

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

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
29 octobre 2020 (29.10.2020)



(10) Numéro de publication internationale
WO 2020/217030 A1

(51) Classification internationale des brevets :
G06F 21/34 (2013.01)

(21) Numéro de la demande internationale :
PCT/FR2020/050702

(22) Date de dépôt international :
24 avril 2020 (24.04.2020)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1904394 25 avril 2019 (25.04.2019) FR

(71) Déposant : COPSONIC [FR/FR] ; 1471 route de Saint-Nauphary, 82000 MONTAUBAN (FR).

(72) Inventeurs : **ALFONSO REYES, Ruben** ; 1240 A chemin de Menescal, 82290 MONTBETON (FR). **PILOTO FONSECA, Carlos David** ; 15 rue Jules Michelet, 82000 MONTAUBAN (FR).

(74) Mandataire : **AUGARDE, Eric** ; BREVALEX, 56 boulevard de l'Embouchure, B.P. 27519, 31075 TOULOUSE Cedex 2 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,

(54) Title: HARDWARE AUTHENTICATION TOKEN WITH REMOTE VALIDATION

(54) Titre : JETON MATÉRIEL D'AUTHENTIFICATION À VALIDATION DÉPORTÉE

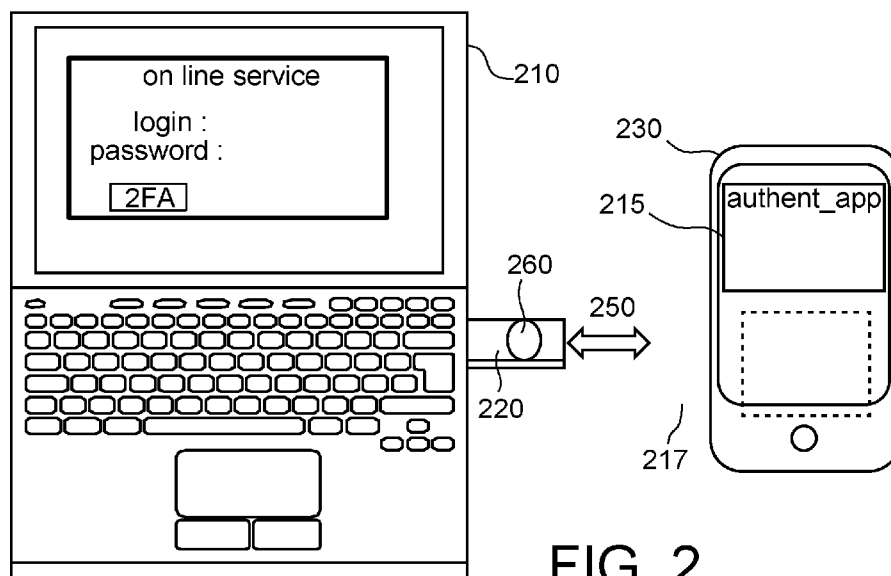


FIG. 2

(57) Abstract: The present invention relates to a hardware authentication token intended for being connected to a computer terminal. This token comprises a confirmation button, a processor and a secure memory area where a first private key is stored. The terminal can ask the user to authenticate using the token by transmitting a first nonce to the user. After the confirmation button has been pressed, the token generates a second nonce, encodes it using ultrasonic signals and transmits it, via an acoustic channel, to the user's smartphone. The token determines from the response whether the second nonce has been signed with a second private key belonging to the user and, if so, returns the first nonce encrypted by the first private key to the computer terminal in order to authenticate the user.

[Suite sur la page suivante]

SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) États désignés (*sauf indication contraire, pour tout titre de protection régionale disponible*) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Publiée:

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

(57) Abrégé : La présente invention concerne un jeton matériel d'authentification destiné à être connecté à un terminal informatique. Ce jeton comprend un bouton de confirmation, un processeur et une zone mémoire sécurisée dans laquelle est stockée une première clé privée. Le terminal peut demander à l'utilisateur de s'authentifier au moyen du jeton en transmettant à celui-ci un premier nonce. Suite à l'actionnement du bouton de confirmation, le jeton génère un second nonce, le code au moyen de signaux ultrasonores et le transmet, via un canal acoustique, au smartphone de l'utilisateur. Le jeton détermine à partir de la réponse si le second nonce a bien été signé par une seconde clé privée appartenant à l'utilisateur et, dans l'affirmative, renvoie au terminal informatique le premier nonce chiffré par la première clé privée afin d'authentifier l'utilisateur.

JETON MATÉRIEL D'AUTHENTIFICATION À VALIDATION DÉPORTÉE

DESCRIPTION

5 **DOMAINE TECHNIQUE**

La présente invention concerne le domaine général des dispositifs matériels d'authentification et plus particulièrement les jetons matériels mettant en œuvre le protocole FIDO 2 (*Fast IDentity Online*).

10 **ÉTAT DE LA TECHNIQUE ANTÉRIEURE**

De manière classique, la sécurisation de l'accès à un service en ligne ou un site web via un terminal informatique est réalisée au moyen d'un identifiant et d'un mot de passe renseignés par l'utilisateur. Toutefois, cette sécurisation d'accès est relativement sommaire en raison de la facilité avec laquelle ces informations peuvent être dérobées, notamment par des techniques d'hameçonnage (*phishing*). Différentes techniques ont été proposées pour renforcer la sécurité de l'accès à de tels services, notamment l'authentification hors bande et l'authentification à deux facteurs.

L'authentification hors bande (OOB) est un type d'authentification forte qui a recours à un canal de communication différent de celui utilisé pour l'accès afin de fournir un second moyen d'authentification. Les canaux de communication hors bande peuvent être par exemple des connexions par e-mail, sms, etc. pour transmettre des codes secrets à usage unique.

L'authentification à deux facteurs (2FA) ou de manière plus générale multi-facteur (MFA) repose sur l'utilisation de plusieurs technologies différentes telles que les mots de passe à usage unique (OTP) ou une infrastructure PKI (*Public Key Infrastructure*).

Le protocole FIDO (*Fast IDentity Online*) normalisé dans le cadre de la FIDO Alliance utilise une infrastructure PKI comme second facteur d'authentification. Plus précisément, selon le protocole FIDO, l'utilisateur crée un couple de clés constitué d'une clé privée et d'une clé publique. La clé publique est transmise au service en ligne et

associée au compte de l'utilisateur. La clé privée reste stockée dans le dispositif d'authentification de l'utilisateur (le terminal informatique lui-même ou bien par exemple une clé USB connectée à ce dernier).

Lorsque l'utilisateur souhaite se connecter au service en ligne, il s'identifie d'abord auprès de lui au moyen de son identifiant. L'utilisateur reçoit alors un nonce (ou défi) qu'il signe avec sa clé secrète et renvoie au service en ligne le nonce ainsi signé. Le service en ligne peut alors vérifier à l'aide de la clé publique de l'utilisateur si le nonce a bien été signé par la clé privée de ce dernier.

Une nouvelle version du protocole FIDO a été reprise dans les spécifications du W3C's Web Authentication (WebAuthn). Ces spécifications prévoient notamment un mode FIDO U2F (*Universal Second Factor*) faisant appel à un jeton matériel pour stocker le couple clé privée - clé publique de l'utilisateur comme décrit en Fig. 1.

On suppose que l'utilisateur s'est préalablement enregistré au moyen de son terminal auprès du service en ligne au moyen d'un identifiant et s'est authentifié au moyen d'un mot de passe (1^{er} facteur d'authentification). Il a également indiqué au service en question qu'il souhaitait activer l'option d'authentification FIDO U2F et lui a transmis en conséquence une clé publique générée pour le service en question.

Le couple de clé privée - clé publique de l'utilisateur est généré et stocké dans un jeton matériel, ici une clé USB, 130.

Lorsque l'utilisateur souhaite accéder au service en ligne, il renseigne d'abord son identifiant et son mot de passe sur la page web correspondante, 120. Le service en ligne l'invite également à s'authentifier au moyen de son second facteur d'authentification (2FA) en lui transmettant un nonce. L'utilisateur insère alors la clé USB dans un port USB de son ordinateur puis appuie sur un bouton de validation, 140, de la clé USB pour signer le nonce en question au moyen de sa clé privée. Le nonce ainsi signé est transmis, via le port USB et le navigateur, au service en ligne qui peut alors vérifier, à l'aide de la clé publique de l'utilisateur, si ce dernier l'a effectivement signé avec sa clé privée.

Il convient de noter que le protocole FIDO U2F autorise d'autres types de jetons qu'une simple clé USB, en particulier des jetons matériels dotés d'une interface BLE (*Bluetooth Low Energy*) ou NFC (*Near Field Communication*).

5 Le protocole FIDO U2F associé à un jeton matériel d'authentification offre une très bonne résistance aux attaques de type hameçonnage. Des clés USB conformes à ce protocole (FIDO U2F *compliant*) sont en outre d'ores et déjà disponibles dans le commerce (Feitian ou YubiKey par exemple).

10 Le protocole FIDO a évolué pour permettre de s'authentifier au moyen d'un simple jeton matériel, sans avoir à fournir un mot de passe (*passwordless*). Dans cette nouvelle version du protocole FIDO, le jeton d'authentification contient non seulement le couple clé privée – clé publique comme précédemment décrit mais également un code PIN de l'utilisateur.

L'utilisateur se rend, au moyen du navigateur, sur le site auquel il souhaite accéder et choisit l'option d'authentification par jeton d'authentification. Le navigateur
15 invite alors l'utilisateur à renseigner son code PIN, celui-ci est transmis au jeton d'authentification avec le nonce préalablement généré par le service en ligne. Si le code PIN correspond à celui stocké dans le jeton, ce dernier fournit l'identifiant de l'utilisateur pour le site en question et signe le nonce avec la clé privée, lorsque l'utilisateur presse le bouton de validation du jeton. Le navigateur transmet alors au service en ligne
20 l'identifiant de l'utilisateur ainsi que le nonce ainsi signé. Le service en ligne donne l'accès à l'utilisateur, après avoir vérifié, au moyen de la clé publique de l'utilisateur, que le nonce a bien été signé avec sa clé privée.

Ce nouveau protocole d'authentification est dénommé FIDO CTAP 2, l'acronyme CTAP signifiant *Client To Authenticator Protocol*.

25 Le protocole antérieur, utilisant le jeton comme second facteur d'authentification (et non comme identifiant), FIDO U2F, a été renommé FIDO CTAP 1 pour se différencier de la nouvelle version du protocole.

Les deux versions du protocole FIDO CTAP 1 et FIDO CTAP 2 sont désormais regroupées au sein d'une même norme, dénommée FIDO 2 (ou W3C WebAuthn). On

pourra trouver les spécification du protocole FIDO2 à l'URL <https://fidoalliance.org/specifications/download/> .

Un jeton matériel conforme au protocole FIDO 2 permet de se connecter de manière sécurisée à partir de n'importe quel terminal possédant un port USB (voire une interface BLE ou NFC). En contrepartie, un utilisateur ayant oublié de retirer sa clé USB pourra être piraté, ceci est particulièrement vrai dans le cas du protocole FIDO CTAP 2 dans la mesure où le jeton contient à la fois l'identifiant et la clé privée : il suffit alors de connaître le code PIN pour avoir accès au service en ligne. Pour réduire ce risque, il est possible de prévoir sur la clé USB elle-même un capteur biométrique tel qu'un capteur d'empreintes digitales. Néanmoins, l'ajout d'un capteur biométrique sur le jeton matériel le rend sensiblement plus complexe et coûteux.

Un but de la présente invention est par conséquent de proposer un jeton matériel d'authentification simple et robuste, qui permette de s'authentifier sur n'importe quel terminal muni d'un port USB (voire d'une interface BLE ou NFC) sans pour autant présenter les risques de sécurité de l'état de la technique.

EXPOSÉ DE L'INVENTION

La présente invention est définie par un jeton matériel d'authentification destiné à être connecté à un terminal informatique au moyen d'une connexion USB, BLE ou NFC, ledit jeton matériel comportant un processeur et une zone mémoire sécurisée, le processeur étant adapté à générer un couple constitué d'une première clé privée et d'une première clé publique d'un premier cryptosystème asymétrique, la première clé privée étant stockée dans la zone mémoire sécurisée, ledit jeton étant original en ce qu'il comprend en outre :

- un codeur/ décodeur acoustique utilisant un dictionnaire de codage S dont les mots de code sont stockés dans la zone mémoire sécurisée, lesdits mots de code représentant des signaux ultrasonores aléatoires ou pseudo-aléatoires ;
- au moins un transducteur permettant au jeton matériel d'établir un canal acoustique en émission et en réception avec un smartphone de l'utilisateur ;

- ledit jeton matériel d'authentification étant configuré pour recevoir un premier nonce dudit terminal via ladite connexion et, sur réception du premier nonce, à transmettre un second nonce, codé à l'aide du dictionnaire S , au smartphone de l'utilisateur, via le canal acoustique, ledit jeton matériel d'authentification étant en outre configuré pour recevoir, via le canal acoustique une réponse du smartphone ;

- le processeur étant adapté à déterminer, à partir de ladite réponse du smartphone si le second nonce a bien été signé par une seconde clé privée appartenant à l'utilisateur et dans l'affirmative à chiffrer le premier nonce au moyen de la première clé privée ;

- ledit jeton matériel d'authentification étant configuré pour retourner au terminal via ladite connexion le premier nonce ainsi chiffré afin d'authentifier l'utilisateur.

Typiquement, le jeton se présente sous la forme d'une clé USB. Il peut comprendre en outre un bouton de confirmation, le jeton ne générant et ne transmettant alors de second nonce qu'après avoir reçu le premier nonce et qu'après que le bouton de confirmation a été actionné.

Il peut en outre comprendre un indicateur lumineux indiquant à l'utilisateur de confirmer la génération et la transmission du second nonce au smartphone, lorsque le premier nonce a été reçu du terminal.

Avantageusement, il comprend également un haut-parleur et un microphone intégré pour émettre et recevoir lesdits signaux ultrasonores via le canal acoustique.

La présente invention concerne également une méthode d'authentification d'un utilisateur au moyen d'un jeton matériel d'authentification tel que défini ci-dessus, d'un terminal informatique et d'un smartphone, ladite méthode étant originale en ce qu'elle comprend :

a) une étape de transmission par le terminal informatique au jeton matériel d'authentification, d'une requête d'authentification comprenant le premier nonce;

b) un stockage temporaire du premier nonce dans une zone mémoire dudit jeton matériel d'authentification ;

c) une étape de génération du second nonce sur réception du premier nonce par ledit jeton matériel d'authentification, le second nonce étant codé sous la forme d'un premier signal ultrasonore au moyen du dictionnaire de codage S ;

5 d) une étape de transmission du premier signal ultrasonore par le jeton d'authentification matériel au smartphone de l'utilisateur, via le canal acoustique, le premier signal ultrasonore étant décodé pour fournir le second nonce ;

e) une étape de signature du second nonce au moyen de la seconde clé privée, par une application d'authentification préalablement ouverte sur le smartphone de l'utilisateur, la signature du second nonce étant codée sous la forme d'un second
10 signal ultrasonore au moyen d'un second dictionnaire de codage S' ;

f) une étape de transmission du second signal ultrasonore par le smartphone au jeton matériel d'authentification, via le canal acoustique, le second signal ultrasonore étant décodé pour fournir la signature du second nonce ;

g) une étape de vérification, par le processeur, de la signature du second
15 nonce au moyen de la seconde clé publique ; et dans le cas d'une vérification positive :

h) une étape de signature, par le processeur, du premier nonce au moyen de la première clé privée, la signature du premier nonce étant transmise sous forme de réponse au terminal pour authentifier l'utilisateur.

Lorsque le jeton est doté d'un bouton de confirmation, l'utilisateur peut
20 actionner ce bouton entre les étapes (b) et (c) pour déclencher la génération du second nonce et la transmission du premier signal ultrasonore au smartphone.

De même, lorsque le jeton est doté d'un indicateur lumineux, celui-ci indique à l'utilisateur la réception d'une requête d'authentification à l'étape (b).

Typiquement, avant l'étape (a), l'utilisateur procède à son enregistrement auprès
25 d'un serveur d'accès à l'aide d'un identifiant, la phase d'enregistrement (A) comprenant en outre la génération du couple constitué par la première clé privée et la première clé publique par le jeton matériel d'authentification, l'enregistrement de ladite première clé publique auprès du serveur, en relation avec l'identifiant de l'utilisateur et le stockage de la première clé privée dans la zone mémoire sécurisée dudit jeton.

De même, préalablement à l'étape (a), l'utilisateur procède à l'association du jeton matériel d'authentification avec le smartphone, la phase d'association (B) comprenant en outre la génération du couple constitué par la seconde clé privée et la seconde clé publique par une application d'authentification du smartphone, la seconde
5 clé publique étant transmise via le canal acoustique au jeton pour y être stockée dans une zone mémoire, la seconde clé privée étant stockée dans une zone mémoire sécurisée de la carte SIM du smartphone.

Avantageusement, postérieurement à l'étape (h), le terminal entre dans une boucle de test en transmettant à chaque itération de ladit boucle un premier nonce de
10 test au jeton matériel d'authentification, et que celui-ci génère automatiquement un second nonce de test pour l'itération courante, le code au moyen du dictionnaire de codage S sous forme d'un troisième signal ultrasonore, puis transmet celui-ci via le canal acoustique au smartphone de l'utilisateur, le smartphone de l'utilisateur décodant le troisième signal ultrasonore et signant automatiquement le second nonce de test à l'aide
15 de la seconde clé privée, codant la signature ainsi obtenue au moyen du second dictionnaire de codage S' pour générer un quatrième signal ultrasonore qui est transmis, via le canal acoustique, au jeton matériel d'authentification, ledit jeton vérifiant à l'aide de la seconde clé publique si le second nonce de test a bien été signé au moyen de la seconde clé privée et, dans l'affirmative, signant le premier nonce de test au moyen de la
20 première clé privée et transmettant au terminal la signature ainsi obtenue.

Dans ce cas, le terminal peut vérifier que le premier nonce de test a bien été signé au moyen de la première clé privée et, dans l'affirmative, génère un nouveau premier nonce de test à l'itération suivante, et, dans la négative, en avertit le serveur d'accès.

BRÈVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture d'un mode de réalisation préférentiel de l'invention, décrit en référence aux figures
30 jointes parmi lesquelles :

La Fig. 1, déjà décrite, illustre de manière schématique un terminal informatique auquel est connecté un jeton matériel d'authentification conforme au protocole FIDO 2, connu de l'état de la technique ;

La Fig. 2 représente de manière schématique un terminal informatique auquel
5 est connecté un jeton matériel d'authentification selon un mode de réalisation de l'invention, en communication avec le smartphone d'un utilisateur ;

La Fig. 3 représente de manière schématique l'architecture d'un jeton matériel d'authentification selon un mode de réalisation de l'invention.

La Fig. 4 représente de manière schématique les échanges entre le terminal, le
10 jeton matériel d'authentification et le smartphone de la Fig. 2 lors d'une procédure d'authentification de l'utilisateur.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

Nous considérerons dans la suite un jeton matériel d'authentification conforme
15 au protocole FIDO 2. En d'autres termes, ce jeton matériel permet à son possesseur de prouver son identité au moyen d'un facteur d'authentification (premier, second ou multiple). Ce jeton matériel comporte une interface lui permettant d'être connecté à un terminal informatique (ordinateur personnel, laptop, phablette, etc.) au moyen d'une connexion USB, BLE ou NFC.

20 Selon une version préférée de réalisation, le jeton matériel d'authentification se présentera sous la forme d'une clé USB présentant des caractéristiques spécifiques, comme décrit plus loin.

L'idée à la base de l'invention est de déporter vers un smartphone le bouton de validation du jeton matériel d'authentification. Ce transfert est rendu possible grâce à un
25 canal acoustique établi entre le jeton matériel d'authentification et le smartphone, la transmission sur ce canal utilisant un codage d'information au moyen d'un dictionnaire dont les mots de code sont des signaux aléatoires ou pseudo-aléatoires.

Comme détaillé plus loin, la procédure d'authentification requiert d'être en possession à la fois du jeton matériel d'authentification et du smartphone de l'utilisateur
30 (en sus de la connaissance du couple login/mot de passe dans FIDO CTAP 1 ou du code

PIN dans FIDO CTAP 2). La probabilité que cet utilisateur oublie son smartphone et laisse le jeton matériel d'authentification connecté au terminal est particulièrement faible. Le risque de piratage est donc particulièrement réduit, *a fortiori* lorsque le smartphone est verrouillé par un capteur biométrique ou un code PIN.

5

Plus précisément, la Fig. 2 représente un cas d'usage du jeton matériel d'authentification selon un mode de réalisation de l'invention.

Le cas d'usage illustré est ici celui d'un utilisateur souhaitant se connecter à un service en ligne à l'aide de son ordinateur personnel, 210. Bien entendu, d'autres cas d'usage pourront être envisagés par l'homme du métier sans sortir du cadre de la présente invention. En particulier, l'utilisateur pourra s'authentifier au moyen de son jeton matériel d'authentification auprès d'une borne d'accès.

Après avoir renseigné de manière classique sur la page web du service en ligne en question son identifiant et son mot de passe (ou son code PIN dans le protocole FIDO CTAP 2), l'utilisateur se voit invité à fournir un (premier ou second) facteur d'authentification au moyen d'un jeton matériel. Cela suppose que, par exemple, lors de la création de son compte auprès (*enrolment*) ou de l'enregistrement de son profil, l'utilisateur ait préalablement sélectionné une option d'authentification par jeton matériel et enregistré auprès du site web une clé publique permettant cette authentification. Plus précisément, l'utilisateur génère pour ce faire un couple de clés d'un cryptosystème de chiffrement asymétrique (autrement d'une infrastructure PKI) constitué d'une première clé privée et d'une première clé publique. Par exemple, ce cryptosystème pourra être celui d'un chiffrement sur courbes elliptiques (ECC) connu en soi. En tout état de cause, seule cette première clé publique sera fournie au serveur du service en ligne et stockée avec le profil de l'utilisateur.

Si l'utilisateur a sélectionné l'option d'authentification au moyen d'un jeton matériel, il peut être invité par le site en ligne à présenter son jeton matériel d'authentification.

L'utilisateur connecte alors son jeton d'authentification 220, en l'enfichant dans un port USB du terminal informatique (en activant la liaison Bluetooth si le jeton possède

30

une interface BLE, en approchant jeton du lecteur NFC si le jeton possède une interface NFC).

Le jeton d'authentification comprend en outre un processeur (DSP), 310 ainsi qu'une zone mémoire sécurisée, 320, comme illustré en Fig. 3.

5 De manière originale, le jeton matériel d'authentification 220 comprend un codeur/décodeur acoustique 330 utilisant un dictionnaire de codage (*codebook*) S constitué de mots de code représentant des signaux ultrasonores aléatoires ou pseudo-aléatoires comme décrit dans la demande publiée sous le numéro FR-A-3052614. Selon une variante un premier dictionnaire de codage S est utilisé pour l'émission et un second
10 dictionnaire de codage S' est utilisé en réception par le jeton.

Le codeur/ décodeur acoustique est avantageusement implémenté par des moyens logiciels dans le DSP. Alternativement, ils peuvent être implémentés par un circuit distinct, 330, de ce dernier.

Dans tous les cas, les mots de code du dictionnaire (voire des dictionnaires) de
15 codage sont stockés dans la zone mémoire sécurisée, 320, par exemple la mémoire du processeur lui-même lorsque le codage/décodage acoustique est réalisé par le DSP. Cette zone mémoire sécurisée contient également la première clé privée précitée.

Enfin, le jeton matériel d'authentification comporte au moins un transducteur permettant d'établir un canal acoustique en émission et en réception avec un
20 smartphone de l'utilisateur, 230. Un seul transducteur peut suffire dès lors que les mots de codes utilisés par le jeton matériel d'authentification (mots de code du dictionnaire S) et ceux utilisés par le smartphone (mots de code du dictionnaire S') pour transmettre sur le canal acoustique sont faiblement corrélés et autorisent par conséquent une utilisation du canal en mode *full duplex*. Le transducteur pourra par exemple être de type
25 piézoélectrique. Alternativement, comme représenté en Fig. 3, on pourra prévoir un haut-parleur 340 et un microphone 350 intégrés pour respectivement émettre et recevoir sur le canal acoustique.

Une fois le jeton matériel d'authentification 220 connecté, celui-ci reçoit du
30 terminal 210 un premier nonce généré par le serveur d'accès du service en ligne. Dans le

protocole FIDO CTAP 1, le premier nonce peut être par exemple calculé comme le hash du numéro de compte de l'utilisateur concaténé avec une information temporelle.

Sur réception de ce premier nonce, le jeton génère un second nonce et le code au moyen du dictionnaire de codage S . La génération du second nonce pourra être automatique, dès réception du premier nonce. De préférence, toutefois, le second nonce ne sera généré qu'après appui sur un bouton de confirmation, 260. La réception du premier nonce par le jeton matériel d'authentification pourra être signalé à l'utilisateur par un signal lumineux clignotant, par exemple par un anneau lumineux clignotant produit par une couronne de LED, entourant le bouton de confirmation.

Le second nonce pourra être identique au premier nonce. Selon une variante préférée, le second nonce résultera de la concaténation du premier nonce avec un numéro de série du jeton matériel en question. En tout état de cause, le second nonce ainsi codé se présente sous la forme d'un signal ultrasonore qui est transmis au smartphone, 230, de l'utilisateur via le canal acoustique, 250. Le smartphone décode le signal ultrasonore à l'aide du dictionnaire de codage S et récupère ainsi le second nonce.

L'utilisateur peut alors s'authentifier en signant, au moyen de son smartphone, 230, le second nonce au moyen d'une seconde clé privée. A cette fin, l'utilisateur aura préalablement téléchargé une application d'authentification, 215 sur son smartphone. La signature au moyen du smartphone pourra par exemple être déclenchée par la pression sur un bouton (tactile) de validation, la réalisation d'un mouvement particulier, après que l'application d'authentification aura invité l'utilisateur (propriétaire du smartphone) à valider son authentification.

Cette application d'authentification a accès à un second cryptosystème de chiffrement asymétrique, constitué d'une seconde clé privée et d'une seconde clé publique, la seconde clé privée étant conservée dans une zone mémoire sécurisée du smartphone, par exemple dans une zone sécurisée ou TEE (*Trusted Execution Environment*) de la carte SIM du smartphone. Il est essentiel de noter que la seconde clé privée est propre à l'utilisateur.

On suppose que la seconde clé publique a été fournie par le smartphone au jeton matériel d'authentification, par exemple lors d'une procédure préalable d'association comme décrit plus loin.

La signature du second nonce est codée au moyen d'un dictionnaire de codage S' pouvant être identique au dictionnaire S et le signal ultrasonore résultant est transmis au jeton matériel d'authentification via le canal acoustique.

Le signal ultrasonore reçu par le transducteur (ou le microphone intégré 350) du jeton est décodé par le décodeur acoustique (au moyen du dictionnaire S' également stocké dans ladite zone mémoire sécurisée du jeton) pour récupérer la signature. Le processeur détermine alors au moyen de la seconde clé publique si le second nonce a bien été signé par la seconde clé privée. Dans l'affirmative, il signe à son tour le premier nonce au moyen de la première clé privée et transmet cette signature au terminal. Lorsqu'elle existe la couronne de LED autour du bouton de confirmation 260 peut alors passer à un état lumineux permanent pour confirmer à l'utilisateur que la signature du second nonce est bien valide.

Le terminal renvoie enfin la signature du premier nonce (encore appelée assertion) au serveur d'accès du service en ligne et ce dernier vérifie que le premier nonce a bien été signé par la première clé privée.

On notera que la première clé privée est propre au jeton matériel d'authentification et n'est pas propre à l'utilisateur. En d'autres termes, la perte du jeton d'authentification sera sans conséquence sur la sécurité d'accès au service en ligne. Seule la possession conjointe du jeton matériel d'authentification et du smartphone permet d'accéder au service en question. Et encore faudrait-il en outre que le pirate ait pu aussi se procurer l'identifiant et le mot de passe de l'utilisateur pour franchir la première étape d'identification (la connaissance du code PIN étant suffisante dans le cas du protocole FIDO CTAP 2).

L'utilisation d'un canal acoustique entre le jeton matériel de chiffrement et le smartphone réduit considérablement les risques d'interception et d'attaques de type *man-in-the-middle* en raison de la faible portée des signaux ultrasonores. En outre, la

transmission sur ce canal au moyen de signaux acoustiques aléatoires ou pseudo-aléatoires renforce considérablement la robustesse du canal à de telles attaques.

La Fig. 4 représente de manière schématique les échanges entre le terminal, le jeton matériel d'authentification et le smartphone de la Fig. 2 lors d'une procédure d'authentification de l'utilisateur.

La procédure d'authentification (C) suppose que la première clé publique du jeton ait été préalablement enregistrée auprès du serveur d'accès en relation avec le compte de l'utilisateur (procédure d'enregistrement A) et que la seconde clé publique de l'utilisateur ait été préalablement enregistrée dans le jeton matériel d'authentification (procédure d'association B).

On a respectivement représenté par les lignes verticales 410, 420, 430 et 440 le serveur du service en ligne, le terminal informatique, le jeton matériel d'authentification et le smartphone de l'utilisateur.

Dans la procédure d'enregistrement (A), lorsque l'utilisateur crée son compte auprès du serveur d'accès, celui-ci l'invite en 451 à lui fournir en 452 un identifiant et un mot de passe.

Si l'utilisateur a sélectionné l'option d'une authentification par un jeton matériel (FIDO 2 authenticator) pour accéder à son compte, il est invité en 453 à connecter le jeton matériel d'authentification au terminal. En 454, le terminal demande au jeton de générer un couple d'un cryptosystème asymétrique constitué d'une première clé privée et d'une première clé publique. La première clé privée, K_1^{priv} , est stockée dans la zone mémoire protégée du jeton alors que la première clé publique, K_1^{pub} est fournie au terminal en 455, puis transmise au serveur d'accès en 456. Le serveur d'accès associe la première clé publique à l'identifiant et, le cas échéant, au mot de passe de l'utilisateur. Avantageusement, la première clé publique n'est pas fournie automatiquement au terminal sur simple requête mais nécessite un actionnement du bouton, lorsqu'il est présent sur le jeton. De préférence, l'utilisateur devra exercer une pression sur le bouton pendant un temps différent (par exemple sensiblement plus long) que lorsqu'il confirme le transfert du second nonce au smartphone.

Dans la procédure d'association (B), le jeton d'authentification est connecté au terminal informatique. A partir d'une fenêtre de contrôle ou bien, si le jeton est doté d'un bouton, en appuyant par exemple pendant un temps long sur celui-ci, le jeton génère en
5 461 une requête sur le canal acoustique. L'application d'authentification du smartphone ayant été ouverte, celle-ci génère sur réception du signal de requête un couple d'un cryptosystème asymétrique constitué d'une seconde clé privée, K_2^{priv} , et d'une seconde clé publique, K_2^{pub} . La seconde clé privée est stockée par exemple dans une zone sécurisée (TEE) de la carte SIM alors que la seconde clé publique, K_2^{pub} , est transmise en
10 462 au jeton via le canal acoustique. Cette seconde clé publique est stockée dans une zone mémoire du jeton (pas nécessairement la zone sécurisée). Si le jeton est mono-utilisateur seule la seconde clé publique est stockée. En revanche, si le jeton d'authentification peut être partagé entre plusieurs utilisateurs, un identifiant de l'utilisateur du smartphone peut être stocké en association avec la seconde clé publique
15 correspondante dans la zone mémoire. Là encore, l'opération de stockage de la seconde clé publique peut ne pas être automatique mais nécessiter d'actionner le bouton (optionnel) du jeton.

Enfin dans la procédure d'authentification proprement dite (C), l'utilisateur est
20 invité dans un premier temps en 471 à s'identifier.

En réponse, l'utilisateur renseigne (dans le cadre du protocole FIDO CTAP 1) son identifiant (login) et son mot de passe dans la fenêtre de saisie du navigateur et ce dernier les transmet en 472 au serveur d'accès. Après avoir reçu ces informations, le serveur d'accès invite en 473 l'utilisateur à fournir son (premier, second, nième) facteur
25 d'authentification en connectant son jeton matériel d'authentification au terminal.

Le serveur d'accès transmet alors un premier nonce, $Nonce_1$ en 474 au terminal. Comme précédemment indiqué, ce nonce peut résulter de la concaténation du numéro de compte de l'utilisateur avec une information temporelle de sorte à éviter les attaques par replay. Le terminal le fait suivre en 475 au jeton matériel d'authentification.

Dans le cas d'un protocole FIDO CTAP 2, on rappelle que l'utilisateur renseigne seulement son code PIN dans la fenêtre du navigateur et que le premier nonce est transmis avec le code PIN au jeton matériel d'authentification.

A ce stade, deux variantes sont possibles. Selon une première variante non illustrée, le jeton génère automatiquement en 476 un second nonce, $Nonce_2$, et le transmet en 477 au smartphone après l'avoir codé au moyen du dictionnaire de codage S . Selon une seconde variante, dans laquelle le jeton est doté d'un bouton de confirmation, le jeton attend une pression sur le bouton en pour générer le second nonce en 476.

Le second nonce peut être une copie du premier nonce ou bien résulter de la concaténation de ce dernier avec un numéro de série du jeton.

En tout état de cause, le second nonce est codé au moyen du dictionnaire de codage S et transmis sous la forme d'un signal ultrasonore au smartphone via le canal acoustique. On suppose par ailleurs que l'utilisateur a ouvert l'application d'authentification sur son smartphone (par exemple avant d'avoir appuyé sur le bouton de confirmation du jeton) ou que celle-ci s'est automatiquement lancée à la réception du second nonce. L'application du smartphone décode alors le signal ultrasonore pour récupérer le second nonce et le signe avec sa clé privée, soit $sign(Nonce_2, K_2^{priv})$, puis code cette signature avec son dictionnaire de codage S' .

A l'étape 481, le smartphone transmet, via le canal acoustique, un signal ultrasonore correspondant à la signature $sign(Nonce_2, K_2^{priv})$ ainsi codée. Ce signal est reçu et décodé par le décodeur acoustique (ou le DSP) du jeton.

En 482, le jeton vérifie, à l'aide de la seconde clé publique K_2^{pub} , que la signature est bien valide, autrement dit que le second nonce a bien été signé par la seconde clé privée.

Dans la négative, le jeton peut le signaler au terminal ou simplement de pas répondre au terminal. En cas de réception d'un message d'échec ou à l'issue d'un temps prédéterminé (*timeout*), le terminal indique à l'utilisateur que l'authentification au moyen du jeton a échoué.

Dans l'affirmative, le jeton et, plus précisément son processeur, signe le premier nonce (qui avait été mis en attente dans un buffer) au moyen de la première clé privée K_1^{priv} , soit $sign(Nonce_1, K_1^{priv})$ en 483, puis transmet cette signature au terminal en 484 qui le fait suivre en 485 au serveur d'accès. Ce dernier vérifie en 486, au moyen de la première clé publique K_1^{pub} , que cette signature est bien valide, autrement dit que le premier nonce a bien été signé par la première clé privée K_1^{priv} .

Dans la négative, le serveur informe le terminal de l'échec de l'authentification et invite, le cas échéant, l'utilisateur à réitérer la procédure d'authentification.

Dans l'affirmative, le serveur permet en 487 à l'utilisateur d'accéder au service en question.

Avantageusement, afin de s'assurer que l'utilisateur ne laisse pas sa session ouverte sur le terminal informatique, une procédure d'authentification continue (ou périodique) peut être initiée par le terminal. Cette procédure peut être lancée dès que l'utilisateur a reçu l'autorisation d'accès au service.

Selon cette procédure, le terminal transmet de manière itérative un premier nonce de test, périodiquement ou bien dès qu'un laps de temps prédéterminé s'est écoulé depuis la dernière réception d'une confirmation de présence du smartphone de l'utilisateur. Le premier nonce de test est modifié d'une itération à la suivante de manière à combattre les attaques par rejeu. Par exemple, si l'on note $Nonce_{ck1}^n$ le premier nonce de test qui a été généré par le terminal à l'itération n , le premier nonce de test à l'itération suivante pourra être obtenu par $Nonce_{ck1}^{n+1} = hash(Nonce_{ck1}^n || ctr(n))$ où $ctr(n)$ est la sortie d'un compteur incrémenté à chaque itération et, le cas échéant, initialisé par un nombre aléatoire au début de la session, $||$ désigne une opération de concaténation et $hash$ est une fonction de hachage.

Lors de l'itération n , le premier nonce de test, $Nonce_{ck1}^n$, est transmis au jeton matériel d'authentification. Sur réception de ce nonce, le jeton le stocke en mémoire et génère un second nonce de test, $Nonce_{ck2}^n$. Ce second nonce de test peut être identique au premier ou bien résulter, par exemple, d'une concaténation du premier avec une

information temporelle. Le second nonce de test est ensuite transmis par le jeton d'authentification au smartphone de l'utilisateur, via le canal acoustique, après avoir été codé sous la forme de signaux ultrasonores au moyen du dictionnaire S , comme décrit précédemment.

5 Ces signaux sont décodés par l'application d'authentification du smartphone et le second nonce de test $Nonce_{ck2}^n$ est signé par la clé privée K_2^{priv} stockée dans la zone sécurisée TEE du smartphone. La signature $sign(Nonce_{ck2}^n, K_2^{priv})$ est codé sous forme de signaux ultrasonores au moyen du dictionnaire de codage S' et transmis au jeton matériel d'authentification via le canal acoustique.

10 Le jeton d'authentification, après avoir décodé la signature en question, vérifie au moyen de la second clé publique K_2^{pub} , que le second nonce de test a bien été signé par la clé privée de l'utilisateur. Si c'est bien le cas, il signe à son tour le premier nonce de test au moyen de la première clé privée K_1^{priv} , soit $sign(Nonce_{ck1}^n, K_1^{priv})$ puis transmet cette signature au terminal.

15 Le terminal vérifie que cette signature est bien valide, c'est-à-dire que le premier nonce de test de l'itération n , $Nonce_{ck1}^n$, a bien été signé par la première clé privée, K_1^{priv} . Dans l'affirmative, le terminal passe à l'itération suivante en envoyant un nouveau nonce de test $Nonce_{ck1}^{n+1}$.

20 L'homme du métier comprendra que cette boucle de test permet de s'assurer que le smartphone de l'utilisateur et le jeton d'authentification sont toujours présents. Si une rupture se produit dans la chaîne d'authentification, le premier ou le second nonce de test n'est pas renvoyé dans un délai prédéterminé. Le terminal en avertit alors le serveur d'accès et l'utilisateur est automatiquement déconnecté du service en ligne.

25 Il convient de noter que la procédure d'authentification continue suppose fait abstraction de la confirmation par l'utilisateur. En d'autres termes, l'utilisateur n'a pas à presser le bouton de confirmation à chaque demande d'authentification : la génération du second nonce de test est réalisé de manière automatique. De même, la signature par le smartphone est automatique et ne requiert une action de validation de l'utilisateur à

chaque itération. Ce mode automatique pourra être signalé au moyen d'un préfixe particulier du nonce en question.

La procédure d'authentification continue décrite ci-dessus est initiée et pilotée par le terminal, dans la mesure où il transmet les premiers nonces de test et vérifie les signatures. Toutefois, selon une variante, cette procédure d'authentification peut être effectuée par le serveur d'accès lui-même. Dans ce cas, sur réception d'une réponse erronée ou en l'absence de réponse pendant une durée prédéterminée, le serveur ferme la session.

Enfin, la présente invention a été décrite dans le cadre d'un accès à un service en ligne. L'homme du métier comprendra toutefois qu'elle pourra également trouver à s'appliquer pour permettre l'accès à une session du terminal lui-même, le terminal jouant alors le rôle du serveur d'accès. De manière similaire, dans ce cas là, le terminal pourra aussi procéder à une authentification continue au moyen du jeton matériel d'authentification et fermer la session ouverte sur le terminal en cas de réception d'une réponse erronée ou d'une absence de réponse pendant une durée prédéterminée.

REVENDICATIONS

1. Jeton matériel d'authentification (220) destiné à être connecté à un terminal informatique (210) au moyen d'une connexion USB, BLE ou NFC, ledit jeton matériel comportant un processeur (310) et une zone mémoire sécurisée (320), le processeur étant adapté à générer un couple constitué d'une première clé privée et d'une première clé publique d'un premier cryptosystème asymétrique, la première clé privée étant stockée dans la zone mémoire sécurisée, caractérisé en ce qu'il comprend en outre :
- un codeur/ décodeur acoustique (330) utilisant un dictionnaire de codage S dont les mots de code sont stockés dans la zone mémoire sécurisée, lesdits mots de code représentant des signaux ultrasonores aléatoires ou pseudo-aléatoires ;
 - au moins un transducteur (340, 350) permettant au jeton matériel d'établir un canal acoustique en émission et en réception avec un smartphone de l'utilisateur ;
 - ledit jeton matériel d'authentification étant configuré pour recevoir un premier nonce dudit terminal via ladite connexion et, sur réception du premier nonce, à transmettre un second nonce, codé à l'aide du dictionnaire S , au smartphone de l'utilisateur, via le canal acoustique, ledit jeton matériel d'authentification étant en outre configuré pour recevoir, via le canal acoustique une réponse du smartphone ;
 - le processeur étant adapté à déterminer, à partir de ladite réponse du smartphone si le second nonce a bien été signé par une seconde clé privée appartenant à l'utilisateur et dans l'affirmative à chiffrer le premier nonce au moyen de la première clé privée ;
 - ledit jeton matériel d'authentification étant configuré pour retourner au terminal via ladite connexion le premier nonce ainsi chiffré afin d'authentifier l'utilisateur.

2. Jeton matériel d'authentification selon la revendication 1, caractérisé en ce qu'il se présente sous la forme d'une clé USB.

3. Jeton matériel d'authentification selon la revendication 1 ou 2, caractérisé en ce qu'il comporte en outre un bouton de confirmation, le jeton ne générant et ne transmettant alors de second nonce qu'après avoir reçu le premier nonce et qu'après que le bouton de confirmation a été actionné.

5

4. Jeton matériel d'authentification selon la revendication 3, caractérisé en ce qu'il comprend un indicateur lumineux indiquant à l'utilisateur de confirmer la génération et la transmission du second nonce au smartphone, lorsque le premier nonce a été reçu du terminal.

10

5. Jeton matériel d'authentification selon l'une des revendications précédentes, caractérisé en ce qu'il comprend un haut-parleur et un microphone intégré pour émettre et recevoir lesdits signaux ultrasonores via le canal acoustique.

15

6. Méthode d'authentification d'un utilisateur au moyen d'un jeton matériel d'authentification selon la revendication 1, d'un terminal informatique et d'un smartphone, caractérisée en ce qu'elle comprend :

- i) une étape de transmission par le terminal informatique au jeton matériel d'authentification, d'une requête d'authentification comprenant le premier nonce;
- 20 j) un stockage temporaire du premier nonce dans une zone mémoire dudit jeton matériel d'authentification ;
- k) une étape de génération du second nonce sur réception du premier nonce par ledit jeton matériel d'authentification, le second nonce étant codé sous la forme d'un premier signal ultrasonore au moyen du dictionnaire de codage S ;
- 25 l) une étape de transmission du premier signal ultrasonore par le jeton d'authentification matériel au smartphone de l'utilisateur, via le canal acoustique, le premier signal ultrasonore étant décodé pour fournir le second nonce ;
- m) une étape de signature du second nonce au moyen de la seconde clé privée, par une application d'authentification préalablement ouverte sur le smartphone
- 30 de l'utilisateur, la signature du second nonce étant codée sous la forme d'un second signal ultrasonore au moyen d'un second dictionnaire de codage S' ;

n) une étape de transmission du second signal ultrasonore par le smartphone au jeton matériel d'authentification, via le canal acoustique, le second signal ultrasonore étant décodé pour fournir la signature du second nonce ;

o) une étape de vérification, par le processeur, de la signature du second nonce au moyen de la seconde clé publique ; et dans le cas d'une vérification positive :

p) une étape de signature, par le processeur, du premier nonce au moyen de la première clé privée, la signature du premier nonce étant transmise sous forme de réponse au terminal pour authentifier l'utilisateur.

10 **7.** Méthode d'authentification d'un utilisateur selon la revendication 6, caractérisée en ce que, le jeton étant doté d'un bouton de confirmation, l'utilisateur actionne ce bouton entre les étapes (b) et (c) pour déclencher la génération du second nonce et la transmission du premier signal ultrasonore au smartphone.

15 **8.** Méthode d'authentification d'un utilisateur selon la revendication 7, caractérisée en ce que, le jeton matériel d'authentification étant doté d'un indicateur lumineux, celui-ci indique à l'utilisateur la réception d'une requête d'authentification à l'étape (b).

20 **9.** Méthode d'authentification d'un utilisateur selon l'une des revendications 5 à 7, caractérisée en ce que, préalablement à l'étape (a), l'utilisateur procède à son enregistrement auprès d'un serveur d'accès à l'aide d'un identifiant, la phase d'enregistrement (A) comprenant en outre la génération du couple constitué par la première clé privée et la première clé publique par le jeton matériel d'authentification,
25 l'enregistrement de ladite première clé publique auprès du serveur, en relation avec l'identifiant de l'utilisateur et le stockage de la première clé privée dans la zone mémoire sécurisée dudit jeton.

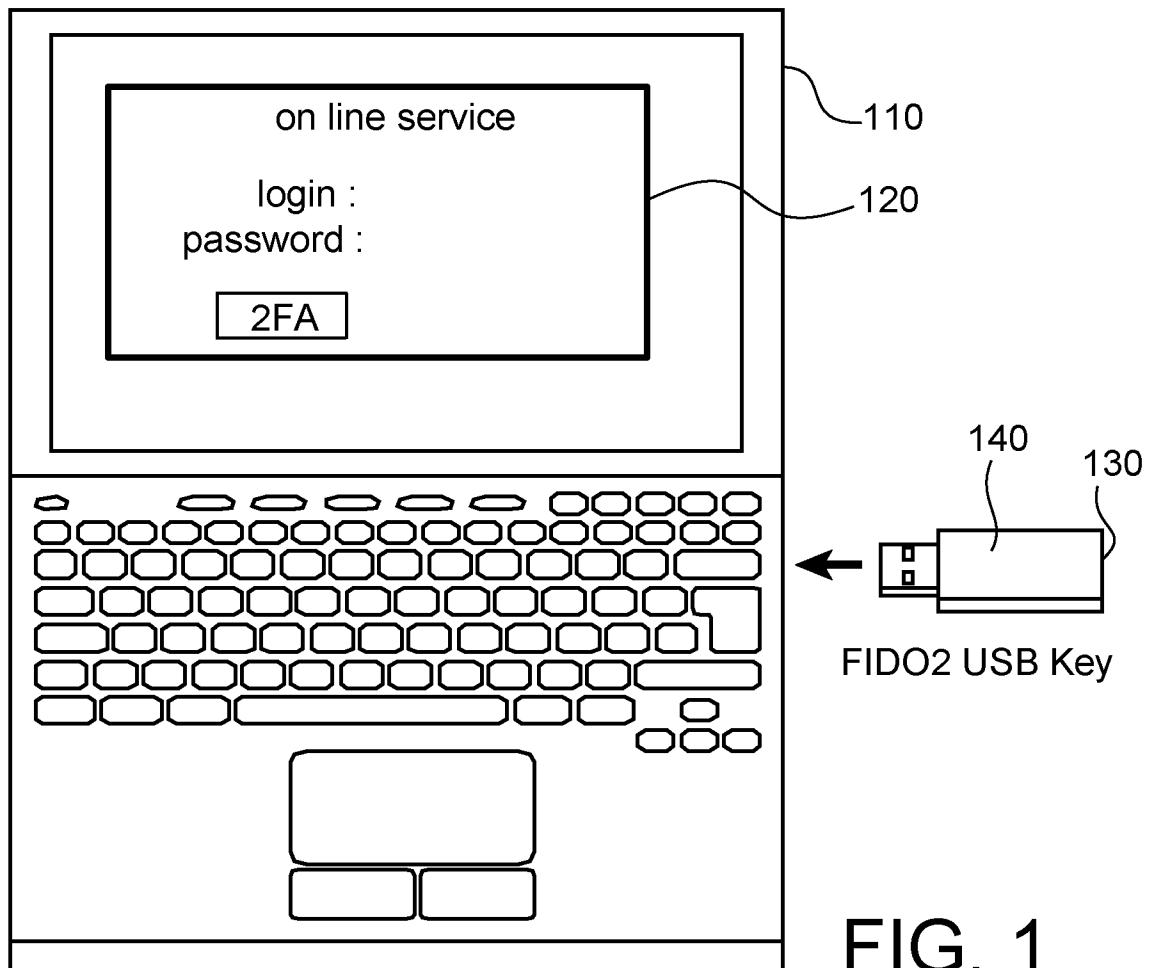
30 **10.** Méthode d'authentification d'un utilisateur selon l'une des revendications 5 à 9, caractérisée en ce que, préalablement à l'étape (a), l'utilisateur procède à l'association du jeton matériel d'authentification avec le smartphone, la phase

d'association (B) comprenant en outre la génération du couple constitué par la seconde clé privée et la seconde clé publique par une application d'authentification du smartphone, la seconde clé publique étant transmise via le canal acoustique au jeton pour y être stockée dans une zone mémoire, la seconde clé privée étant stockée dans une zone mémoire sécurisée de la carte SIM du smartphone.

11. Méthode d'authentification d'un utilisateur selon l'une des revendications 5 à 10, caractérisée en ce que, postérieurement à l'étape (h), le terminal entre dans une boucle de test en transmettant à chaque itération de ladit boucle un premier nonce de test au jeton matériel d'authentification, et que celui-ci génère automatiquement un second nonce de test pour l'itération courante, le code au moyen du dictionnaire de codage S sous forme d'un troisième signal ultrasonore, puis transmet celui-ci via le canal acoustique au smartphone de l'utilisateur, le smartphone de l'utilisateur décodant le troisième signal ultrasonore et signant automatiquement le second nonce de test à l'aide de la seconde clé privée, codant la signature ainsi obtenue au moyen du second dictionnaire de codage S' pour générer un quatrième signal ultrasonore qui est transmis, via le canal acoustique, au jeton matériel d'authentification, ledit jeton vérifiant à l'aide de la seconde clé publique si le second nonce de test a bien été signé au moyen de la seconde clé privée et, dans l'affirmative, signant le premier nonce de test au moyen de la première clé privée et transmettant au terminal la signature ainsi obtenue.

12. Méthode d'authentification d'un utilisateur selon la revendication 11, caractérisée en ce que le terminal vérifie que le premier nonce de test a bien été signé au moyen de la première clé privée et, dans l'affirmative, génère un nouveau premier nonce de test à l'itération suivante, et, dans la négative, en avertit le serveur d'accès.

1 / 3



2 / 3

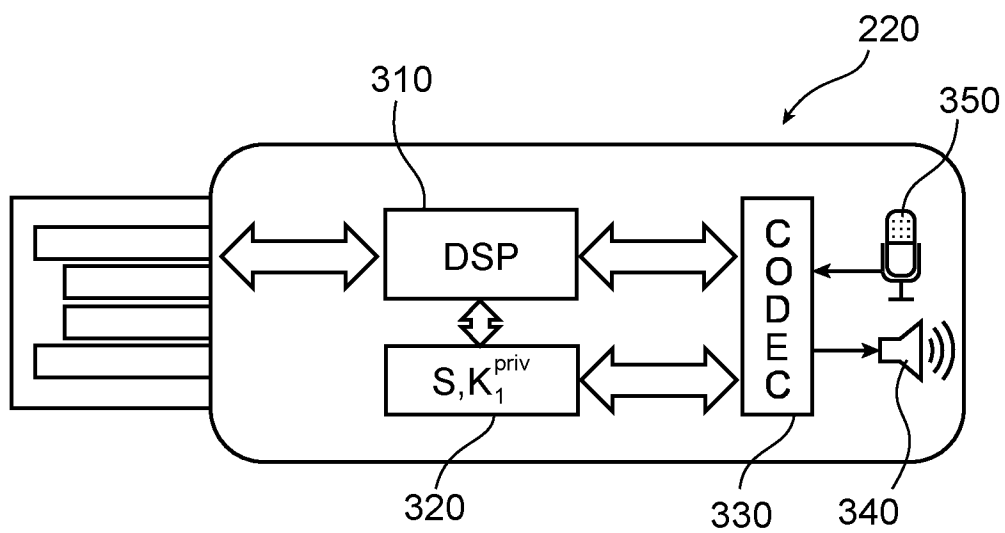
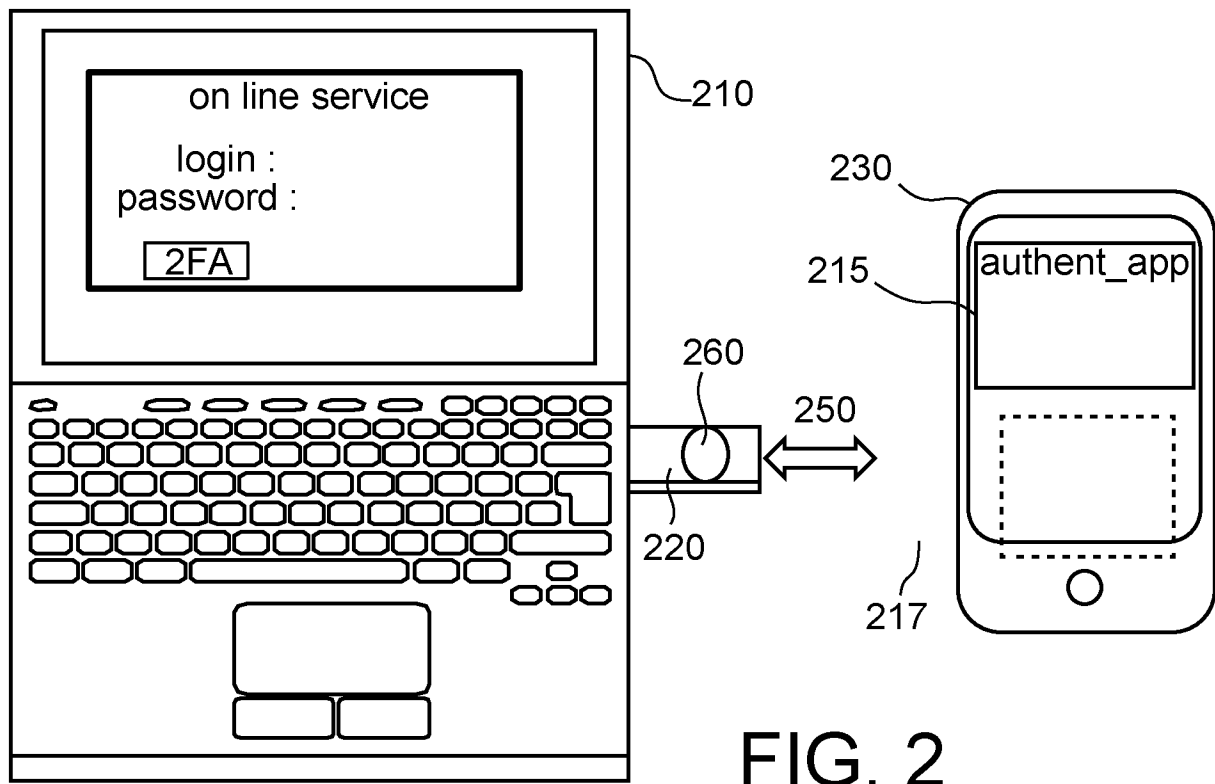


FIG. 3

3 / 3

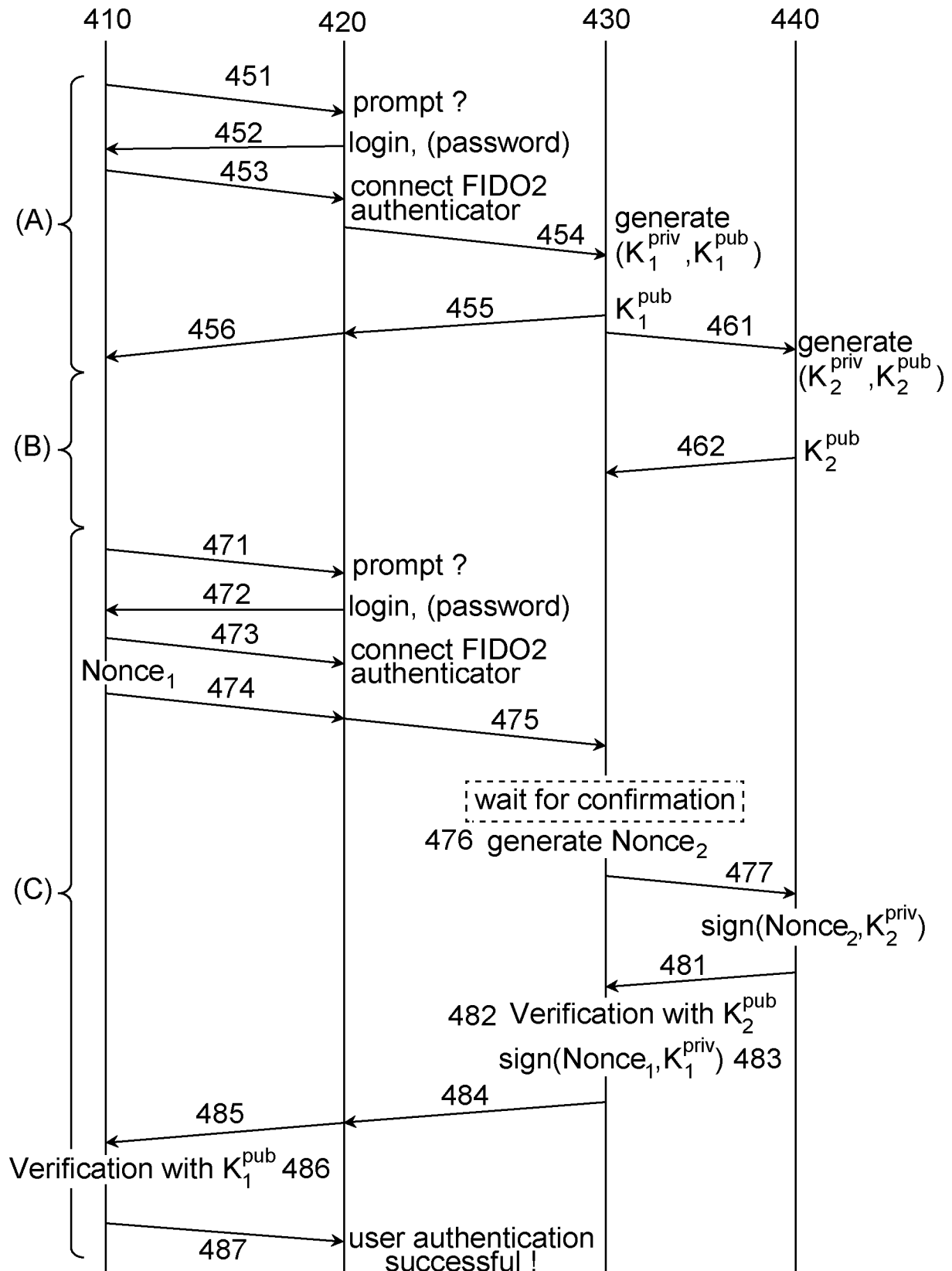


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FR2020/050702**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/34**(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 105657468 B (SHENZHEN NAT ENG LABORATORY OF DIGITAL TELEVISION CO LTD) 12 March 2019 (2019-03-12)	1-3,6,7
A	abstract paragraph [0001] - paragraph [0052]	4,5,8-12
Y	US 2018123799 A1 (HAMID LAURENCE [CA] ET AL) 03 May 2018 (2018-05-03) paragraph [0023] - paragraph [0057] paragraph [0131] - paragraph [0136]	1-3,6,7
A	EP 2940905 A1 (RAKUTEN INC [JP]) 04 November 2015 (2015-11-04) abstract paragraph [0001] - paragraph [0069]	1-12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

“E” earlier application or patent but published on or after the international filing date

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

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

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

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

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

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

“&” document member of the same patent family

Date of the actual completion of the international search

20 July 2020

Date of mailing of the international search report

05 August 2020

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. (+31-70)340-2040

Facsimile No. (+31-70)340-3016

Authorized officer

Ghani, Hamza

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/FR2020/050702

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	105657468	B	12 March 2019	NONE			
US	2018123799	A1	03 May 2018	US	2016148597	A1	26 May 2016
				US	2018123799	A1	03 May 2018
EP	2940905	A1	04 November 2015	CN	104885387	A	02 September 2015
				CN	104919732	A	16 September 2015
				EP	2940905	A1	04 November 2015
				EP	2940906	A1	04 November 2015
				ES	2633457	T3	21 September 2017
				ES	2757876	T3	30 April 2020
				JP	6228539	B2	08 November 2017
				JP	6275040	B2	07 February 2018
				JP	WO2014104284	A1	19 January 2017
				JP	WO2014104285	A1	19 January 2017
				TW	201431306	A	01 August 2014
				US	2015309151	A1	29 October 2015
				US	2015318983	A1	05 November 2015
				WO	2014104284	A1	03 July 2014
				WO	2014104285	A1	03 July 2014

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2020/050702

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/34
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	CN 105 657 468 B (SHENZHEN NAT ENG LABORATORY OF DIGITAL TELEVISION CO LTD) 12 mars 2019 (2019-03-12)	1-3,6,7
A	abrégé alinéa [0001] - alinéa [0052] -----	4,5,8-12
Y	US 2018/123799 A1 (HAMID LAURENCE [CA] ET AL) 3 mai 2018 (2018-05-03) alinéa [0023] - alinéa [0057] alinéa [0131] - alinéa [0136] -----	1-3,6,7
A	EP 2 940 905 A1 (RAKUTEN INC [JP]) 4 novembre 2015 (2015-11-04) abrégé alinéa [0001] - alinéa [0069] -----	1-12



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



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

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

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

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

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

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

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

20 juillet 2020

Date d'expédition du présent rapport de recherche internationale

05/08/2020

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

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

Fonctionnaire autorisé

Ghani, Hamza

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2020/050702

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
CN 105657468	B	12-03-2019	AUCUN	
US 2018123799	A1	03-05-2018	US 2016148597 A1	26-05-2016
			US 2018123799 A1	03-05-2018
EP 2940905	A1	04-11-2015	CN 104885387 A	02-09-2015
			CN 104919732 A	16-09-2015
			EP 2940905 A1	04-11-2015
			EP 2940906 A1	04-11-2015
			ES 2633457 T3	21-09-2017
			ES 2757876 T3	30-04-2020
			JP 6228539 B2	08-11-2017
			JP 6275040 B2	07-02-2018
			JP W02014104284 A1	19-01-2017
			JP W02014104285 A1	19-01-2017
			TW 201431306 A	01-08-2014
			US 2015309151 A1	29-10-2015
			US 2015318983 A1	05-11-2015
			WO 2014104284 A1	03-07-2014
			WO 2014104285 A1	03-07-2014