



- (51) Classification internationale des brevets :
G06F 21/20 (2006.01) **H04L 9/32** (2006.01)
G06F 21/00 (2006.01) **H04L 29/06** (2006.01)
G06F 21/24 (2006.01)

- (21) Numéro de la demande internationale :
PCT/EP2011/004514

- (22) Date de dépôt international :
8 septembre 2011 (08.09.2011)

- (25) Langue de dépôt : français

- (26) Langue de publication : français

- (30) Données relatives à la priorité :
FR 10/03601 9 septembre 2010 (09.09.2010) FR

- (71) Déposant (pour tous les États désignés sauf US) :
LOGINPEOPLE SA [FR/FR]; Les Algorithmes, Bât.
Aristote A, 2000, route des Lucioles, F-06901 Sophia
Antipolis (FR).

- (72) Inventeur; et

- (75) Inventeur/Déposant (pour US seulement) : **ISRAEL,
Maurice** [FR/FR]; 20 chemin de la croix bidoux,
F-27630 Ecos (FR).

- (74) Mandataire : **SCHUFFENECKER, Thierry**; 120,
Chemin de la Maure, F-06800 Cagnes sur Mer (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, 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, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

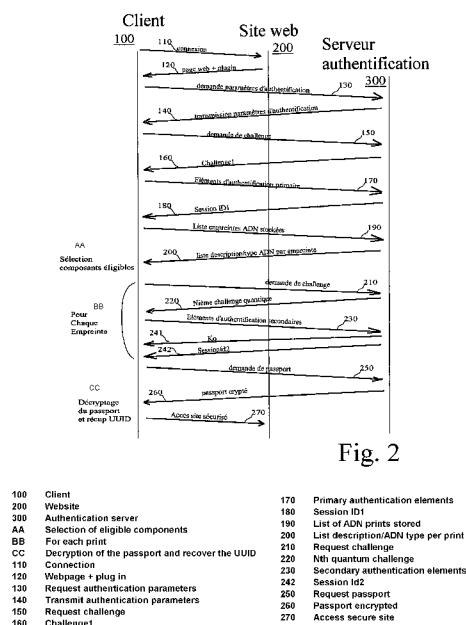
Déclarations en vertu de la règle 4.17 :

- relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)

[Suite sur la page suivante]

- (54) Title : METHOD OF AUTHENTICATION FOR ACCESS TO A WEBSITE

- (54) Titre : PROCEDE D'AUTHENTICATION POUR L'ACCES A UN SITE WEB



(57) Abstract : Method of strengthened authentication based on the collecting of data representative of hardware components contained in a system (I.H.S), said method comprising a step of enrolment and a step of authentication comprising the steps: - connection (10) to a website and reception (20) of a web page comprising executable code; - detection and collection (30) of a list of hardware components on the basis of the information collected by the operating system, in particular for the loading of drivers; characterized in that the enrolment procedure furthermore comprises the following steps: display of a list of hardware components resulting from said collection and selection (40) of a subset of said list with the aim of constructing an item of digital reference information (ADNN) for the system of the user; - generating of a digital reference item of information item (ADNN) on the basis of said subset, said digital reference information resulting from a hash operation applied to the raw data constituted by the collected data; - use of said digital reference information item (ADNN) with a seed received from an authentication server with the aim of generating a one-time password (OTP).

(57) Abrégé : Procédé d'authentification renforcé basé sur la collecte de données représentatives de composants matériels contenus dans un système (I.H.S), ledit procédé comportant une étape d'enrôlement et une étape d'authentification comportant les étapes : - connexion

[Suite sur la page suivante]



— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii))*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport (règle 48.2.g))*

(10) à un site web et réception (20) d'une page web comportant code exécutable; - détection et collecte (30) d'une liste de composants matériels à partir des informations collectées par le système d'exploitation, notamment pour le chargement des pilotes; caractérisé en ce que la procédure d'enrôlement comporte en outre les étapes suivantes : - affichage d'une liste de composants matériels résultant de ladite collecte et sélection (40) d'un sous-ensemble de ladite liste dans le but de constituer une information numérique de référence (ADNN) du système de l'utilisateur; - génération d'une information numérique de référence (ADNN) à partir dudit sous- ensemble, ladite information numérique de référence résultant d'une opération de hash appliquée aux données brutes que composent les données collectées; - utilisation de ladite information numérique de référence (ADNN) avec une semence reçue d'un serveur d'authentification dans le but de générer un mot de passe à usage unique (OTP).

Procédé d'authentification pour l'accès à un site web

Domaine technique de l'invention

5

La présente invention concerne les télécommunications numériques (internet) et plus particulièrement un procédé d'authentification pour l'accès à un site web sur le réseau internet ou sur un réseau Intranet.

10

Etat de la technique

Le réseau Internet a suscité un développement spectaculaire des échanges numériques dans le monde entier via des applications en ligne sur des sites web.

15 Une identité numérique (comprenant un identifiant dit "login" et un mot de passe) permet l'accès d'un utilisateur à une application sur ledit site web. Comme on le sait, les pirates et fraudeurs ont développé des outils et des techniques pour usurper de telles identités numériques, notamment les *"chevaux de Troie"*, les logiciels *"espions"*, les *"keyloggers"* et les *renifleurs de réseau* tels que le "Man in the

20 Middle". Par ces techniques, il leur devient possible de récupérer les identifiants et mots de passe d'un utilisateur régulièrement enregistré sur un site web, et de se faire passer pour lui auprès de ce site, et à son insu. La détection d'une telle fraude s'avère difficile en raison du fait que les données numériques peuvent être modifiées quasiment sans laisser de traces. En outre, l'attaque peut être portée

25 instantanément depuis un ordinateur distant à des milliers de kilomètres, rendant particulièrement ardue toute protection, notamment sur le plan judiciaire.

La multiplication des usurpations d'identités numériques s'avère aujourd'hui être une menace majeure pour l'économie numérique en général et le commerce en

30 ligne en particulier.

D'où il en résulte une source d'insécurité significative.

On connaît déjà des techniques pour améliorer la sécurité du contrôle d'accès pour les applications numériques. Désignées sous l'appellation «*authentification forte*», elles ajoutent au contrôle de ce que l'utilisateur autorisé sait (son mot de passe), ce qu'il possède (un élément matériel) ou ce qu'il est (ses données biométriques comme par exemple ses empreintes digitales).

Une première technique connue sous l'appellation anglo-saxonne "*One Time Password*" consiste à doter chaque utilisateur légitime d'un dispositif électronique capable de générer un nombre aléatoire servant de mot de passe lors de sa connexion à l'application en ligne. Ainsi l'interception ou la capture du mot de passe ne permettra pas l'accès à l'application en question, parce que ce mot de passe ne sera plus valable dès lors qu'il aura déjà été utilisé et donc aura été valable une seule fois, d'où la dénomination de *One Time Password*.

Une autre technique connue sous le nom de «*hors bande*» consiste à envoyer un message sur un autre canal de communication, par exemple un SMS sur le téléphone mobile de l'utilisateur lorsque celui-ci souhaite se connecter à son système d'information ou au site web en question. La procédure d'authentification n'aboutit que lorsque le serveur web reçoit communication du code expédié à l'utilisateur via l'autre voie de communication. Il en résulte qu'un pirate aura beau intercepter et contrôler ce que l'utilisateur licite fait sur son poste de travail, il ne pourra cependant pas récupérer l'élément manquant transmis par le téléphone mobile et hors de portée de lui.

Une autre technique fondée sur les infrastructures à clés publiques (PKI) consiste à équiper le système de chaque utilisateur d'un certificat électronique. Lorsque l'utilisateur se connecte à l'application, le mécanisme de contrôle d'accès vérifie la présence dudit certificat sur son interface et valide une séquence d'authentification.

Une autre technique encore consiste à comparer le fichier biométrique de l'utilisateur autorisé, par exemple son empreinte digitale, avec une caractéristique biométrique de référence et stockée, soit dans une carte à puce ou dans le serveur de contrôle d'accès au moment de l'enrôlement de cet utilisateur.

Toutes ces techniques génèrent un jeton d'accès, dénommé dans la littérature anglo-saxonne par l'appellation "*token*", lequel permet l'authentification – en principe – du seul utilisateur légitime. Comme on le comprend, il apparaît fondamental dans toutes ces techniques qu'une seconde présentation de ce jeton (ie un nouveau
5 « *jeu* » du jeton ou *token*) par un tiers ne puisse aboutir à une authentification illégitime et, par suite, une fraude sur le réseau.

Bien que ces techniques présentent une efficacité avérée et incontestable, il convient d'observer qu'elles ont été conçues et mises en œuvre à une période
10 précédent le déploiement massif de l'Internet tel qu'on le connaît aujourd'hui. A cet égard, ces techniques présentent aujourd'hui des inconvénients rédhibitoires alors même que la société évolue vers une économie complètement dématérialisée et que le grand public tend à généraliser l'usage du réseau Internet pour toutes sortes de transactions possibles. De ce fait, des techniques qui pouvaient apparaître
15 efficaces et adaptées à un cercle restreint d'utilisateurs – à savoir des utilisateurs avertis capables d'installer sans difficulté des systèmes et logiciels sophistiqués sur leur machine – ces mêmes techniques présentent aujourd'hui des inconvénients rédhibitoires lorsqu'il s'agit de faire bénéficier le plus grand nombre des bénéfices résultant de l'utilisation du réseau Internet.

20

La demande de brevet européen 04368072.7 déposée le 1^{er} Décembre 2004 par le titulaire de la présente requête décrit un procédé d'authentification très efficace basé sur la collecte des très nombreuses informations par le système d'exploitation, notamment celles requises pour lui permettre de vérifier la présence des pilotes
25 pour l'interfaçage avec le système d'exploitation. Ces informations, une fois collectées, permettent la génération d'une information unique, caractéristique du système, et permettant de le distinguer des autres systèmes. Cette information – désignée sous l'appellation « *ADN du numérique* » ou ADNN par la société titulaire de la demande de brevet, permet d'accroître significativement la sécurité de la
30 procédure d'authentification.

Le procédé qui est décrit dans la demande de brevet précitée renforce ainsi considérablement la sauvegarde de l'identité des personnes et ne requiert nullement la divulgation des éléments d'identité personnelle de l'utilisateur (nom,

domicile, etc...). Ce procédé présente cependant l'inconvénient d'exposer de manière non opportune cette information numérique particulièrement sensible qu'est l'« ADN du numérique » rendant unique la machine de l'utilisateur.

- 5 Ainsi, tout tiers pourrait être amené à intercepter cette information « ADN numérique », de la détourner de son usage légitime et de procéder à une usurpation d'identité, ce que l'on souhaitait justement éviter.

Pour éviter une telle situation, il convient de disposer d'une technique spécifique,
10 parfaitement adaptée à la protection de l'information ADNN notamment lors de son transit sur le réseau Internet.

Tel est le problème à résoudre par l'objet de la présente demande de brevet.

15

Résumé de l'invention

- 20 C'est un but de la présente invention de réaliser une procédure d'authentification renforcée pouvant, le cas échéant, se substituer au traditionnel identifiant-mot (*login-password*) de passe tout en laissant à l'utilisateur la possibilité de définir lui-même le jeton (*token*) utilisé pour son authentification

- 25 C'est un autre but de la présente invention que d'assurer la protection du jeton utilisateur lors de son utilisation lors des diverses procédures d'authentification.

- C'est un troisième but de la présente invention de contrôler l'accès à une application numérique en cours d'exécution sur un serveur distant géré par un
30 fournisseur d'applications à partir d'un système de traitement de l'information exploité par un utilisateur autorisé.

C'est est un quatrième but de la présente invention de protéger l'identité numérique nécessaire pour accéder à une application numérique, de façon à prévenir le vol d'identité et l'usurpation de l'identité de l'utilisateur autorisé.

- 5 C'est un cinquième but de la présente invention de permettre l'utilisation d'une identité numérique afin de contrôler l'accès d'un système d'information IHS (*Information Handling System*) à une application numérique de telle sorte que si l'identité numérique s'avérait interceptée, elle ne puisse être utilisée pour accéder à l'application protégée.

10

C'est un sixième but de la présente invention de réaliser un système d'authentification forte ne nécessitant pas l'installation complexe d'un logiciel sur les machines génériques permettant l'accès du grand public au réseau Internet et aux sites web qui le composent.

15

C'est un septième but de la présente invention de réaliser cette authentification forte sans que l'utilisateur ait à transmettre sur le réseau une information privée sensible.

- 20 C'est un huitième but de la présente invention de réaliser un procédé d'authentification forte n'exigeant pas de l'utilisateur qu'il mémorise un mot de passe.

- 25 C'est enfin un neuvième but de la présente invention que de réaliser un procédé d'authentification forte qui soit complètement transparent pour l'utilisateur qui pourra procéder à son inscription et son authentification sur un site web de manière totalement automatique.

- 30 L'invention réalise ces buts au moyen d'un procédé d'authentification renforcé basé sur la collecte de données représentatives de composants matériels contenus dans un système (I.H.S), ledit procédé comportant une étape d'enrôlement et une étape d'authentification comportant les étapes :

- connexion à un site web et réception d'une page web comportant un code exécutable ;
- détection et collecte d'une liste de composants matériels à partir des informations collectées par le système d'exploitation, notamment pour le chargement des pilotes ;

Caractérisé en ce que la procédure d'enrôlement comporte en outre les étapes suivantes :

- affichage d'une liste de composants matériels résultant de ladite collecte et sélection d'un sous-ensemble de ladite liste dans le but de constituer une information numérique de référence (ADNN) du système de l'utilisateur ;
- génération d'une information numérique de référence (ADNN) à partir dudit sous-ensemble, ladite information numérique de référence résultant d'une opération de hash appliquée aux données brutes que composent les données collectées ;
- utilisation de ladite information numérique de référence (ADNN) avec une semence reçue d'un serveur d'authentification dans le but de générer un mot de passe à usage unique (*OTP – One Time Password dans la littérature anglo-saxonne*).

Dans un mode de réalisation particulier, la semence générée par le site d'authentification provient d'un générateur quantique intégré au dit site d'authentification.

Dans un mode de réalisation spécifique, l'OTP est généré en outre à partir du code PIN de l'utilisateur, concaténé avec ladite information numérique de référence ADNN, et l'aléa .

De préférence, l'OTP est généré en outre à partir d'une information numérique de référence relative au serveur d'authentification, lequel est concaténé au code PIN et à la dite information numérique de référence ADNN du système de l'utilisateur, et l'aléa.

L'on pourra également venir concatener, à l'information de base servant à générer l'OTP, un timestamp permettant d'inscrire une information de chronodatage dans ledit OTP.

5

Ainsi l'invention permet d'utiliser avantageusement un ou plusieurs identifiant matériels choisis par l'utilisateur, de façon à réaliser un jeton-utilisateur (*user token*) permettant une authentification renforcée, et de protéger ce jeton au sein d'une procédure d'authentification intégrant un double *challenge-response*.

10

15

Description des dessins

20

D'autres caractéristiques, but et avantages de l'invention apparaîtront à la lecture de la description et des dessins ci-après, donnés uniquement à titre d'exemples non limitatifs. Sur les dessins annexés :

25

La figure 1 illustre le principe d'un mode de réalisation autorisant l'utilisateur à définir lui-même le jeton d'authentification intégrant un ou plusieurs éléments matériels pour la génération de l'information numérique ADNN.

30

La figure 2 illustre les échanges de flux dans un second mode de réalisation de l'invention.

Description d'un mode de réalisation préféré

Les recherches conduites par le demandeur ont montré que l'information ADNN (ADN du numérique ®) facilite de manière significative l'authentification forte entre un prestataire de service et un utilisateur du service, connecté par un LAN, un WAN ou Internet, à travers un ordinateur ou un *smartphone* (Symbian ® , iPhone®, Android®, Windows Mobile®). Dans une première étape d'enrôlement, l'utilisateur décide quel composant matériel va lui servir de token, ce qui l'authentifiera de manière unique par la suite.

10

En effet, comme on va le voir dans le premier mode de réalisation décrit ci-après, cette information numérique ADNN autorise l'utilisateur à procéder lui-même à la définition du jeton (*token*) qui lui servira d'authentification.

15

I. Premier mode de réalisation d'un procédé d'enrôlement et d'authentification

L'on décrit à présent, en relation avec la figure 1, un premier mode de réalisation d'un procédé d'authentification permettant soit de se substituer à la méthode conventionnelle de l'identifiant/mot de passe (*login-pw*), soit de venir en complément de cette méthode pour renforcer significativement l'authentification de cet utilisateur au moyen d'un jeton (*token*) directement choisi par l'utilisateur.

25

Le procédé qui sera décrit ci-après met en œuvre trois entités, à savoir un logiciel *client* tournant chez l'utilisateur, un site web accessible sur le réseau intranet ou internet, et un serveur d'authentification agissant en qualité de tiers de confiance, les trois éléments 100, 200 et 300 pouvant communiquer via des canaux sécurisés tels que CHAP (*Challenge Hardware Authentication Protocol*), HTTPs , bien connus d'un homme du métier et qu'il n'est ni nécessaire ni opportun de développer plus avant.

30

Le procédé comporte une phase d'enrôlement, laquelle sera ensuite suivie d'une phase d'authentification.

5 1. Enrôlement.

L'on suppose que l'utilisateur souhaite se connecter sur un site Internet via le réseau internet et lance par conséquent son logiciel navigateur installé dans son système. Le procédé démarre par conséquent par une étape 10 qui est une connexion transmise au site web.

Dans une étape 20, le site web répond, par exemple au moyen d'une réponse de type 200 définie dans la RFC2616 portant sur le *HyperText Transfer Protocol* et bien connue d'un homme du métier, au moyen d'une page web comportant par exemple un plugin ou applet java, à savoir un code exécutable permettant l'exécution de la suite de la procédure décrite ci-après et commençant pas inviter l'utilisateur à présenter à un identifiant de connexion (*login*) assorti d'un mot de passe (*password*).

20

En pratique, la réponse de l'étape 20 du site web pourra se conformer à une grande variété de situations et protocoles distincts. En effet, outre la bien connue page « 200 » du protocole http, l'on pourra considérer toutes les possibilités permettant l'ouverture d'une page d'authentification, notamment CHAP, MSCHAP (la version éditée par l'américain MICROSOFT Corp.), mais également les versions BASIC et CHALLENGE RESPONSE, et également RADIUS (*Remote Access Dial-in User Service*) bien connues d'un homme du métier. Dans un mode de réalisation particulier, qui est celui choisi par le titulaire de la présente demande de brevet, un kit logiciel est proposé aux éditeurs de site web pour la mise en œuvre des procédés décrits dans la présente demande.

30

Dans l'étape 20 peut comporter notamment la transmission par le serveur d'authentification d'une liste de classes correspondant à une liste de types de matériels et composants éligibles au calcul des empreintes ADNN du système de

l'utilisateur. Cette liste peut comporter le type de processeur, la carte mère, des types de périphériques USB, voire de périphériques communiquant (tel qu'un SMARTPHONE ou Portable Document Assistant (PDA) etc...

- 5 L'exécution de l'applet contenue dans la réponse reçue du site web provoque alors, dans une étape 30, une collecte des données, à savoir le démarrage d'une procédure de détection des composants matériels du système dans le but de recueillir des données auprès desdits composants au travers des pilotes et rapports au système d'exploitation .

10

- D'une manière générale, on pourra s'inspirer largement des développements existants dans la demande de brevet européen 04368072.7 précitée, laquelle donne des exemples de composants pouvant être utilisés. Comme cela est décrit
15 dans cette demande de brevet, un grand nombre d'informations concernant les divers composants matériels sont reportés au système d'exploitation, qu'il s'agisse de WINDOWS sous ses diverses moutures (XP, VISTA, WINDOWS 7...) ou LINUX etc, notamment dans le but de permettre le chargement des pilotes nécessaires à l'interfaçage du système d'exploitation avec ces composants. L'apport de la
20 demande précitée, consiste à rassembler cette information significative, initialement destinée au fonctionnement « interne » du composant, dans le but de constituer une information numérique unique (ADNN) pouvant servir à la mise en œuvre d'une opération d'authentification renforcée.

- 25 Ainsi, dans le cas d'une clé USB conventionnelle, on relève que jusqu'à 16 caractéristiques (la marque, le modèle, le numéro de série, la taille mémoire...etc...) sont accessibles au système d'exploitation et peuvent être potentiellement utilisées pour la génération de l'information numérique désignée par l'appellation ADNN.

- 30 Dans un mode de réalisation particulier, la détection de composants est réalisée en se conformant à une liste de classes de classes définie par le site d'authentification et transférée depuis celui-ci lors de l'étape 20.

Une fois l'opération de détection achevée, le procédé propose à l'utilisateur, lors d'une étape 40, la sélection d'un sous-ensemble des composants identifiés lors de l'étape 30 dans le but de collecter les données accessibles au système d'exploitation et représentatives du sous-ensemble de composants sélectionnés par l'utilisateur. Dans un mode de réalisation, la sélection de l'utilisateur est une option par défaut, et l'absence de sélection par ce dernier conduit alors à la génération d'un jeton utilisateur intégrant un ensemble pré-déterminé de composants matériels présents dans le système, notamment tel que défini par l'administrateur du système.

Comme on le voit, l'utilisateur peut ainsi choisir, lors de l'étape 40, son ordinateur comme élément matériel ou bien un élément à mémoire connecté à son ordinateur (une clé USB, un lecteur MP3...) ou bien un smartphone. Le composant matériel sélectionné est celui depuis lequel va être extrait l'information qui permettra la génération ultérieure de l'information ADNN (l'ADN du numérique ®) . L'utilisateur peut combiner plusieurs éléments physiques comme son ordinateur et une clef USB. Il pourra compléter le dispositif par un PIN code afin d'éviter l'utilisation abusive de son matériel en cas de perte ou de vol.

Dans une étape 50 , le procédé peut à présent effectuer un traitement de données visant à concatener les données brutes collectées lors de l'étape précédente dans le but de générer une information numérique représentative des composants matériels présents dans le système. Ces données brutes concaténées font ensuite l'objet d'une opération de hash dans le but de générer une information numérique de référence : désignée par l'appellation « l'ADN du numérique » ou ADNN. Cette information ADNN résulte donc de la transformation, au moyen d'un d'un algorithme de hash réalisé sur la chaîne de caractères concatenant les différentes informations extraites par l'OS des composants matériels. On pourra à cet égard considérer les algorithmes MD4 ou MD5 de M. Ronald Rivest, ou l'algorithme plus récent SHA mis au point par NIST.

30

Dans un mode de réalisation particulier, on effectue une empreinte particulière de cette information ADNN au moyen de l'opération suivante :

PKCS_PBKDF2_HMAC<SHA256> (sha256(pin code user) + hash(ADNN) + magic number + seed).

Le résultat de cette opération sera désigné, dans la suite, sous le vocable
5 « empreinte ADNN ». Mais il ne s'agit que d'un exemple illustratif, nullement limitatif
et l'on pourrait indifféremment considérer toute autre opération. Plus
particulièrement, l'on pourrait même désigner la chaîne de caractères concatenées
sous l'appellation ADNN et désigner sous le vocable « empreinte de l'ADNN » le
résultat d'un hash sur cette chaîne de caractères.

10

De multiples variantes d'exécutions sont possibles. L'essentiel étant que
l'empreinte ADNN qui est susceptible d'être transmise sur le réseau (dans une
variante particulière) est le résultat d'au moins un hash pour assurer la protection de
l'information originelle composée de la chaîne de caractères des composants
15 matériels du système I.H.S. de l'utilisateur..

En effet, le recours à l'algorithme de HASH assure ici que les données
brutes servant à la génération de l'information ADNN ne seront jamais divulguées.
Le système peut effectuer une analyse de la qualité des données brutes pour
20 déterminer si elle est satisfaisante pour une utilisation, comme certains composants
numériques ne peuvent avoir suffisamment de critères d'unicité nécessaires.

Ne pouvant remonter aux données brutes, l'empreinte ADNN pourra être
transmise au serveur d'authentification pour y être stockée et servir ultérieurement à
25 des fins de vérification.

Alternativement, comme on va le voir à présent, il sera même possible de
s'affranchir de la transmission de l'information numérique de référence ADNN, afin
d'accroître encore la sécurité du procédé d'authentification.

30

A cet effet, le procédé poursuit avantageusement avec une étape 60 qui
consiste en l'intégration de l'information numérique ADNN à la génération d'un mot
de passe à usage unique (OTP), tel que défini notamment par la norme RFC 2289.
A cet effet, l'on vient concatener l'information ADNN ou alternativement son

empreinte, avec une semence (seed) fournie par le serveur d'authentification et le tout faisant l'objet d'une série d'opérations de hash dans le but de générer un OTP.

Dans un mode de réalisation particulier, on intègre l'information numérique de référence ADNN à une semence générée par un générateur quantique de manière à accroître considérablement la résistance du procédé d'authentification.

Dans un autre mode de réalisation, on intègre également dans l'OTP, en même temps que l'aléa quantique, le PIN code de l'utilisateur, un time stamp ainsi que l'information numérique de référence correspondant au serveur d'authentification. Il reste de cette combinaison multiple une grande robustesse au mécanisme d'OTP et, par conséquent, à la protection de l'information ADNN.

Comme on le voit, le procédé qui vient d'être décrit en référence à la figure 1 présente l'avantage significatif, que ne permettaient pas les techniques connues, de générer un jeton utilisateur (user token) puisque c'est ce dernier qui peut choisir le ou les composants qui serviront à générer l'information ADNN, laquelle peut ne jamais être transmise sur le réseau.

Par ailleurs, on notera qu'il est donné à l'utilisateur la possibilité d'enregistrer plusieurs « empreintes ADNN » de manière à lui permettre de créer plusieurs modalités différentes d'enrôlement et d'authentification, chacune étant liée, par exemple, à un composant matériel (clé USB, mobile etc...) distinct.

C'est là un avantage considérable de la solution préconisée. C'est l'utilisateur qui garde la maîtrise de la définition de l'élément matériel qu'il possède et qui servira à la constitution de son information ADNN et, par conséquent, l'authentifiera sur les sites Internet. Ainsi, ce n'est plus un matériel spécifique fourni par un prestataire qui assure cette authentification, mais c'est tout composant matériel susceptible de se connecter à l'ordinateur de l'utilisateur.

Le procédé décrit présente en outre un avantage décisif par rapport à d'autres techniques d'authentification forte, notamment basées sur la biométrie. En effet, les utilisateurs sont toujours réticents à l'idée de voir des données personnelles

transiter sur les réseaux et cette inquiétude est parfaitement légitime. La solution qui est proposée permet un niveau de sécurité comparable (en raison de la grande diversité des composants matériels et des informations spécifiques remontées au système d'exploitation, par exemple 16 paramètres dans le cas d'une clé USB, jusqu'à 43 paramètres dans le cas d'un ordinateur) , tout en préservant l'utilisateur d'une divulgation de ses données biométriques, donc permettant de connaître ou d'usurper son identité.

La technique proposée dans la présente demande de brevet, parce qu'elle substitue aux données biométriques une information bien moins personnelle – l'ADN du numérique – permet néanmoins d'assurer une authentification très performante. Et que l'on peut aisément réinitialiser en cas d'usurpation, contrairement aux données biométriques qui sont immuables.

La procédure d'enrôlement qui vient d'être décrite peut servir de support à une procédure d'authentification forte permettant de tirer avantage de l'empreinte ou de la diversité des empreintes ADN créées par l'utilisateur.

2. Procédé d'authentification forte

20

La mise en œuvre de la procédure d'authentification de l'OTP décrit précédemment (dit *OTP user token* pour exprimer le fait que c'est l'utilisateur qui définit lui-même le composant matériel servant à l'authentification) requiert la mise en place d'une fonctionnalité spécifique, et ce au moyen d'un code approprié présent dans sa page d'authentification) communique avec le poste client, lui même équipé d'un logiciel installé uniquement la première fois (appliquette JAVA, module ActiveX, plug-in du navigateur, widget, autre...) :

1. Un certificat X509v3 original disposé sur le serveur d'authentification permet au navigateur de l'utilisateur de vérifier que l'identité du serveur n'a pas été usurpée (tentative de *phishing* ou hameçonnage par exemple)

2. L'utilisateur clique sur l'authentification par ADN du numérique qui a remplacé le couple « login-password » sur la page du site. Il doit renseigner uniquement son identifiant et le serveur vérifie la cohérence entre cet identifiant et son information numérique ADNN stockée, le cas échéant, sur le serveur. Il doit ensuite indiquer
5 son code PIN - de manière optionnelle suivant le choix du site web concerné - pour s'authentifier.

3. L'information numérique de référence (ADNN ou ADN du Numérique®) est calculée, soit à partir de l'ordinateur lui-même, par plusieurs des composants internes (carte mère, processeur, disque dur...) ou encore à partir d'un composant
10 amovible (clé USB)). Il est ensuite complété optionnellement par le code PIN saisi par l'utilisateur. Une génération aléatoire (random) permet de créer le challenge avec le serveur mais également le chiffrement d'une résultante de hash. Ce hash [ADNN + random + identifiant + (PIN)] transite alors vers le serveur d'authentification via un tunnel chiffré conventionnel (https) tel que l'on rencontre
15 dans un système OTP classique. Ce serveur d'authentification va alors directement autoriser (ou pas) la connexion au site web, ou va passer l'autorisation à un autre serveur (Active Directory, LDAP, ou Radius). En aucun cas, le client ne transmet le mot de passe en clair au serveur sous https.

20

II. Second mode de réalisation du procédé d'enrôlement et d'authentification

L'on décrit à présent, en relation avec la figure 2 un second mode de
25 réalisation venant préciser d'avantage un exemple de procédure d'enrôlement et d'authentification.

Comme on le voit sur la figure, le procédé met en œuvre le logiciel *client* 100
localisé au sein de l'ordinateur de l'utilisateur ou internaute, un site web 200 sur le
30 Réseau Internet, et un serveur d'authentification 300 agissant en qualité de tiers de confiance, les trois éléments 100, 200 et 300 pouvant communiquer via des canaux sécurisés de type HTTPS bien connus d'un homme du métier.

Dans une étape 110, le procédé démarre par conséquent par une connexion transmise au site web.

5 Dans une étape 120, si l'application client pour la mise en œuvre des procédures décrites ci-après n'est pas déjà installée sur le poste client, alors le site web répond au moyen d'une page web comportant un plugin ou applet java pour la mise en œuvre des procédures et méthodes décrites ci-après, et commençant par inviter l'utilisateur à présenter à un identifiant de connexion (*login*) assorti d'un mot de passe (*password*).

10

L'exécution de l'application client ou de l'applet contenue dans la réponse reçue du site web provoque alors, dans une étape optionnelle 130, une connexion au serveur d'authentification dans le but de solliciter les paramètres d'authentification, lesquels serviront à la génération du mot de passe OTP. D'une
15 manière générale, les paramètres d'authentification fournissent la liste de classes de matériels éligibles pour permettre la connexion au serveur web considéré : CPU, carte mère, périphériques USB, smartphone, etc. La liste des classes éligibles est définie par l'administrateur du serveur. La liste est un string codé en base 64.

20

Puis, dans une étape 140, elle aussi optionnelle, le serveur d'authentification envoie une information représentative d'une liste de types de matériels et composants éligibles au calcul de l'ADNN caractéristique du système de l'utilisateur. Cette liste peut comporter le type de processeur, la carte mère, des types de périphériques USB, voir de périphériques communiquant (tel qu'un smartphone ou
25 un Portable Document Assistant (PDA) etc...

30

Dans une étape 150, l'applet transmet un message sollicitant du serveur d'authentification 300 un challenge, conformément à la spécification de la norme RFC 2289.

30

Dans un mode de réalisation nullement limitatif, le message de requête du challenge, transmis dans l'étape 150, comporte un certain nombre de paramètres, lesquels sont :

A titre d'exemple nullement limitatif, on pourra adopter un challenge et une séquence d'authentification telle que définie ci-après :

5 **DDNA User has the fields :**

- login = user login
- mobUid = mobUid returned by the server
- authKey = generated strongkey (also called authKey)
- userSettings :
- 10 - email
- password = SHA256 (user pin code)

refKeystore has the fields :

- cipherData = refKeystoreData;
- 15 - type = 0;

keystore has the fields :

- cipherData = keystoreData;
- dnaMetaData =
- 20 - challengeKey = dnaChallengeKey
- migrationKey = dnaMigrationKey
- description = dna.description
- type = dna.type
- deviceList =
- 25 - description
- deviceClass
- type = STRONG

Initialisation

30 openApi()
 list<Device>
 listConnectedDevices()
 policy
 getParameter(accountid, type)

35 registerUser(login, userSettings(email, pin code>), dna(description, type,
 list<Devices>, Uid))
 generateMobUid()
 mobUid
 40 addDnaUserKeystore(accountid, dnaUser, refKeystore, keystore)

Generate passport

45 generate "refKeystoreData"
 generate "keystoreData"
 generate "dnaChallengeKey" et "dnaMigrationKey"

Select Devices

- dnaChallengeKey = PKCS_PBKDF2_HMAC<SHA512> (SHA256 (pin code
 50 user) + qki_hash(selected devices) + magic_number , SALT2)
- dnaMigrationKey = qki_hash(selected devices)
- mobUid = the mobUid returned by the server
- strongKey(authKey) = SHA256 (random, sel)
- privKey = SHA256 (random, sel)

- ref_key = PKCS5_PBKDF2_HMAC<SHA512> (SHA256 (user pin code) +
 magic_number, SALT1)
 - refKeystoreData= Crypt_AES (passport, refKey)
 5 - key = PKCS5_PBKDF2_HMAC<SHA512> (SHA256 (user pin code) +
 qki_hash(selected devices) + magic_number, SALT2)
 - keystoreData= Crypt_AES (passport, key)

register user with DDNA

10
 Dans une étape 160, le serveur d'authentification génère par conséquent un premier challenge, lequel est un objet renvoyé par le serveur ayant, entre autres, un champ "challenge" de type string. Dans un mode de réalisation particulier, le
 15 contenu du challenge est généré en intégrant un aléa généré par carte quantique intégré au serveur d'authentification.

De préférence, le challenge se présente de manière définie dans la RFC
 « ONE TIME PASSWORD » :

20 otp-<identifiant de l'algorithme> <numéro séquence> <seed>

tel que par exemple otp-md5 487 dog2 venant préciser l'utilisation de
 l'algorithme de hash MD5, un numéro de séquence 487 et une semence égale à
 25 « dog2 » .

Dans un mode de réalisation particulier, l'inventeur a découvert qu'il était
 possible de renforcer de manière suprenante la robustesse de l'algorithme en
 optant pour une semence générée au moyen d'un générateur quantique assurant
 30 un aléa parfait. Un tel générateur quantique fonctionne sur le principe d'un choix
 d'un photon susceptible de traverser ou non une lame semi-réfléchissante.

Dès réception du premier challenge, l'application client ou l'applet génère,
 lors d'une étape 170, la réponse circonstanciée correspondant à ce premier
 35 challenge. Pour le détail de la réponse à transmettre au serveur, en fonction du
 challenge reçu, l'on pourra s'inspirer par exemple des protocoles CHAP
 (*Challenge Hardward Authentication system*) bien connus d'un homme du métier.
 D'une manière générale, on observera que le procédé qui est décrit est adapté à

l'emploi d'un grand nombre de variantes de challenge/response qui sont à la portée d'un homme du métier et qui ne seront pas développés plus avant.

5 Puis le procédé procède à la génération d'une information d'authentification primaire comportant :

- le LOGIN de l'utilisateur ;
- un hash du code PIN de l'utilisateur (e.g. le sha256 de la librairie open source cryptopp) ;
- 10 - la réponse au premier challenge.

Cette information d'authentification primaire est ensuite transmise au serveur d'authentification suivant un canal sécurisé HTTPs , par exemple.

15 Dans une étape 180, le serveur d'authentification 300, qui dispose au sein de sa base de données les informations d'identification (login , PIN) vérifie l'information d'authentification primaire et transmet sa réponse, négative ou positive. Lorsque la réponse est positive, le serveur transmet un premier identifiant de session *sessionID1*, ce qui prouve l'existence de l'utilisateur dans la base et
20 démarre le véritable dialogue d'authentification entre le client et le serveur.

A partir de ce moment, l'application cliente ou l'applet communique avec le serveur d'authentification 300 au moyen de l'identifiant de session *sessionID1* et non plus au moyen d'une identification de login conventionnel, lequel pourrait avoir
25 été usurpé. Comme on le voit, on améliore ici significativement la sécurité du procédé d'authentification.

En effet, dans une étape 190, l'application cliente ou l'applet transmet un message de requête au serveur d'authentification 300 en utilisant l'information
30 *Session ID1* et sollicite que lui soit transmise une information représentative du nombre d'empreintes ADNN et, pour chacune d'entre elles, la liste des classes de composants matériels (processeurs, périphériques , clés USB etc...) auxquelles elles correspondent. Il est à noter, et cela est important pour la compréhension du niveau de sécurité permis par le procédé, que les empreintes ADNN ne sont

nullement transmises lors de cette étape 190... Seule une « liste » indiquant les identifiants des empreintes et la définition des classes correspondant à chaque élément de la « liste » fait l'objet de la transmission.

5 Dans une étape 200, le serveur d'authentification répond et transmet cette « liste » précisant le nombre d'empreintes ADNN et pour chacune d'entre elles, la définition des classes utilisées.

10 A suite de la réception de cette description, le procédé mis en œuvre par l'applet entre dans une boucle, illustrée dans la figure 2 par les étapes 210-241 ou 210-242), laquelle boucle va tenter une authentification secondaire au moyen d'un traitement séquentiel de chacun des éléments de la liste d'empreintes reçue lors de l'étape 200 .

15 En effet, pour chacune des empreintes listées dans la liste de l'étape 200, l'applet transmet, dans une étape 210 un message sollicitant un nouveau challenge, auquel le serveur répond, lors d'une étape 220 par un nouveau challenge, intégrant une semence (seed) (Nième challenge), basée sur le générateur quantique mentionné précédemment.

20 Puis, lors d'une étape 230, l'application cliente ou l'applet calcule l'information ADNN correspondant aux classes associées à l'empreinte considérée (et définie sur la liste de l'étape 200), et prépare une réponse au challenge de l'étape 220.

25 L'étape 230 s'achève par la transmission au serveur d'authentification des éléments d'authentification secondaires, lesquels comportent notamment les informations suivantes :

- 30
- l'identifiant de connexion SessionID2 (permettant de retrouver dans la base du serveur d'authentification le login de l'utilisateur)
 - le hash du code PIN (si cette option a été choisie)
 - le résultat du calcul de l'empreinte ADNN pour l'élément considéré de la liste de l'étape 200

- la réponse présumée valide ou invalide au Nième challenge quantique (un challenge par matériel trouvé dans la liste des empreintes ADNN pour l'utilisateur considéré).

5 Puis, le serveur d'authentification les éléments d'authentification puis envoie sa réponse négative (flèche 241) ou positive (flèche 242), comportant un identifiant secondaire de session *sessionID2*.

10 Dans le cas d'une réponse négative, l'application cliente tente une authentification secondaire basée sur l'élément suivant de la liste de l'étape 200 jusqu'à épuiser tous les éléments de cette liste et, dans ce cas, rejeter la demande d'authentification.

15 Au contraire, lorsque l'authentification secondaire a abouti, le procédé poursuit avec une étape 250 au cours de laquelle l'applet sollicite en utilisant le *sessionID2* un « *passport* » au bénéfice de l'utilisateur.

Dans une étape 260, le serveur d'authentification 300 répond avec un « *passport* » crypté.

20 Dans un mode de réalisation particulier, le *passport* est créé, chiffré et stocké lors de l'enrôlement de l'utilisateur (en intégrant ou non l'information ADNN), de la manière suivante :

Le logiciel client concatène dans un string :

- un UUID demandé au server
- 25 - une *strongKey* créée en générant un string aléatoire hashée en SHA256 avec une semence (*seed*)
- une *privateKey* (réservée à un usage ultérieur)

30 Ce *passport* est ensuite chiffré par le logiciel client en AES en utilisant comme clé de chiffrement (*strongkey*) :

PKCS_PBKDF2_HMAC<SHA256> (sha256(pin code user) + hash(ADNN) + magic number + seed)

Le passeport est stocké sur le serveur d'authentification pour les authentifications ultérieures de l'utilisateur via sa *strongkey*.

5 Le passeport est stocké temporairement pendant la durée autorisée de la session (fixée par l'administrateur du système) sur le serveur d'authentification, valable pour toutes les authentifications de l'utilisateur sur le site web considéré. Le système peut également passer cette autorisation d'authentification de manière optionnelle à d'autres systèmes tels que RADIUS ou ACTIVE DIRECTORY.

10 Puis, dans une étape 270, l'applet décrypte le passeport pour récupérer la *strongkey* de l'utilisateur. Il utilise pour se faire le code PIN de l'utilisateur et l'ADNN du serveur d'authentification. Le client peut alors accéder de manière sécurisée au site web au moyen de la *strongkey*.

15 **III. Avantages de l'invention**

Le processus d'authentification présente deux avantages majeurs : l'utilisateur n'a pas accès et ne connaît donc pas l'ADN du Numérique car ce dernier est généré seul le challenge -qui est un hash- est envoyé.

20 L'ADN du numérique s'appuie sur des schémas standards de sécurité (https, Challenge Handshake Authentication Protocol (CHAP), SHA, AES...). La génération des challenges est basée sur un aléa quantique qui répond aux bonnes pratiques de sécurité les plus strictes.

25 Le secret partagé entre client et serveur se résume à une information relative à certains composants matériels du client et enfouie dans ces matériels, couplée à un challenge de type OTP. Cette information numérique de référence est désignée par l'appellation : « ADNN ». (ADN du numérique ®)

La protection de cette information est assurée de la manière suivante :

30 - Import sécurisé des paramètres d'enrôlement et d'authentification : les caractéristiques matérielles du poste client que l'application va collecter (soit tout ou partie des composants du poste et/ou un ou plusieurs périphériques

amovibles) sont importés du serveur via un protocole sécurisé (chiffrement SSL).

5 - Transfert sécurisé des données d' enrôlement et d'authentification vers le serveur : les données matérielles choisies par l'utilisateur pour être enrôlées sont collectées par l'application puis transmises vers le serveur au travers d'un protocole sécurisé (https). Ce protocole s'appuie sur un échanges de clé initié par le serveur au début de la session et par un chiffrement AES des données avant transmission. Il y a également un ajout de *seed* « une graine » et de timestamp pour assurer la sécurité et la validité
10 des messages.

- Protection des données rémanentes : toutes les données rémanentes sensibles (clés AES, données matérielles, paramètres) sont effacées des mémoires du PC hôte à la fin de la session.

15 - Intégration d'un double challenge-réponse pour interdire le rejeu : le protocole d'échanges des données entre le serveur et le client intègre une protection contre le rejeu des trames d'authentification, basé sur l'échange de challenges et sur une fenêtre temporelle à respecter pour réaliser l'échange. L'algorithme de chiffrement utilisé est l'AES 256 en mode CBC. Pour le challenge/réponse, l'algorithme utilisé est le HMAC-SHA256.

20 - Encapsulation de l'enveloppe PKCS#11 dans l'enveloppe X9.84 contenant l'ADN Numérique : pour être conforme à l'interopérabilité des solutions d'authentification existantes, le système dispose optionnellement de deux bibliothèques pour la gestion des codes PIN / PUK :

25 - Bibliothèque PKCS#11 permettant pour les applications non Microsoft une communication normalisée avec les commandes PIN de l'ADN.

Dans cette gestion, on retrouve notamment la durée de vie du PIN, le nombre d'essai du PIN, l'activation / désactivation du code PUK.

30 Toutes les règles de sécurité du PKCS#11 sont incorporées dans la bibliothèque de l'ADN du numérique®.

- Bibliothèque CSP : permettant pour les applications Microsoft (IE, Outlook, Windows) une interopérabilité avec l'ADN numérique liée à un 2ème facteur qu'est le code PIN.

5 A noter que la communication entre les DLL PKCS#11, CSP et l'ADN Numérique sont signées par un certificat qui peut être signé par l'AC du client tout comme l'ensemble des DLL et Services de l'ADN du numérique®.

- Appliquette signée (personnalisée par code PIN) numériquement par un certificat X509v3 ce qui aide à détecter les tentatives de *phishing*.
- 10 - Verrouillage du code: Le code exécutable de l'ADN du Numérique® est protégé par *obfuscation* contre le désassemblage. Des mesures de sécurité sont également implémentées afin de renforcer la sécurité lors de l'exploitation (fermeture de la session forcée après une période d'inactivité ou une erreur par exemple). Enfin, les assembly (DLL et exécutables) sont
15 signées.

De même, le fournisseur de l'application peut identifier un mécanisme d'authentification de secours, pour permettre à un utilisateur qui a perdu son IHS
20 utilisé pour l'accès d'authentification de l'application protégée. C'est sa responsabilité de s'assurer que ce mécanisme de secours présente un compromis acceptable entre le niveau de risque et de la frustration des utilisateurs. L'approche recommandée consiste à avoir chaque utilisateur autorisé inscrire plusieurs IHS.

25 Dans un mode de réalisation préféré, l'invention est conforme à la norme IEEE-802 de services et de la famille des protocoles de norme relative aux réseaux locaux (LAN) et réseaux métropolitains (MAN).

L'invention peut trouver des applications dans des situations logiques de contrôle
30 d'accès, en particulier, mais pas nécessairement lorsque la norme de sécurité ANSI X9.84 doit être respectée. Elle peut également être utilisée pour reconnaître un

utilisateur chaque fois qu'il revient sur un site web, comme le font les "cookies" souvent utilisés dans de tels environnements.

5 Le contrôle d'accès logique se réfère à la pratique de la limitation de l'accès aux ressources logiques, telles que les applications numériques ou les données numériques.

10 Le contrôle d'accès logique se trouve principalement dans les environnements d'entreprise, pour contrôler l'accès à un réseau privé dans les locaux d'une entreprise (par exemple via un réseau local) ou d'accéder aux données depuis l'extérieur de la société vers les locaux de l'entreprise (par exemple via un réseau privé virtuel). De plus en plus souvent, le contrôle d'accès logique est nécessaire en fonction des environnements web, soit pour accéder aux données sensibles (santé, services bancaires, etc) ou pour confirmer des transactions par exemple de
15 commerce électronique, les opérations financières, de gestion de contenu web, les réseaux sociaux, etc.

L'invention est bien adaptée à apporter une garantie suffisante à l'ensemble de ces opérations.

20

Dans de nombreuses situations, où le vol d'identité numérique est en jeu, mais la véritable identité de l'utilisateur n'a pas d'importance, une simple procédure d'inscription en ligne peut suffire couplée avec l'ADN du numérique.

25 Dans les situations où un accès illimité à un service est lié au paiement d'un abonnement, l'invention est beaucoup plus efficace qu'un mot de passe pour limiter la fraude résultant du partage du mot de passe avec d'autres utilisateurs non autorisés.

30 Une autre utilisation de l'invention réside dans l'accès au site sans demander à l'utilisateur son identifiant, et où la question primordiale n'est pas la nécessité de reconnaître précisément un utilisateur parmi tous les utilisateurs autorisés. L'invention fournit le même niveau de confiance, sans avoir à déranger l'utilisateur en lui demandant d'entrer son identifiant.

Une autre utilisation réside dans la nécessité pour les prestataires de nombreuses applications d'être conscients de savoir si le visiteur est nouveau ou ancien. L'invention est plus efficace que les cookies, car l'ADN numérique de l'utilisateur
5 IHS ne peut être caché, alors que les cookies le peuvent.

Les domaines d'application de l'invention sont les plus divers sur Internet: les services bancaires en ligne, l'e-commerce, e-gouvernement, abonnements à base de web (revues, musique, vidéo), e-gaming, les réseaux sociaux, ne sont que
10 quelques exemples de domaines où l'invention peut être utilisée avec profit.

Revendications

1. Procédé d'authentification renforcé basé sur la collecte de données
5 représentatives de composants matériels contenus dans un système (I.H.S), ledit
procédé comportant une étape d'enrôlement et une étape d'authentification
comportant les étapes :

- connexion (10) à un site web et réception (20) d'une page web comportant un
10 code exécutable par un logiciel navigateur;
- détection et collecte (30) d'une liste de composants matériels à partir des
informations collectées par le système d'exploitation, notamment pour le
chargement des pilotes ;

15 caractérisé en ce que la procédure d'enrôlement comporte en outre les étapes
suivantes :

- affichage d'une liste de composants matériels résultant de ladite collecte et
sélection (40) d'un sous-ensemble de ladite liste dans le but de constituer une
20 information numérique de référence (ADNN) du système de l'utilisateur ;
- génération d'une information numérique de référence (ADNN) à partir dudit sous-
ensemble, ladite information numérique de référence résultant d'une opération de
hash appliquée aux données brutes que composent les données collectées.

25 2. Procédé selon la revendication 1 caractérisé en ce que ladite information
numérique de référence (ADNN) constitue une empreinte qui est transmise sur un
serveur d'authentification pour y être stockée et servir à des fins de vérification.

3. Procédé selon la revendication 1 caractérisée en ce que ladite information
30 numérique de référence (ADNN) est combinée à une semence reçue d'un serveur
d'authentification dans le but de générer un mot de passe à usage unique (OTP).

4. Procédé selon la revendication 3, caractérisé en ce que ladite semence (Seed) est générée à partir d'un générateur quantique.

5 5. Procédé selon la revendication 3 ou 4, caractérisé en ce que ledit OTP est généré en outre à partir d'un code PIN de l'utilisateur, concaténé avec ladite information numérique de référence ADNN, et un aléa.

10 6. Procédé selon la revendication 4, caractérisé en ce que ledit OTP est généré en outre à partir d'une information numérique de référence relative au serveur d'authentification, lequel est concaténé à un code PIN de l'utilisateur et à la dite information numérique de référence ADNN du système de l'utilisateur, et l'aléa.

15 7. Procédé selon la revendication 6, caractérisé en ce que ledit OTP est généré en outre à partir d'un timestamp, lequel est concaténé avec ladite information numérique de référence du serveur d'authentification, du PIN et de ladite information numérique de référence ADNN du système de l'utilisateur, et l'aléa.

20 8 Procédé d'authentification basé sur la collecte de données représentatives de composants matériels contenus dans un système de traitement de l'information (I.H.S.) d'un utilisateur, ledit système communiquant avec un site web et un serveur d'authentification, ledit procédé comportant les étapes suivantes :

- demande de connexion (110) audit site web via un logiciel navigateur transmise par ledit système ;
- réception par ledit système (120) d'une page web et d'un code exécutable par un logiciel navigateur en réponse à ladite connexion ;
- demande de connexion (130) via le logiciel navigateur transmise audit serveur d'authentification afin de solliciter les paramètres d'authentification destinés à la génération d'un OTP ;
- transmission (140) par ledit serveur d'authentification d'une information représentative d'une liste de types de matériels et composants éligibles pour le calcul d'une information numérique de référence (ADNN) et réception par ledit système de traitement de l'information (I.H.S.) ;
- demande de challenge (150) transmise par ledit système audit serveur d'authentification ;

- génération (160) par ledit serveur d'authentification d'un premier challenge ;
- transmission (170) par ledit système de l'utilisateur d'une information d'authentification audit serveur d'authentification, ladite information comporte :

- 5
- le LOGIN de l'utilisateur ;
 - un hash du code PIN de l'utilisateur ;
 - l'identifiant du premier challenge reçu

- 10
- vérification (180) par ledit serveur d'authentification de ladite information d'authentification transmise par ledit système de l'utilisateur ;

- en cas de succès de ladite vérification, demande (190) par ledit système de l'utilisateur de la description et du type des empreintes (ADNN) stockées sur ledit serveur d'authentification, les dites empreintes (ADDN) étant associées à des matériels susceptibles d'être présents dans le système de l'utilisateur ;;

- 15
- transmission (200) audit système utilisateur par ledit serveur d'authentification de la description et du type des empreintes de l'information numérique de référence (ADNN) stockée sur ledit serveur ;

- détermination d'une liste de matériels à tester sur ledit système utilisateur ;
 - pour chacun des composants matériels correspondant à ladite liste , effectuer les
- 20
- étapes suivantes (210-241);

- transmission (210) d'une demande de challenge audit serveur d'authentification ;
- réception d'un challenge (220) dudit serveur d'authentification ;
- transmission d'une réponse (230) comportant :

25

- l'identifiant de connexion (login) associé à la connexion au site web
- une empreinte basée sur ladite information numérique de référence (ADNN) de composant matériel testé ;
- un hash ;

30

- vérification des éléments d'authentification par le serveur d'authentification et transmission d'une réponse (241, 242) audit système utilisateur comportant un identifiant de session (sessionID2);

- transmission (250) par le système utilisateur d'une demande de passeport associée audit identifiant de session (session ID2) ;
 - transmission (260) par ledit serveur d'authentification du passeport sous une forme crypté ;
- 5 - décryptage par ledit système utilisateur dudit passeport et accès audit site web.
- .

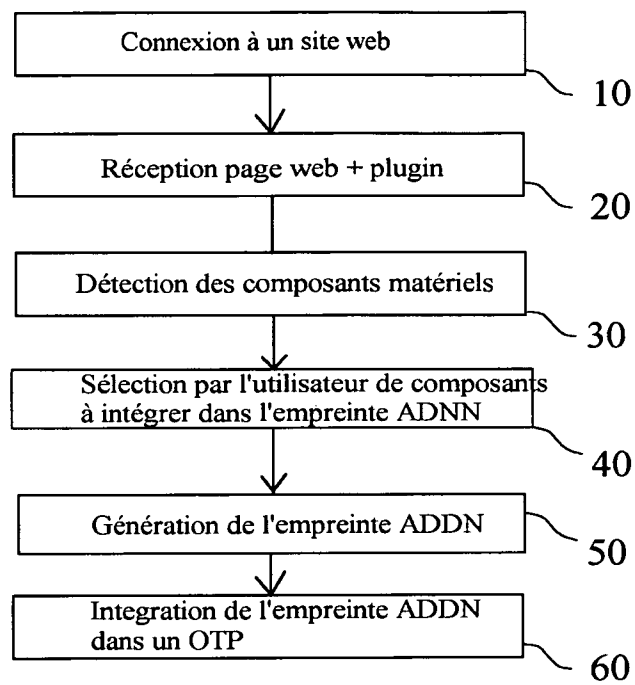


Fig. 1

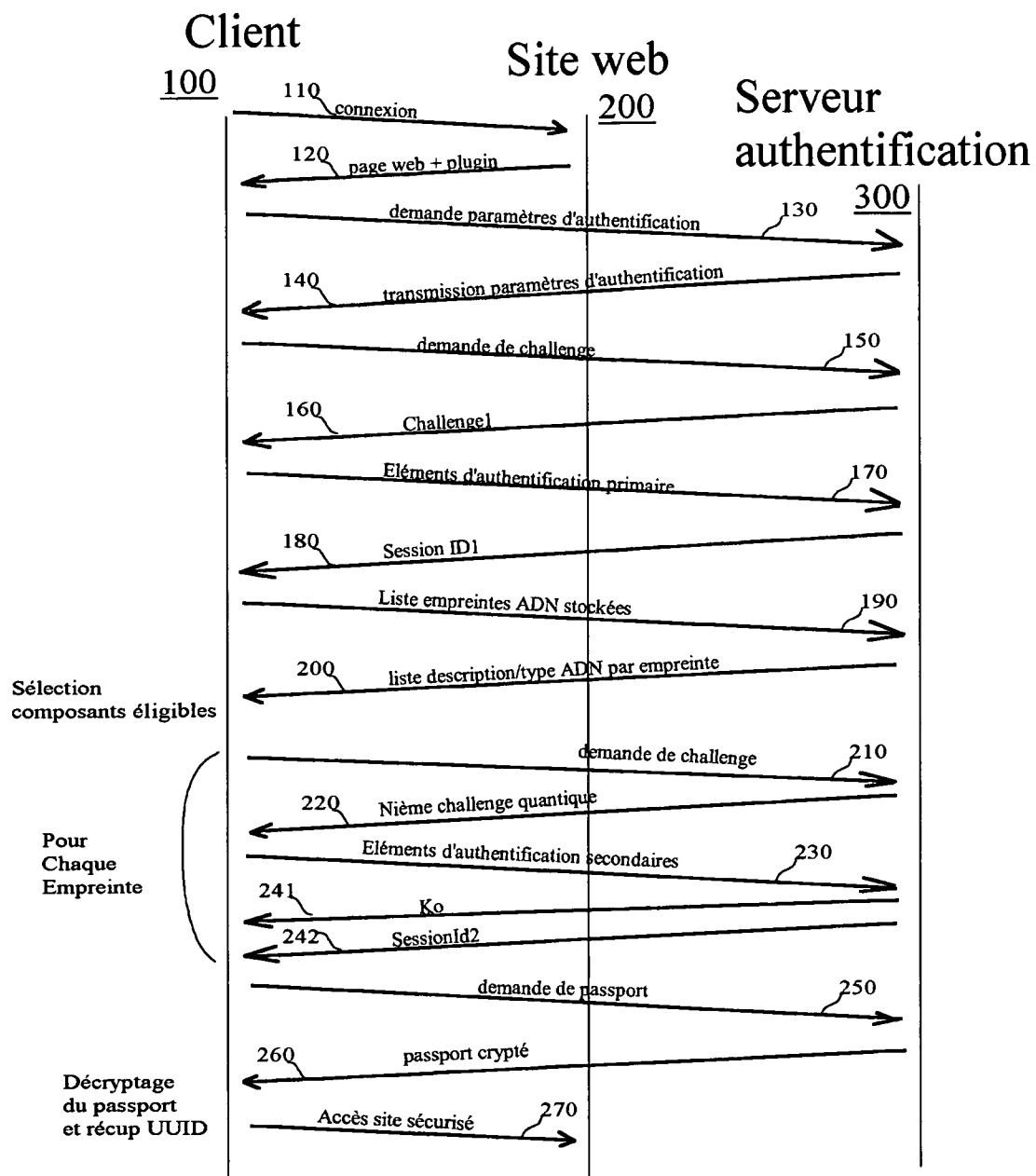


Fig. 2