l'utilisateur U au dispositif D d'un code d'identification personnel. Ce mode nécessite là aussi une interface homme-machine particulière, à savoir ici au minimum un écran et un clavier.

[0103] Dans un mode de réalisation encore plus simplifié, l'étape de validation V peut consister en la pression sur un bouton ou tout autre dispositif physique simple avec

lequel un utilisateur U peut interagir, comme un interrupteur, ou un curseur, ou une zone réceptive à la pression d'une partie du corps. Dans ce cas, il sera adapté que le dispositif D soit attribué à un utilisateur U donné. Dans ce mode, le dispositif D distinct du terminal T ne mémorisera les données d'authentification DAT que pour un utilisateur U donné. Le dispositif D pourra prendre tout type de forme. Il pourra être par exemple sous forme d'une carte de crédit, et éventuellement comprendre, en plus d'un mécanisme permettant la validation V (bouton, interrupteur, glissière ou tout autre mécanisme équivalent), des éclairages indiquant le besoin d'une validation V et le succès de celle-ci. Le dispositif D peut aussi prendre la forme d'une clé USB (acronyme pour *Universal Serial Bus*) qui peut effectuer la mémorisation E1 des données d'authentification DAT, clé modifiée pour pouvoir effectuer une opération de validation V et une opération de fourniture E4 à la suite de la validation V.

[0104] Dans ces modes de réalisation, dans lesquels la validation V effectuée par l'utilisateur U sur le dispositif D est très simple, il existe un risque d'usurpation d'identité. En effet, un utilisateur parmi les utilisateurs U, U', U'' pourrait dérober le dispositif D attribué à un utilisateur U donné, demander à accéder au service S par le terminal T sous l'identité de l'utilisateur U, et réaliser la validation V à sa place en utilisant le dispositif D, quand la validation V consiste en un geste simple comme dans les modes décrits précédemment.

[0105] Pour éviter ce risque d'usurpation, un mode de réalisation de l'étape de validation V, non représenté sur la [Fig.1], va consister en ce que l'étape de validation V comprend une étape préalable de mémorisation d'une base de correspondances entre des identifiants d'utilisateur U et des données d'identification respectives, et en ce que l'étape de validation V réussit, ce qui permet la fourniture par le dispositif des données d'authentification DAT d'un utilisateur U donné, après l'exécution des étapes suivantes :

- Obtention d'une donnée d'identification par le dispositif D ;
- Détermination d'un identifiant d'utilisateur U correspondant dans la base mémorisée à la donnée d'identification obtenue ;
- Vérification que l'identifiant d'utilisateur U déterminé correspond bien à l'utilisateur U donné.

[0106] De cette manière, les données d'authentification DAT d'un utilisateur U donné ne sont fournies par le dispositif D que quand c'est bien l'utilisateur U qui réalise l'étape de validation V sur le dispositif D distinct du terminal T. Plusieurs possibilités sont offertes pour réaliser cette variante de l'étape de validation V, selon les capacités du dispositif D.

[0107] Dans un mode de réalisation, le dispositif D peut être un ordinateur ou un ordiphone et comprendre des interfaces homme-machine telles qu'un écran et un clavier (réel ou

virtuel). Les données d'identifications mémorisées et obtenues par le dispositif D peuvent être alors un mot de passe, et l'utilisateur U sera identifié grâce à ce mot de passe lors de l'étape de validation V.

[0108] Dans un autre mode de réalisation, le dispositif D comprend des capacités de vérification de caractéristiques biométriques des utilisateurs U, U', U''. De telles capacités sont par exemple bien connues sur les ordinateurs et les ordiphones, avec des lecteurs d'empreintes digitales intégrés à l'ordinateur ou à l'ordiphone, ou bien des lecteurs d'iris utilisant les caméras de l'ordinateur ou de l'ordiphone, ou bien des dispositifs de reconnaissance du locuteur utilisant les microphones de l'ordinateur ou de l'ordiphone. D'autres capacités de vérification sont également possibles. Un dispositif D très simple, d'un format carte de crédit, dédié à l'invention, peut également présenter une capacité de vérification de caractéristiques biométriques, et en premier lieu un lecteur d'empreintes digitales. Un dispositif D peut également être un périphérique du terminal T et par exemple servir de dispositif de pointage à l'utilisateur U sur le terminal T. Une capacité de vérification biométrique peut être intégrée dans un tel dispositif D, par exemple un lecteur d'empreintes digitales, ou bien un vérificateur de la transmission des signaux électriques à travers le corps humain.

[0109] La présence de capacités de vérification de caractéristiques biométriques dans le dispositif D permet de rendre l'étape de validation V facile à exécuter et pratique pour l'utilisateur U. De plus, la vérification de caractéristiques biométriques permet de s'assurer que c'est bien l'utilisateur U qui effectue l'étape de validation V qui permet, quand elle réussit, au dispositif D de fournir les données d'authentification DAT de l'utilisateur U pour le service S. De cette manière, grâce à ce mode de réalisation, il devient plus difficile à un utilisateur autre que U d'accéder aux données d'authentification DAT de U, et celles-ci sont protégées plus efficacement.

[0110] Dans un mode de réalisation, l'étape de validation V comprend une étape préalable de mémorisation d'une base de correspondances entre des identifiants de terminal et des données d'identification respectives, et l'étape de validation V réussit, ce qui permet la fourniture E4 par le dispositif D des données d'authentification DAT d'un utilisateur U donné, après l'exécution des étapes suivantes :

- Obtention d'une donnée d'identification par le dispositif D ;
- Détermination d'un identifiant de terminal correspondant dans la base mémorisée à la donnée d'identification obtenue ;
- Vérification que l'identifiant de terminal déterminé correspond bien au terminal T.

[0111] Dans ce mode, l'étape de validation V comprend l'identification du terminal T par le dispositif D. Une telle identification peut se faire en utilisant le protocole Bluetooth. Le dispositif D sera alors, dans une phase préalable, appairé au terminal T. Lorsque des

données d'authentification DAT doivent être fournies E4, elles ne pourront l'être qu'après établissement d'une liaison Bluetooth entre le dispositif D et le terminal T. L'établissement de cette liaison implique une identification du terminal T par le dispositif D. De cette façon, les données d'authentification DAT ne sont fournies E4 qu'à un terminal T préalablement appairé au dispositif D puis identifié lors de l'étape de validation V.

[0112] L'identification du terminal T peut se faire en complément de l'identification de l'utilisateur U, ou bien alternativement à l'identification de l'utilisateur U. Par exemple, l'étape de validation V peut se limiter à une interaction sans identification de l'utilisateur U (celui-ci presse un bouton du dispositif D) et par contre comprendre une identification du terminal T qui va limiter la fourniture E4 de données d'authentification DAT à un terminal T préalablement appairé avec le dispositif D. Mais dans un autre mode, l'étape de validation V comprend à la fois l'identification de l'utilisateur U (celui-ci doit par exemple fournir un mot de passe au dispositif D, ou bien ses caractéristiques biométriques doivent être reconnues) ainsi que l'identification du terminal T (la fourniture E4 ne se fait que vers un terminal T préalablement appairé avec le dispositif D).

[0113] Une fois l'étape de validation V réussie, le dispositif D peut procéder à la fourniture E4 des données d'authentification DAT de l'utilisateur U pour le service. Comme pour l'étape E3, la réalisation de cette étape E4 dépendra de la liaison de communication permettant d'interagir avec le dispositif D. Si le procédé utilise des techniques de cryptographie, l'étape E4 peut comprendre une phase de déchiffrement des données d'authentification DAT comme vu précédemment.

[0114] La [Fig.2], quant à elle, décrit la succession des étapes selon l'invention.

[0115] Dans une étape préalable, le terminal T va demander au dispositif D la mémorisation E1 de données d'authentification DAT. Cette étape a lieu quand un utilisateur U crée de nouvelles données d'authentification DAT pour se connecter au service S depuis le terminal T. ceci peut avoir lieu par exemple à la création d'un compte de l'utilisateur U auprès du service S, ou bien lors d'un changement de mot de passe pour accéder au service S.

[0116] Un utilisateur U va à un moment effectuer une demande E2 d'accès au service S depuis le terminal T. Le dispositif va alors recevoir E3 une requête d'obtention des données d'authentification DAT précédemment mémorisées E1.

[0117] L'utilisateur U va alors devoir effectuer une étape de validation V sur le dispositif D. Quand l'étape de validation V réussit, le dispositif D procède à une étape de fourniture E4 des données d'authentification DAT permettant l'accès de l'utilisateur U au service S.

[0118] Les figures suivantes précisent les intervenants des différentes étapes.

[0119] La [Fig.3] présente un mode de réalisation possible du procédé.

[0120] Dans ce mode, c'est le terminal T qui effectue la requête d'obtention des données d'authentification DAT reçue E31 par le dispositif. Puis, après validation V, le dispositif D fournit E41 les données d'authentification DAT au terminal T. Celui-ci va ensuite les transférer au service S afin de compléter la demande E2 d'accès au service S par l'utilisateur U depuis le terminal T.

[0121] Ce mode de réalisation peut particulièrement être utilisé dans le contexte où le terminal T est un ordiphone et le service S est accédé à travers une application mobile qui s'exécute dans le terminal T, ou bien lorsque le service S est un service Web et est accédé depuis le terminal T à travers un navigateur Web. Dans ces contextes, pour que l'utilisateur U puisse accéder au service S, le terminal T devra fournir ou bien un mot de passe, ou bien un jeton d'authentification, témoin d'une connexion précédente de l'utilisateur U, qui est considéré comme suffisant par le service S. De tels éléments, mot de passe ou jeton, constituent des données d'authentification DAT. Ces éléments, en particulier les jetons d'authentification, peuvent être enregistrés dans le terminal T pour éviter de devoir redemander un mot de passe à l'utilisateur U. Mais la présence de données d'authentification DAT dans le terminal T constitue un risque de sécurité.

[0122] Dans des modes de réalisation de l'invention, les données d'authentification DAT sont reçues par le terminal T après la fourniture E41 par le dispositif D, utilisées par le terminal T pour compléter l'accès de l'utilisateur U au service S, puis effacées par le terminal T de l'ensemble des zones mémoire du terminal T dans laquelle les données d'authentification DAT ont pu se trouver. L'avantage de ces modes de réalisation est de garantir que les données d'authentification DAT ne sont pas mémorisées dans le terminal T après leur usage, ce qui lève un risque de sécurité pesant sur ces données d'authentification DAT.

[0123] La [Fig.4] présente un autre mode de réalisation possible du procédé.

[0124] Dans ce mode, c'est le terminal T qui effectue la requête d'obtention des données d'authentification DAT reçue E31 par le dispositif. Puis, après validation V, le dispositif D fournit E42 les données d'authentification DAT directement au service S. Un avantage de ce mode de réalisation est de fournir plus rapidement les données d'authentification DAT au service S pour accélérer l'accès de l'utilisateur U au service S.

[0125] La [Fig.5] présente un autre mode de réalisation possible du procédé.

[0126] Dans ce mode, c'est le service S qui effectue la requête d'obtention des données d'authentification DAT reçue E32 par le dispositif. Puis, après validation V, le dispositif D fournit E42 les données d'authentification DAT directement au service S. Un avantage de ce mode de réalisation est d'éviter que les données d'authentification DAT transitent par le terminal T. Comme celui-ci est partagé entre les utilisateurs U,

U', U'', il est possible que des utilisateurs malveillants aient installé des logiciels espions dans le terminal T qui pourraient détourner des données d'authentification DAT. Ce mode de réalisation évite ce risque.

[0127] La [Fig.6] présente un autre mode de réalisation possible du procédé.

[0128] Dans ce mode, c'est le service S qui effectue la requête d'obtention des données d'authentification DAT reçue E32 par le dispositif. Puis, après validation V, le dispositif D fournit E41 les données d'authentification DAT au terminal T. Ce mode de réalisation combine la rapidité de la requête directe des données d'authentification DAT par le service S avec la praticité de fournir les données d'authentification DAT au terminal T par lequel l'utilisateur U accède au service S.

[0129] Comme déjà vu lors de la présentation de la [Fig.3], dans certains modes de réalisation, le terminal T effacera les données d'authentification DAT après la fourniture E41 et l'utilisation des données d'authentification DAT par le terminal T pour compléter l'accès au service S de l'utilisateur U.

[0130] La [Fig.7] présente un autre mode de réalisation possible du procédé.

[0131] Dans ce mode, l'étape de mémorisation E1 de données d'authentification DAT est déclenchée par une interaction de l'utilisateur U avec le dispositif D. Le dispositif D va par exemple disposer d'un clavier et d'un écran qui vont permettre à l'utilisateur U de rentrer les données d'authentification DAT dans le dispositif D qui va ensuite les mémoriser E1.

[0132] Lors d'une demande d'accès E2 ultérieur de U au service S depuis le terminal T, il y aura besoin d'accéder aux données d'authentification DAT. Le terminal T effectue une demande de ces données d'authentification DAT, demande reçue E3 par le dispositif D. L'étape de validation V comprend dans ce mode de réalisation une étape d'identification du terminal T. Cette identification a pu être préparée par exemple par un appairage Bluetooth entre le dispositif D et le terminal T. Le dispositif D reconnaissant le terminal T lors de l'étape de validation V peut procéder à la fourniture E4 des données d'authentification DAT.

[0133] Dans ce mode de réalisation, la fourniture E4 des données d'authentification DAT consiste en l'affichage des données à l'utilisateur U. Le dispositif D dispose donc dans ce mode de réalisation d'un écran qui va lui permettre d'afficher les données d'authentification DAT. L'utilisateur U pourra alors lire les données d'authentification DAT sur l'écran du dispositif D puis les rentrer lui-même dans le terminal T ce qui permettra de procéder à son accès au service S depuis le terminal T.

[0134] La [Fig.8] présente un autre mode de réalisation possible du procédé.

[0135] Dans ce mode, comme dans le mode décrit précédemment, l'étape de mémorisation E1 de données d'authentification DAT est déclenchée par une interaction de l'utilisateur U avec le dispositif D. Comme dans le mode précédent, l'étape de va-

lidation V comprend une identification du terminal T. Le fait que le terminal T soit identifié apporte une garantie de sécurité supplémentaire. Le dispositif D procède ensuite à la fourniture E41 des données d'authentification DAT directement au terminal T. Celui-ci pourra ensuite utiliser les données d'authentification DAT pour réaliser l'accès de l'utilisateur U au service S depuis le terminal T.

[0136] Signalons par ailleurs que cette description a été faite en parlant d'un seul service S. Cependant, l'invention décrite dans la présente demande peut aussi bien s'appliquer quand les utilisateurs U, U', U'' cherchent à accéder à plusieurs services S, S', S''. Les données d'authentification DAT dont il est question ici sont comprises comme servant à un utilisateur U donné à accéder à un service S donné. Plusieurs données d'authentification DAT peuvent être mémorisées E1 pour un même utilisateur U dans le dispositif D, les différentes données d'authentification DAT servant à accéder différents services S, S', S''. Des éléments d'identification des services S, S', S'' sont alors inclus dans les données d'authentification DAT afin de permettre au dispositif D de reconnaître les données DAT qu'il doit fournir E4 suivant les tentatives d'accès de l'utilisateur U à un service S donné.

[0137] Dans des modes de réalisation, l'opération de fourniture E4 peut consister en l'export d'informations relatives à plusieurs jeux de données d'authentification DAT vers un terminal T. Les informations exportées peuvent être relatives à l'ensemble des données d'authentification DAT présentes dans le dispositif D, ou seulement relatives à une partie de celles-ci. Cet export permet à l'utilisateur U de réaliser une gestion de ses données d'authentification DAT en dehors des terminaux T avec lesquels il va accéder aux services S. Les informations relatives aux données d'authentification DAT sont connues du terminal T et permettent à celui-ci de requêter le dispositif D pour obtenir les données d'authentification DAT dont le terminal T a besoin. Les différents terminaux T seront identifiés et des catégories de terminaux T pourront être définies pour faciliter la gestion des données d'authentification DAT par l'utilisateur U. Par exemple, certaines données seront adaptées pour une connexion depuis des terminaux T de type ordinateur et d'autres données le seront pour des terminaux T de type ordiphone.

[0138] L'export d'informations relatives aux données d'authentification DAT permet aussi de répondre à la problématique de transférer l'utilisation des données d'authentification DAT vers un nouveau terminal T. Quand un utilisateur U dispose d'un nouveau terminal T, il procèdera à l'export d'informations relatives aux données d'authentification DAT vers ce nouveau terminal, en appliquant un filtrage par le type de terminal si besoin. Ces informations relatives aux données d'authentification DAT permettront ensuite au nouveau terminal T d'interagir avec le dispositif D pour requêter quand ce sera nécessaire les dites données d'authentification DAT.

[0139] Signalons enfin ici que, dans le présent texte, le terme « module » peut correspondre aussi bien à un composant logiciel qu'à un composant matériel ou un ensemble de composants matériels et logiciels, un composant logiciel correspondant lui-même à un ou plusieurs programmes ou sous-programmes d'ordinateur ou de manière plus générale à tout élément d'un programme apte à mettre en œuvre une fonction ou un ensemble de fonctions telles que décrites pour les modules concernés. De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions pour le module concerné (circuit intégré, carte à puce, carte à mémoire, etc.).

Revendications

[Revendication 1] Procédé de gestion de données d'authentification (DAT) permettant l'accès à un service (S) d'un utilisateur (U) depuis un terminal (T), l'accès d'un utilisateur (U) donné à un service (S) requérant une fourniture au service (S) de données d'authentification (DAT) relatives audit utilisateur (U), procédé caractérisé en ce qu'il comprend les étapes suivantes :

- Une étape préalable de demande par ledit terminal (T) à un dispositif (D) distinct du terminal (T) de mémorisation (E1) de données d'authentification (DAT) d'un utilisateur (U) pour le service (S) ;
- Suite à une demande (E2) d'accès au service (S) par un utilisateur (U) donné depuis ledit terminal (T), une étape de réception (E3) par le dispositif (D) d'une requête d'obtention des données d'authentification (DAT) de l'utilisateur (U) donné pour le service (S) ;
- Une étape de validation (V) effectuée par l'utilisateur (U) sur le dispositif (D) ;
- En cas de réussite de l'étape de validation (V), une étape de fourniture (E4) par le dispositif (D) des données d'authentification (DAT) de l'utilisateur (U) donné pour le service (S).

[Revendication 2] Procédé de gestion selon la revendication 1, caractérisé en ce que l'étape de validation (V) comprend une étape préalable de mémorisation d'une base de correspondances entre des identifiants d'utilisateur et des données d'identification respectives, et en ce que l'étape de validation (V) réussit, ce qui permet la fourniture (E4) par le dispositif (D) des données d'authentification (DAT) d'un utilisateur (U) donné, après l'exécution des étapes suivantes :

- Obtention d'une donnée d'identification par le dispositif (D) ;
- Détermination d'un identifiant d'utilisateur correspondant dans la base mémorisée à la donnée d'identification obtenue ;
- Vérification que l'identifiant d'utilisateur déterminé correspond bien à l'utilisateur (U) donné.

[Revendication 3] Procédé de gestion selon la revendication 1 ou 2, caractérisé en ce que l'étape de validation (V) comprend une étape préalable de mémorisation d'une base de correspondances entre des identifiants de terminal et des données d'identification respectives, et en ce que l'étape de validation (V) réussit, ce qui permet la fourniture (E4) par le dispositif (D) des données d'authentification (DAT) d'un utilisateur (U) donné, après l'exécution des étapes suivantes :

- Obtention d'une donnée d'identification par le dispositif (D) ;
- Détermination d'un identifiant de terminal correspondant dans la base mémorisée à la donnée d'identification obtenue ;
- Vérification que l'identifiant de terminal déterminé correspond bien au terminal (T).

[Revendication 4] Procédé de gestion selon l'une des revendications 1 à 3, caractérisé en ce que :

- La requête d'obtention des données d'authentification (DAT) d'un utilisateur (U) reçue (E31) par le dispositif (D) est en provenance du terminal (T) ;
- La fourniture (E41) par le dispositif (D) des données d'authentification (DAT) d'un utilisateur (U) est à destination du terminal (T).

[Revendication 5] Procédé de gestion selon l'une des revendications 1 à 3, caractérisé en ce que :

- La requête d'obtention des données d'authentification (DAT) d'un utilisateur (U) reçue (E31) par le dispositif (D) est en provenance du terminal (T) ;
- La fourniture (E42) par le dispositif (D) des données d'authentification (DAT) d'un utilisateur (U) est à destination du service (S).

[Revendication 6] Procédé de gestion selon l'une des revendications 1 à 3, caractérisé en ce que :

- La requête d'obtention des données d'authentification (DAT) d'un utilisateur (U) reçue (E32) par le dispositif (D) est en

provenance du service (S) ;

- La fourniture (E42) par le dispositif (D) des données d'authentification (DAT) d'un utilisateur (U) est à destination du service (S).

[Revendication 7] Procédé de gestion selon l'une des revendications 1 à 3, caractérisé en ce que :

- La requête d'obtention des données d'authentification (DAT) d'un utilisateur (U) reçue (E32) par le dispositif (D) est en provenance du service (S) ;
- La fourniture (E41) par le dispositif (D) des données d'authentification (DAT) d'un utilisateur (U) est à destination du terminal (T).

[Revendication 8] Procédé de gestion selon l'une des revendications 4 ou 7 caractérisé en ce que, après la fourniture (E41) par le dispositif (D) des données d'authentification (DAT) à destination du terminal (T), le terminal (T) utilise les données d'authentification (DAT) pour compléter l'accès demandé (E2) au service (S) par un utilisateur (U) depuis le terminal (T), puis le terminal (T) efface lesdites données d'authentification (DAT) de l'ensemble des zones mémoire du terminal (T).

[Revendication 9] Procédé de gestion selon l'une des revendications 1 à 3, caractérisé en ce que l'étape de fourniture (E4) par le dispositif (D) des données d'authentification (DAT) d'un utilisateur (U) donné consiste en l'affichage par le dispositif (D) des données (DAT).

[Revendication 10] Procédé de gestion selon l'une des revendications 1 à 9, caractérisé en ce que l'étape préalable de mémorisation (E1) de données d'authentification (DAT) d'un utilisateur (U) pour le service (S) est déclenchée par une interaction directe de l'utilisateur (U) avec le dispositif (D).

[Revendication 11] Procédé de gestion selon l'une des revendications 1 à 10, caractérisé en ce que l'étape de fourniture (E4) par le dispositif (D) des données d'authentification (DAT) de l'utilisateur (U) consiste en un transfert d'informations relatives aux données d'authentification (DAT) de l'utilisateur (U) pour différents services (S) vers le terminal (T).

[Revendication 12] Système (SYS) comprenant un terminal (T) apte à accéder à un service

(S), l'accès au service (S) d'un utilisateur (U) donné requérant une fourniture au service (S) de données d'authentification (DAT) relatives audit utilisateur (U), caractérisé en ce que le système (SYS) comprend en outre un dispositif (D) distinct du terminal (T), et en ce que le terminal (T) comprend les modules suivants :

- Un module (101) de demande au dispositif (D) de mémorisation (E1) de données d'authentification (DAT) d'un utilisateur (U) pour le service (S) ;
- Un module (102) de demande (E2) d'accès au service (S) par un utilisateur (U) ;

et en ce que le dispositif (D) comprend les modules suivants :

- Un module (201) de mémorisation (E1) de données d'authentification (DAT) ;
- Un module (202) de réception (E3) d'une requête d'obtention de données d'authentification (DAT) d'un utilisateur (U) donné pour le service (S) ;
- Un module (203) de validation (V) par un utilisateur (U) de la fourniture (E4) de données d'authentification (DAT) ;
- Un module (204) de fourniture (E4) de données d'authentification (DAT).

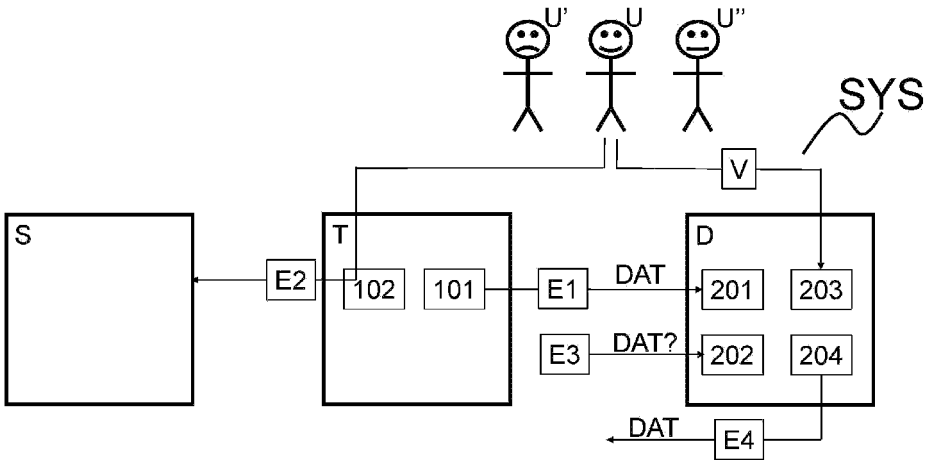
[Revendication 13] Programme d'ordinateur apte à être mis en œuvre par un terminal (T), le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur, réalise les étapes effectuées par le terminal (T) du procédé de gestion défini dans la revendication 1.

[Revendication 14] Programme d'ordinateur apte à être mis en œuvre par un dispositif (D), le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur, réalise les étapes effectuées par le dispositif (D) du procédé de gestion défini dans la revendication 1.

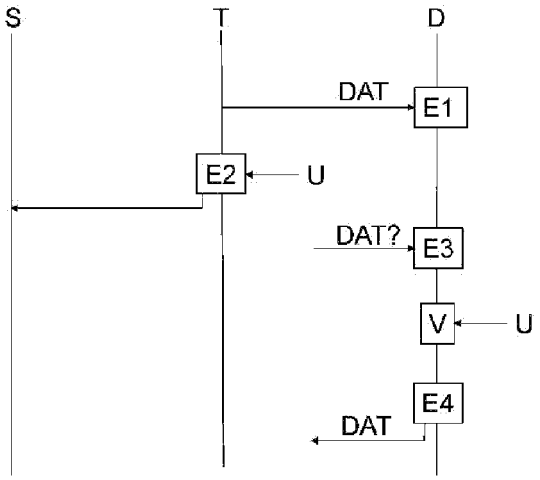
[Revendication 15] Support de données, sur lequel est enregistré un programme d'ordinateur conforme à la revendication 13.

[Revendication 16] Support de données, sur lequel est enregistré un programme d'ordinateur conforme à la revendication 14.

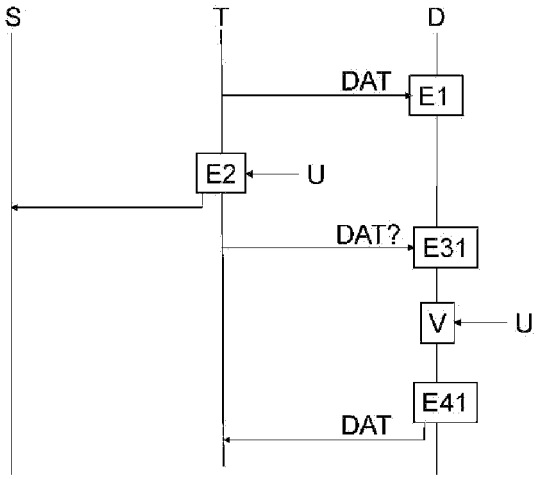
[Fig. 1]



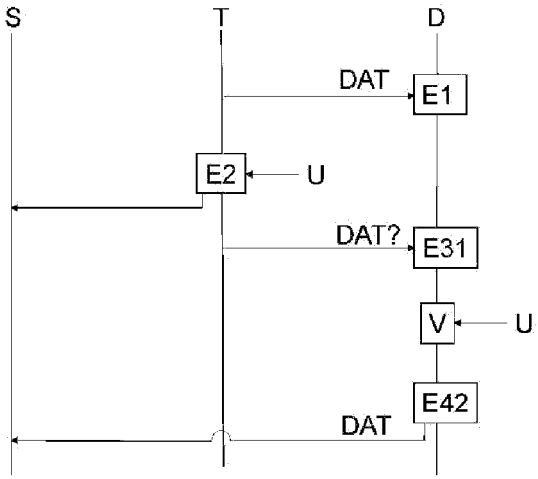
[Fig. 2]



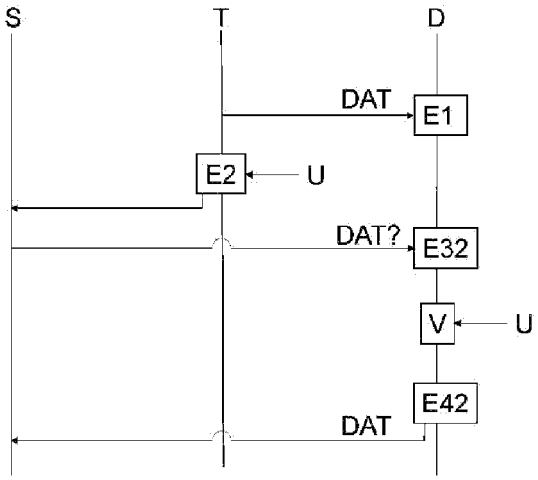
[Fig. 3]



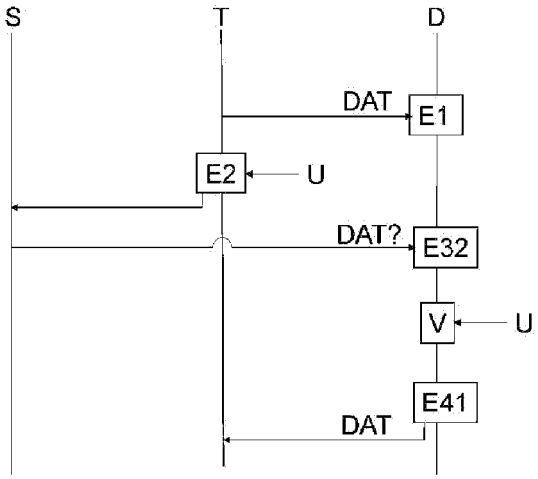
[Fig. 4]



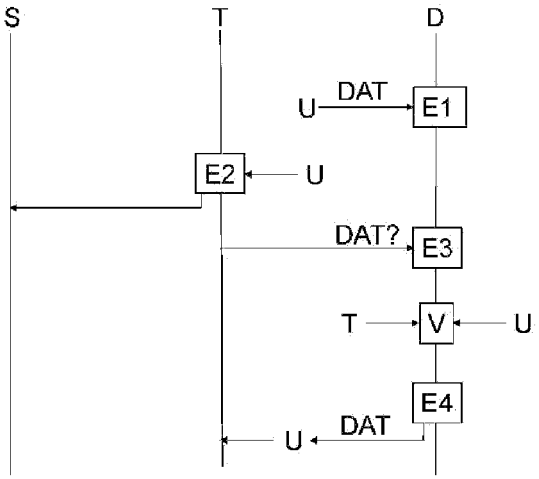
[Fig. 5]



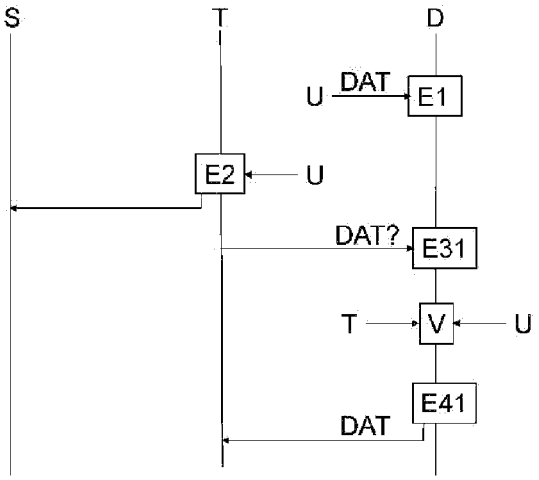
[Fig. 6]



[Fig. 7]


S
T
D
U
DAT
E1
E2
U
DAT?
E3
T
V
U
E4
DAT
U

[Fig. 8]


S
T
D
U
DAT
E1
E2
U
DAT?
E31
T
V
U
E41
DAT

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 913037
FR 2210381

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 2016/267261 A1 (TOOLEY II MACIO P [US]) 15 septembre 2016 (2016-09-15) * alinéa [0027] - alinéa [0064]; figures 1,3,2,8 *	1-16	G06F21/34 H04W12/06
X	US 2015/096001 A1 (MORIKUNI JAMES J [US] ET AL) 2 avril 2015 (2015-04-02) * alinéa [0015] - alinéa [0031]; figures 2A, 2B *	1-16	
X	EP 2 306 361 A1 (THOMSON LICENSING [FR]) 6 avril 2011 (2011-04-06) * alinéa [0016] - alinéa [0024]; figure 1 *	1-16	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F H04L H04W

Date d'achèvement de la recherche	Examinateur
10 mai 2023	Jardak, Christine

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 2210381 FA 913037

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 **10-05-2023**
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 2016267261 A1	15-09-2016	AUCUN	
US 2015096001 A1	02-04-2015	CN 106716433 A	24-05-2017
		EP 3053080 A1	10-08-2016
		US 2015096001 A1	02-04-2015
		US 2016248764 A1	25-08-2016
		WO 2015050890 A1	09-04-2015
EP 2306361 A1	06-04-2011	AUCUN	

EPO FORM P0465