(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
30 juin 2016 (30.06.2016)

WIPO | PCT

(10) Numéro de publication internationale
WO 2016/102834 A1

(51) Classification internationale des brevets :
G06F 21/32 (2013.01) *G06F 21/83* (2013.01)
H04L 29/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2015/053605

(22) Date de dépôt international :
17 décembre 2015 (17.12.2015)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1463168 22 décembre 2014 (22.12.2014) FR

(71) Déposant : **OBERTHUR TECHNOLOGIES** [FR/FR]; 420 rue d'Estienne d'Orves, 92700 Colombes (FR).

(72) Inventeurs : **DOTTAX, Emmanuelle**; 420 rue d'Estienne d'Orves, 92700 Colombes (FR). **MURESIANU, Philippe**; 420 rue d'Estienne d'Orves, 92700 Colombes (FR). **SARTORI, Michele**; 420 rue d'Estienne d'Orves, 92700 Colombes (FR). **CORDIER, Fabien**; 420 rue d'Estienne d'Orves, 92700 Colombes (FR).

(74) Mandataire : **ORSINI, Fabienne**; Coralis, 14-16 rue Ballu, 75009 Paris (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

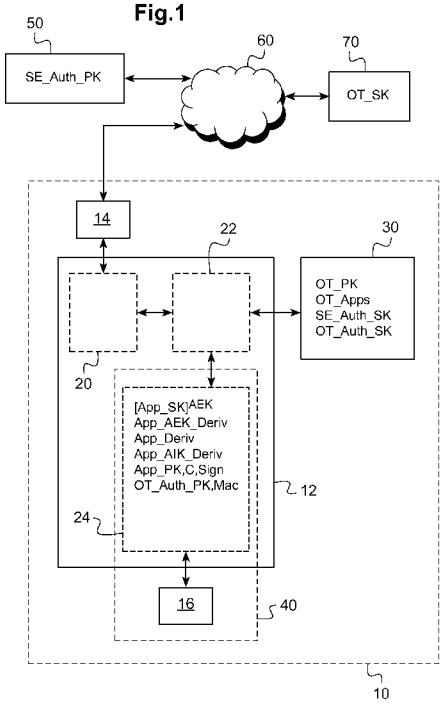
(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, 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).

[Suite sur la page suivante]

(54) **Title** : METHOD FOR AUTHENTICATING A USER AND A SECURE MODULE, ASSOCIATED ELECTRONIC APPARATUS AND SYSTEM

(54) **Titre** : PROCÉDÉ D'AUTHENTIFICATION D'UN UTILISATEUR ET D'UN MODULE SÉCURISÉ, APPAREIL ÉLECTRONIQUE ET SYSTÈME ASSOCIES

Fig.1



(57) Abstract : The invention relates to a method for authenticating a user by means of an electronic apparatus (10) comprising an authentication module (40) and a secure module (30), which comprises the following steps: the authentication module (40) transmits a recognition result to the secure module (30) according to a process that allows the authentication module (40) to be authenticated by the secure module (30); the secure module (30) generates an authentication token by signing, with a private key (SE_Auth_SK) stored in the secure module (30), data comprising data representing at least one feature of the authentication module (40); and transmitting the generated authentication token. The invention also describes an associated secure module, electronic apparatus and system. Figure

(57) Abrégé : L'invention concerne un procédé d'authentification d'un utilisateur à l'aide d'un appareil électronique (10) comprenant un module d'authentification (40) et un module sécurisé (30), comprenant les étapes suivantes : - émission par le module d'authentification (40) d'un résultat de reconnaissance à destination du module sécurisé (30) selon un processus permettant l'authentification du module d'authentification (40) par le module sécurisé (30); - génération d'un jeton d'authentification par le module sécurisé (30) par signature, au moyen d'une clé privée (SE_Auth_SK) mémorisée dans le module sécurisé (30), de données comprenant

[Suite sur la page suivante]

WO 2016/102834 A1

Publiée :

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

des données représentatives d'au moins une caractéristique du module d'authentification (40); - émission du jeton d'authentification généré. Un module sécurisé, un appareil électronique et un système associés sont également décrits.

PROCEDE D'AUTHENTIFICATION D'UN UTILISATEUR ET D'UN MODULE SECURISE, APPAREIL ELECTRONIQUE ET SYSTEME ASSOCIES

DOMAINE TECHNIQUE AUQUEL SE RAPPORTE L'INVENTION

La présente invention concerne l'authentification d'un utilisateur au moyen d'un appareil électronique.

Elle concerne plus particulièrement un procédé d'authentification d'un utilisateur, ainsi qu'un module sécurisé, un appareil électronique et un système associés.

L'invention s'applique particulièrement avantageusement dans le cas où un serveur distant requiert l'authentification de l'utilisateur.

ARRIERE-PLAN TECHNOLOGIQUE

Il est connu d'utiliser un appareil électronique équipé d'un module d'authentification afin d'authentifier un utilisateur de l'appareil électronique auprès d'une entité électronique requérant une telle authentification, par exemple un serveur distant en communication avec une application exécutée sur l'appareil électronique.

Pour ce faire, le module d'authentification effectue une reconnaissance (par exemple biométrique) de l'utilisateur et, lorsque le résultat de la reconnaissance est positif, l'appareil électronique émet un jeton d'authentification à destination de l'entité électronique requérant l'authentification.

OBJET DE L'INVENTION

Dans ce contexte, la présente invention propose un procédé d'authentification d'un utilisateur à l'aide d'un appareil électronique comprenant un module d'authentification et un module sécurisé, comprenant les étapes suivantes :

- émission par le module d'authentification d'un résultat de reconnaissance à destination du module sécurisé selon un processus permettant l'authentification du module d'authentification par le module sécurisé ;

- génération d'un jeton d'authentification par le module sécurisé par signature, au moyen d'une clé privée mémorisée dans le module sécurisé, de données comprenant des données représentatives d'au moins une caractéristique du module d'authentification ;

- émission du jeton d'authentification généré.

Ainsi, le module sécurisé est assuré de la provenance du résultat de reconnaissance et le jeton d'authentification contient des informations relatives au module d'authentification qui a effectivement généré ce résultat de reconnaissance.

On entend par signature des données l'application d'un algorithme cryptographique de signature aux données, utilisant ici la clé privée mémorisée dans le module sécurisé.

La caractéristique du module d'authentification qui fait ainsi partie du jeton d'authentification est par exemple un identifiant du module d'authentification, le type d'authentification mise en œuvre par le module d'authentification, une méthode de protection des clés cryptographiques utilisée par le module d'authentification, ou une méthode de communication utilisée par le module d'authentification.

Le processus permettant l'authentification du module d'authentification par le module sécurisé utilise par exemple une clé privée du module d'authentification.

Selon un mode de réalisation envisageable, le processus permettant l'authentification du module d'authentification par le module sécurisé comprend les étapes suivantes :

- transmission d'un défi du module sécurisé au module d'authentification ;
- génération d'une réponse par le module d'authentification par application au défi d'un algorithme de signature utilisant la clé privée du module d'authentification ;
- transmission de la réponse du module d'authentification au module sécurisé ;
- vérification de la réponse par le module sécurisé au moyen de la clé publique associée à la clé privée du module d'authentification.

En variante, le processus permettant l'authentification du module d'authentification par le module sécurisé pourrait comprendre l'établissement d'un canal sécurisé entre le module d'authentification et l'émission du résultat de reconnaissance du module d'authentification au module sécurisé pourrait alors être réalisée via ce canal sécurisé.

Selon des caractéristiques optionnelles, et donc non limitatives :

- ladite clé publique est reçue par le module sécurisé avec une signature associée et la signature est vérifiée par le module sécurisé au moyen d'une clé mémorisée dans le module sécurisé ;

- le résultat de reconnaissance est émis signé au moyen de la clé privée du module d'authentification ;

- le procédé d'authentification comprend une étape de déchiffrement, par le module d'authentification, de la clé privée du module d'authentification à partir d'une version chiffrée de la clé privée du module d'authentification ;

- ladite version chiffrée est mémorisée dans une mémoire non-volatile de l'appareil électronique ;

- la clé privée du module d'authentification obtenue par l'étape de déchiffrement est mémorisée dans une mémoire vive de l'appareil électronique ;

- l'étape de déchiffrement met en œuvre un algorithme cryptographique de déchiffrement utilisant une clé dérivée à partir de données reçues (d'un serveur requérant l'authentification ou du module sécurisé) et de données mémorisées dans l'appareil électronique ;

- lesdites données représentatives sont reçues par le module sécurisé en provenance du module d'authentification avec une signature associée et la signature est vérifiée au moyen d'une clé mémorisée dans le module sécurisé ;

- le module d'authentification comprend un capteur d'authentification ;

- le résultat de reconnaissance est déterminé par le module d'authentification par comparaison entre des données acquises par le capteur d'authentification et des données mémorisées par le module d'authentification ;

- le module d'authentification est mis en œuvre au moins en partie par une application d'authentification exécutée par un processeur de l'appareil électronique ;

- l'appareil électronique est un téléphone mobile, ou une tablette numérique ;

- l'appareil électronique comprend un élément de maintien sur une partie du corps de l'utilisateur (il peut s'agir par exemple d'une montre connectée ou de lunettes connectées) ;

- le module sécurisé et le module d'authentification échangent des données au moyen d'un protocole de type ISO 7816 ou SPI ou HCI/SWP.

L'invention propose également un module sécurisé comprenant au moins

une mémoire mémorisant une clé privée et un processeur programmé pour mettre en œuvre les étapes suivantes (par exemple du fait de l'exécution par le processeur d'instructions mémorisées dans la mémoire susmentionnée ou une autre mémoire du module sécurisé) :

- réception, en provenance d'un module d'authentification, d'un résultat de reconnaissance selon un processus permettant l'authentification du module d'authentification par le module sécurisé ;

- génération d'un jeton d'authentification par signature, au moyen de ladite clé privée, de données comprenant des données représentatives d'au moins une caractéristique du module d'authentification ;

- émission du jeton d'authentification généré.

Selon une possibilité de réalisation, le processeur peut être programmé pour recevoir lesdites données représentatives signées, c'est-à-dire avec une signature associée, en provenance du module d'authentification et pour vérifier la signature des données représentatives reçues au moyen d'une clé mémorisée dans le module sécurisé.

Le processeur peut par ailleurs être programmé pour mettre en œuvre le processus permettant l'authentification du module d'authentification par le module sécurisé selon les étapes suivantes :

- émission d'un défi à destination du module d'authentification ;

- réception d'une réponse en provenance du module d'authentification ;

- vérification de la réponse au moyen d'une clé publique associée à une clé privée du module d'authentification.

Le processeur peut enfin être programmé pour vérifier une signature de ladite clé publique au moyen d'une clé mémorisée dans le module sécurisé.

L'invention propose en outre un appareil électronique comprenant un module d'authentification, un module sécurisé tel que proposé ci-dessus, et une unité de commande mémorisant une application exécutable par un processeur de l'unité de commande.

L'application est par exemple une application de paiement ou une application d'accès.

L'invention propose aussi un système comprenant un serveur et un appareil électronique comme il vient d'être mentionné, dans lequel l'appareil électronique est conçu pour émettre le jeton d'authentification généré à destination

du serveur et dans lequel le serveur est conçu pour recevoir le jeton d'authentification émis et pour vérifier le jeton d'authentification reçu.

Le serveur peut en outre recevoir, par exemple au cours d'une étape préalable, des données relatives au module d'authentification en provenance d'un autre serveur. Le serveur peut également émettre un message d'autorisation ou d'information à destination de l'application en cas de vérification du jeton d'authentification reçu.

DESCRIPTION DETAILLEE D'UN EXEMPLE DE REALISATION

La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

Sur les dessins annexés :

- la figure 1 représente schématiquement un exemple de contexte dans lequel peut être mise en œuvre l'invention ;

- la figure 2 représente les étapes principales d'un exemple de procédé d'authentification d'un utilisateur d'un appareil électronique auprès d'un serveur ; et

- la figure 3 représente les étapes principales d'une variante de réalisation du procédé de la figure 2.

La figure 1 représente schématiquement un exemple de contexte dans lequel peut être mise en œuvre l'invention.

Dans cet exemple de contexte, un appareil électronique 10 (par exemple un téléphone portable (ou téléphone mobile), éventuellement de type "*intelligent*", ou "*smartphone*" selon l'appellation anglo-saxonne) comprend une unité de commande 12, un module de communication 14, un capteur d'authentification 16 et un module sécurisé 30. En variante, l'appareil électronique pourrait être par exemple une tablette numérique, une montre connectée ou des lunettes connectées. Dans ces derniers cas, l'appareil électronique comprend un élément de maintien sur une partie du corps de l'utilisateur (par exemple un bracelet dans le cas d'une montre connectée, ou des branches dans le cas de lunettes connectées).

L'unité de commande 12 est par exemple un microcontrôleur qui comprend un processeur et des mémoires, telles qu'une mémoire vive et une mémoire non-volatile réinscriptible.

L'unité de commande 12 mémorise, dans l'une au moins des mémoires susmentionnées, des applications qui permettent, lorsqu'elles sont exécutées par le processeur, la mise en œuvre par l'unité de commande 12 de procédés tels que ceux décrits plus bas.

Ces applications comprennent notamment une application client 20, un coordinateur d'authentification 22 et une application d'authentification 24.

L'application client 20 est par exemple une application de paiement ou une application d'accès.

Lorsqu'elle est exécutée par le processeur de l'unité de commande 12, l'application d'authentification 24 coopère avec le capteur d'authentification 16 de manière à former un module d'authentification 40 utilisé comme expliqué dans la suite. Un tel module d'authentification 40, ou module de reconnaissance, est parfois désigné par l'appellation anglo-saxonne "*Recognition Factor*". Il peut s'agir d'un module de reconnaissance biométrique (par exemple reconnaissance d'empreinte digitale, reconnaissance d'iris ou reconnaissance faciale), d'un module de reconnaissance vocale ou d'un clavier de saisie de code personnel (ou PIN). Dans certains modes de réalisation, le module d'authentification 40 pourrait être constitué seulement d'une application, interagissant par exemple avec une interface utilisateur (écran tactile) pour la saisie d'un code personnel.

Au sein de l'appareil électronique 10, le module sécurisé 30 et le module d'authentification 40 échangent des données par exemple au moyen d'un protocole de type ISO 7816, ou SPI, ou encore HCI/SWP

L'application client 20 peut échanger des données, au moyen du module de communication 14 et via un réseau de télécommunication 60, avec un serveur 50 (par exemple un serveur bancaire lorsque l'application client 20 est une application de paiement). On dénomme parfois "*serveur distant*" un tel serveur du fait qu'il est accessible via un réseau de télécommunication. Lorsque l'appareil électronique 10 est un téléphone portable, le réseau de télécommunication 60 comprend par exemple un réseau de téléphonie mobile (comprenant notamment des stations de base conçues pour communiquer par ondes radio avec le module de communication 14) et un réseau informatique public, tel que le réseau Internet. Les données peuvent être échangées au moyen de protocoles de type IP, GSM, http et/ou https.

Un serveur d'une autorité extérieure 70 est également connecté au

réseau de télécommunication 60 et peut ainsi échanger des données avec le serveur 50 ou avec l'appareil électronique 10.

Dans certains modes de réalisation envisageable, certaines des applications peuvent être exécutées dans un environnement d'exécution de confiance (ou TEE pour "*Trusted Execution Environment*"), voire au sein d'un autre module sécurisé (ou élément sécurisé) présent dans l'appareil électronique 10 et éventuellement associé au capteur d'authentification 16.

Le module sécurisé 30 est par exemple un élément sécurisé intégré (ou eSE pour "*embedded Secure Element*"), par exemple soudé dans l'appareil électronique 10. En variante, il peut s'agir d'une carte à microcircuit, par exemple une carte d'abonnement à un réseau de téléphonie mobile (ou carte SIM pour "*Subscriber Identity Module*"), ou une carte de type UICC (pour "*Universal Integrated Circuit Card*"), ou encore une carte micro-SD sécurisée.

Le module sécurisé 30 comprend un processeur (par exemple un microprocesseur) et des mémoires, telles qu'une mémoire vive et une mémoire non volatile réinscriptible.

Une mémoire non volatile du module sécurisé 30, par exemple la mémoire non volatile réinscriptible, mémorise les clés cryptographiques suivantes, qui ont par exemple été inscrites dans cette mémoire lors d'une phase de personnalisation du module sécurisé 30 par l'autorité extérieure :

- une clé publique de l'autorité extérieure OT_PK ;
- une clé racine OT_Apps (utilisable pour toutes les applications d'authentification préparées par ou en collaboration avec l'autorité extérieure) ;
- une clé privée de génération de jeton d'authentification SE_Auth_SK ;
- une clé privée d'authentification du module sécurisé OT_Auth_SK.

On remarque que ces clés sont mémorisées chiffrées ou non au sein du module sécurisé rendu inaccessible du fait de son haut niveau de sécurité. Ainsi, le module sécurisé 30 assure la confidentialité et l'intégrité des clés stockées.

Le serveur 50 mémorise la clé publique SE_Auth_PK associée à la clé privée d'authentification du module sécurisé SE_Auth_SK.

Selon une variante envisageable, la clé privée de génération du jeton d'authentification SE_Auth_SK n'est pas inscrite lors d'une phase de personnalisation comme indiqué ci-dessus, mais générée par le module sécurisé 30 lui-même lors d'une phase d'enregistrement (en anglais "*registration*") du

module d'authentification 40 auprès du serveur 50.

Lors de cette phase d'enregistrement, on peut par exemple prévoir la création d'un canal sécurisé entre le module sécurisé 30 et le serveur 50 (par exemple après une authentification de type identifiant – mot de passe, ou "*login/password*" selon l'appellation anglo-saxonne), la génération de la paire de clés SE_Auth_SK/SE_Auth_PK par le module sécurisé 30 et la transmission de la clé publique SE_Auth_PK au serveur 50 via le canal sécurisé.

L'application d'authentification 24 a quant à elle accès aux données suivantes, mémorisées par exemple dans la mémoire non volatile réinscriptible de l'unité de commande 12 :

- une clé privée de l'application App_SK, chiffrée par une clé secrète AEK (et notée de ce fait $[App\_SK]^{AEK}$ sur les figures) ;

- une clé publique de l'application App_PK et des données caractéristiques C du module d'authentification 40, signées par la clé privée de l'autorité extérieure OT_SK (correspondant à la clé publique OT_PK susmentionnée), c'est-à-dire accompagnée d'une signature Sign obtenue par application, à la clé publique de l'application App_PK et aux données caractéristiques C, d'un algorithme de signature utilisant la clé privée OT_SK ;

- des données de dérivation de clé App_Deriv, App_AEK_Deriv, App_AIK_Deriv (spécifiques à l'application concernée) ;

- la clé publique OT_Auth_PK correspondant à la clé privée d'authentification du module sécurisé OT_Auth_SK et un code d'authentification de message Mac obtenu par application à la clé publique OT_Auth_PK d'un algorithme cryptographique utilisant une clé AIK.

De telles données sont par exemple inscrites dans la mémoire non volatile réinscriptible lors de l'installation de l'application d'authentification 24 au sein de l'unité de commande 12. Ces données n'étant en général pas mémorisées dans un module sécurisé, les données sensibles sont mémorisées sous forme chiffrée, comme indiqué ci-dessus.

Dans l'exemple décrit ici, l'application d'authentification 24 est fournie par (ou en collaboration avec) l'autorité extérieure et la clé privée de l'application App_SK peut ainsi être chiffrée par la clé secrète AEK dérivée (comme expliqué plus bas) à partir de la clé racine OT_Apps mémorisée dans le module sécurisé 30 (également fourni par l'autorité extérieure).

Ces données sont utilisées comme expliqué ci-dessous en référence à la figure 2.

La figure 2 représente les étapes principales d'un premier exemple de procédé d'authentification d'un utilisateur de l'appareil électronique 10 auprès du serveur 50.

Ce procédé est mis en œuvre lorsque le serveur 50 qui échange des données avec l'application client 20 requiert une authentification de l'utilisateur du terminal 10.

Lors d'une étape préalable E0 (effectuée par exemple lors de l'installation de l'application d'authentification 24 au sein de l'appareil électronique 10), le serveur de l'autorité extérieure 70 transmet au serveur 50 un identifiant ID du module d'authentification 40 ainsi que des métadonnées associées, qui représentent par exemple des caractéristiques du module d'authentification 40.

À l'étape E2, le serveur 50 requiert comme indiqué ci-dessus une authentification de l'utilisateur et émet ainsi une requête d'authentification à destination de l'application client 20 avec laquelle il a préalablement échangé des données. Cette requête d'authentification est accompagnée de l'identifiant ID du module d'authentification à utiliser pour cette authentification et/ou d'un ensemble de critères MC (pour "*Match Criteria*") définissant les caractéristiques possibles de l'authentification requise et/ou du module d'authentification permettant cette authentification. L'ensemble de critères MC est par exemple une liste d'un ou plusieurs élément(s) représentant chacun une combinaison de critères acceptée par le serveur 50 pour l'authentification de l'utilisateur, chaque critère correspondant à une caractéristique possible d'un module d'authentification, par exemple un type d'authentification mise en œuvre par le module d'authentification (par reconnaissance faciale, par reconnaissance vocale, par reconnaissance d'iris, par reconnaissance d'empreinte digitale, par saisie d'un code personnel, etc.), une méthode de protection des clés cryptographiques utilisée par le module d'authentification (utilisation ou non d'un environnement d'exécution de confiance, utilisation ou non d'un module sécurisé, *etc.*), une méthode de communication utilisée par le module d'authentification.

La requête d'authentification est reçue à l'étape E4 par l'application client 20, qui la transmet (avec l'identifiant ID et l'ensemble de critères MC) au coordinateur d'authentification 22 (étape E6).

Le coordinateur d'authentification 22 reçoit la requête d'authentification avec l'identifiant ID et l'ensemble de critères MC et adresse à l'étape E8 une demande de reconnaissance (ou "*Recognition Request*" selon l'appellation anglo-saxonne) au module d'authentification 40 désigné par l'identifiant ID, en vérifiant que ce module d'authentification 40 respecte les critères définis dans l'ensemble de critères MC reçu avec la requête d'authentification. Dans certains modes de réalisation, aucun identifiant n'est transmis et le coordinateur d'authentification 22 envoie alors la demande de reconnaissance à un module d'authentification vérifiant l'une au moins des combinaisons de critères définie dans l'ensemble de critères MC.

Le module d'authentification concerné 40 (en pratique l'application d'authentification 24) reçoit la demande de reconnaissance à l'étape E10.

Selon une variante de réalisation différente de celle décrite ici, on peut alors établir un canal sécurisé entre le module d'authentification et le module de sécurisé, ce qui permet d'empêcher un attaquant passif d'avoir accès (par simple observation) aux données échangées.

Pour ce faire, le module sécurisé 30 et le module d'authentification 40 utilisent par exemple un schéma de type Diffie-Hellman, en générant chacun de leur côté une clé éphémère, en signant cette clé éphémère avec leur clé secrète, en vérifiant la signature effectuée par l'autre module et, en cas de vérification, en déduisant de ces éléments un secret commun et des clés de session à utiliser pour chiffrer les échanges ultérieurs.

Dans le mode de réalisation décrit ici, le module d'authentification 40 génère alors un défi App_Ch destiné au module sécurisé 30, par exemple par tirage aléatoire (étape E12).

Le module d'authentification 40 émet alors à destination du module sécurisé 30 le défi App_Ch, la donnée de dérivation App_Deriv et la clé publique de l'application App_PK (accompagnée des données caractéristiques C du module d'authentification), signée par la clé privée de l'autorité extérieure OT_SK, c'est-à-dire avec la signature Sign mentionnée plus haut (étape E14).

On remarque que les échanges de données sont ici réalisés directement entre le module d'authentification 40 et le module sécurisé 30, mais pourraient éventuellement être réalisés via le coordinateur d'authentification 22 (sans traitement des données par celui-ci).

Le module sécurisé 30 reçoit le défi App_Ch, la donnée de dérivation App_Deriv, ainsi que la clé publique de l'application App_PK et les données caractéristiques C du module d'authentification 40, avec la signature Sign, à l'étape E16 et vérifie la signature Sign de la clé publique de l'application App_PK et des données caractéristiques C du module d'authentification 40 au moyen d'un algorithme cryptographique de vérification de signature et de la clé publique de l'autorité extérieure OT_PK (étape E18).

Le module sécurisé 30 génère alors à son tour un défi SE_Ch, par exemple par tirage aléatoire, à l'étape E20.

Le module sécurisé 30 dérive ensuite à l'étape E22 une première clé dérivée OT_App_K par application d'une fonction de dérivation G à la clé racine OT_Apps et à la donnée de dérivation App_Deriv :

OT_App_K=G(OT_Apps, App_Deriv).

Le module sécurisé 30 génère une signature SIG1 par application au défi App_Ch généré à l'étape E12 et reçu à l'étape E16 d'un algorithme cryptographique de signature et de la clé privée d'authentification du module sécurisé OT_Auth_SK (étape E24).

Le module sécurisé 30 émet à destination du module d'authentification 40 la signature SIG1, le défi SE_Ch généré à l'étape E20 et la première clé dérivée OT_App_K (étape E26).

Le module d'authentification 40 reçoit la signature SIG1, le défi SE_Ch et la première clé dérivée OT_App_K à l'étape E28.

Le module d'authentification 40 dérive à l'étape E30 une seconde clé dérivée AEK par application d'une fonction de dérivation F à la première clé dérivée OT_App_K et à la donnée de dérivation App_AEK_Deriv (mémorisée en mémoire non-volatile comme déjà indiqué) :

AEK = F(OT_App_K,App_AEK_Deriv).

Cette seconde clé de dérivation AEK est égale à la clé secrète avec laquelle a été chiffrée la clé privée de l'application App_SK mémorisée dans l'unité de commande 12 en association avec l'application d'authentification 24. (Comme déjà indiqué, dans le mode de réalisation décrit ici, l'application d'authentification 24 a été fournie par ou en collaboration avec l'autorité extérieure qui a pu calculer la clé secrète AEK et chiffrer la clé privée de l'application App_SK avec cette clé secrète AEK avant installation de l'application d'authentification 24 dans l'appareil

électronique 10).

Ainsi, le module d'authentification 40 peut déchiffrer la clé privée de l'application App_SK à l'aide de cette seconde clé de dérivation AEK (étape E32). La clé privée de l'application App_SK peut alors être momentanément mémorisée dans la mémoire vive de l'unité de commande 12.

Le module d'authentification 40 dérive ensuite à l'étape E34 une troisième clé dérivée AIK par application de la fonction de dérivation F à la première clé dérivée OT_App_K et à une autre donnée de dérivation, ici la donnée de dérivation App_AIK_Deriv :

AIK = F(OT_App_K,App_AIK_Deriv).

Le module d'authentification 40 peut ainsi vérifier à l'étape E36 l'intégrité de la clé publique OT_Auth_PK en comparant un code d'authentification de message, obtenu par application à la clé publique OT_Auth_PK d'un algorithme cryptographique utilisant une clé AIK dérivée à l'étape E34, et le code d'authentification de message Mac mémorisé en association avec la clé publique OT_Auth_PK dans la mémoire non-volatile de l'unité de commande 12.

Si cette vérification est positive, le module d'authentification 40 peut vérifier la signature SIG1 à l'aide de la clé publique OT_Auth_PK (étape E38), en comparant par exemple le défi App_Ch généré à l'étape E12 et le résultat de l'application à la signature reçue SIG1 d'un algorithme cryptographique de vérification de signature utilisant la clé publique OT_Auth_PK. Selon une variante envisageable, la signature SIG1 peut être vérifiée en appliquant, au défi App_Ch et à la signature reçue SIG1, un algorithme cryptographique de vérification de signature utilisant la clé publique OT_Auth_PK et produisant (directement) un résultat positif ou négatif.

Si la signature SIG1 est correctement vérifiée, ceci implique que le module sécurisé 30 s'est correctement authentifié auprès du module d'authentification 40.

Naturellement, dans le cas non représenté sur la figure 2 où l'une des deux vérifications précitées se solde par un échec, il est mis fin au processus d'authentification de l'utilisateur sans émission d'un jeton d'authentification.

Dans le cas où la signature SIG1 est correctement vérifiée à l'étape E38, le module d'authentification 40 procède à l'étape E40 à la reconnaissance de l'utilisateur, par exemple par reconnaissance d'empreinte digitale, ce qui permet

de générer un résultat de reconnaissance R (positif ou négatif).

Le résultat de reconnaissance R est généralement déterminé par le module d'authentification par comparaison entre des données acquises par le capteur d'authentification (par exemple des données biométriques représentatives d'une partie adéquate du corps de l'utilisateur placée face au capteur d'authentification) et des données mémorisées par le module d'authentification 40, par exemple dans la mémoire non-volatile réinscriptible de l'unité de commande 12. Ces dernières données ont par exemple été mémorisées au préalable par le module d'authentification 40 lors d'une phase d'apprentissage (parfois dénommée phase d'enrôlement, de l'appellation anglo-saxonne "*enrollment*").

Le résultat de reconnaissance R obtenu à l'étape E40 et le défi SE_Ch reçu à l'étape E28 sont signés au moyen d'un algorithme cryptographique de signature et de la clé privée de l'application App_SK momentanément mémorisée en mémoire vive (après quoi cette clé privée App_SK peut être effacée de la mémoire vive), ce qui permet d'obtenir une signature SIG2 (étape E42).

Le résultat de reconnaissance R et la signature SIG2 sont envoyés du module d'authentification 40 au module sécurisé 30 (étape E44).

Le module sécurisé 30 reçoit ainsi à l'étape E46 le résultat de reconnaissance R et la signature SIG2.

Le module sécurisé 30 peut alors vérifier à l'étape E48 la signature SIG2 à l'aide de la clé publique de l'application App_PK obtenue à l'étape E18, par exemple en appliquant cette clé publique App_PK à la signature SIG2 au moyen d'un algorithme cryptographique de vérification de signature et en comparant le résultat obtenu au résultat de reconnaissance R reçu et au défi SE_Ch généré à l'étape E20 (et envoyé à l'étape E26). Selon une variante envisageable, la signature SIG2 peut être vérifiée en appliquant, au résultat de reconnaissance R, au défi SE_Ch et à la signature reçue SIG2, un algorithme cryptographique de vérification de signature utilisant la clé publique App_PK et produisant (directement) un résultat positif ou négatif.

Si la signature SIG2 est correctement vérifiée, cela signifie que le module d'authentification 40 s'est correctement authentifié auprès du module sécurisé 30.

Le module sécurisé 30 peut ainsi associer de manière certaine les données caractéristiques C du module d'authentification 40 reçues à l'étape E16 au module d'authentification 40 authentifié.

La signature SIG2 permet en outre de s'assurer que le résultat de reconnaissance R est bien celui émis par le module d'authentification 40.

On remarque que, dans la variante mentionnée ci-dessus où un canal sécurisé est d'abord établi entre le module sécurisé 30 et le module sécurisé 40, il n'est pas nécessaire (mais toutefois possible) de procéder aux échanges de type défi-réponse (en anglais "*challenge-response*") qui visent l'authentification mutuelle du module sécurisé 30 et du module sécurisé 40, puisque l'utilisation du canal sécurisé permet déjà une telle authentification mutuelle.

Lorsque le résultat de reconnaissance est positif, le module sécurisé peut par conséquent générer un jeton d'authentification TOK à l'étape E50, en appliquant, à un ensemble de données incluant une partie au moins des données caractéristiques C du module d'authentification 40, un algorithme cryptographique de signature utilisant la clé privée de génération de jeton d'authentification SE_Auth_SK. Le jeton d'authentification TOK peut notamment inclure, outre cette signature, les données caractéristiques C du module d'authentification 40.

On remarque que l'ensemble de données précité peut également inclure un défi (ou "*challenge*" selon l'appellation anglo-saxonne) généré par le serveur 50 avant l'étape E2 et transmis avec la requête d'authentification du serveur 50 à l'application client 20 (étape E2), puis de l'application client 20 au coordinateur d'authentification 24 (étape E4), puis du coordinateur d'authentification 24 au module d'authentification 40 avec la demande de reconnaissance (étape E8), puis enfin du module d'authentification 40 au module sécurisé 30 à l'étape E14.

Les données caractéristiques du module d'authentification 40 incluses dans les données signées au moyen de la clé privée SE_Auth_SK comprennent par exemple un identifiant du module d'authentification et/ou un type d'authentification mise en œuvre par le module d'authentification et/ou une méthode de protection des clés cryptographiques utilisée par le module d'authentification et/ou une méthode de communication utilisée par le module d'authentification.

Le jeton d'authentification TOK est alors émis par le module sécurisé 30 à destination du coordinateur d'authentification 22 (étape E52), puis du coordinateur d'authentification 22 à l'application client 20 (étape E54), puis enfin de l'application client 20 au serveur 50 (étape E56).

Le jeton d'authentification TOK est ainsi reçu par le serveur 50 à l'étape

E58 et peut être vérifié au niveau du serveur 50 au moyen de la clé publique SE_Auth_PK (en tenant compte éventuellement du défi possiblement généré par le serveur 50 avant l'étape E2 comme indiqué ci-dessus), ce qui permet d'authentifier auprès du serveur 50 l'utilisateur reconnu par le module d'authentification 40.

Le serveur 50 peut également vérifier à cette occasion que l'ensemble de données signé par le module sécurisé 30 (étape E50) inclut bien les caractéristiques C du module d'authentification 40 (par exemple incluses dans le jeton d'authentification TOK) et que celles-ci respectent les critères définis (avant envoi à l'étape E2) dans l'ensemble de critères MC. La validité de ces caractéristiques C est garantie par leur signature au moyen de la clé privée SE_Auth_SK mémorisée dans le module sécurisé 30.

Le serveur 50 peut alors émettre à l'étape E60 un message d'autorisation MOK (ou message d'information sur l'état d'autorisation) à destination de l'application client 20.

L'application client 20 reçoit le message d'autorisation MOK à l'étape E62 et est ainsi informée de la réussite du processus d'authentification de l'utilisateur. L'application client 20 peut alors commander l'affichage d'un message indicatif de la réussite de l'authentification sur une interface utilisateur (non représentée) de l'appareil électronique 10.

Dans l'exemple qui vient d'être décrit, le serveur 50 mémorise une clé publique SE_Auth_PK pour chaque ensemble module d'authentification – module sécurisé enregistré auprès du serveur 50. Pour éviter cette nécessité de mémorisation, on peut prévoir selon une autre possibilité de réalisation que le module sécurisé 30 mémorise un certificat comprenant la clé publique SE_Auth_PK (associée à sa propre clé privée SE_Auth_SK) et une signature de cette clé publique SE_Auth_PK générée au préalable par une autorité de confiance (au moyen d'une clé privée de cette autorité de confiance). Le module sécurisé pourrait alors émettre ce certificat avec le jeton d'authentification TOK (étape E54) et le serveur pourrait alors vérifier tout d'abord la signature de la clé publique SE_Auth_PK contenue dans le certificat (au moyen d'une clé publique de l'autorité de confiance), puis le jeton d'authentification TOK au moyen de la clé publique SE_Auth_PK (comme à l'étape E58).

La figure 3 représente les étapes principales d'une variante de réalisation

du procédé d'authentification qui vient d'être décrit en référence à la figure 2.

Un tel procédé est mis en œuvre dans un contexte du même type que celui de la figure 1 décrit ci-dessus, mises à part les différences suivantes :

- la clé racine OT_Apps n'est pas mémorisée dans le module sécurisé 30 mais au niveau du serveur 50 ;

- l'application d'authentification 24 mémorise (par exemple dans la mémoire non-volatile réinscriptible de l'unité de commande 12) les données de dérivation App_AEK_Deriv et App_AIK_Deriv, mais la donnée de dérivation App_Deriv visible en figure 1 n'est en revanche pas utilisée.

Cette variante est utilisable lorsque l'application d'authentification 24 n'a pas été fournie par (ou en collaboration avec) l'autorité extérieure ayant fourni le module sécurisé 30.

Au cours d'une étape E100, le serveur 50 émet à destination de l'application client 20 une requête d'authentification. Cette requête d'authentification est accompagnée de l'identifiant ID du module d'authentification à utiliser pour cette authentification et/ou d'un ensemble de critères MC (pour "*Match Criteria*"), du même type que décrit ci-dessus en référence à la figure 2 et dans lequel a été introduite en outre la clé racine OT_Apps (par exemple au sein d'un champ spécifique dédié).

La requête d'authentification accompagnée de l'identifiant ID et de l'ensemble de critères MC intégrant la clé racine OT_Apps est reçue par l'application client 20 à l'étape E102 et transmise au coordinateur d'authentification 22.

Le coordinateur d'authentification 22 reçoit ainsi l'identifiant ID et l'ensemble de critères MC intégrant la clé racine OT_Apps à l'étape E104.

Le coordinateur d'authentification 22 peut ainsi émettre, à destination du module d'authentification 40 désigné par l'identifiant ID et/ou respectant les critères définis dans l'ensemble de critères MC, une demande de reconnaissance accompagnée de l'ensemble de critères MC intégrant la clé racine OT_Apps (étape E106).

Le module d'authentification 40 reçoit la demande de reconnaissance à l'étape E108 et peut ainsi extraire de l'ensemble de critères MC la clé racine OT_Apps à l'étape E110.

Le module d'authentification 40 peut ainsi calculer à l'étape E112 la clé

dérivée AEK, par application d'une fonction de dérivation H à la clé racine OT_Apps (extraite à l'étape E110) et aux données de dérivation App_AEK_Deriv (mémorisées en association avec l'application d'authentification 24, comme indiqué ci-dessus) :

AEK=H(OT_Apps,App_AEK_Deriv).

Comme dans le cas de la figure 2, la clé dérivée AEK a été utilisée au préalable (avant installation de l'application d'authentification 24 dans l'appareil électronique 10) pour chiffrer la clé privée de l'application App_SK.

Le module d'authentification 40 peut donc déchiffrer la clé privée de l'application App_SK (mémorisée sous forme chiffrée dans la mémoire non-volatile de l'unité de commande 12) par application d'un algorithme de déchiffrement utilisant la clé dérivée AEK (étape E114) et mémoriser, de manière temporaire, la clé privée de l'application App_SK (non chiffrée) dans la mémoire vive de l'unité de commande 12.

Le module d'authentification 40 génère alors un défi App_Ch, par exemple par tirage aléatoire (étape E116).

Le module d'authentification 40 transmet ensuite à l'étape E118 la clé publique de l'application App_PK et les données caractéristiques C du module d'authentification 40, signées par la clé privée de l'autorité extérieure OT_SK et donc accompagnées de la signature Sign, ainsi que le défi App_Ch.

Ces données sont reçues par le module sécurisé 30 à l'étape E120.

Le module sécurisé 30 vérifie à l'étape E122 la signature Sign de la clé publique de l'application App_PK et des données caractéristiques C du module d'authentification 40 au moyen d'un algorithme cryptographique de vérification de signature et de la clé publique de l'autorité extérieure OT_PK (mémorisée comme indiqué en figure 1 dans la mémoire non-volatile du module sécurisé 30).

Le module sécurisé 30 génère alors un défi SE_Ch, par exemple par tirage aléatoire (étape E124).

Le module sécurisé 30 génère une signature SIG1 par application au défi App_Ch, généré à l'étape E116 et reçu à l'étape E120, d'un algorithme cryptographique de signature utilisant la clé privée d'authentification du module sécurisé OT_Auth_SK (étape E126).

À l'étape E126, le module sécurisé 30 émet à destination du module d'authentification 40 la signature SIG1 et le défi SE_Ch généré à l'étape E124.

Le module d'authentification 40 reçoit la signature SIG1 et le défi SE_Ch à l'étape E128.

Le module d'authentification 40 dérive ensuite à l'étape E130 une clé dérivée AIK par application de la fonction de dérivation H à la clé racine OT_Apps extraite à l'étape E110 et à une autre donnée de dérivation, ici la donnée de dérivation App_AIK_Deriv :

AIK = H(OT_Apps,App_AIK_Deriv).

Le procédé se poursuit alors comme indiqué ci-dessus en référence à la figure 2 à partir de l'étape E36.

REVENDICATIONS

1. Procédé d'authentification d'un utilisateur à l'aide d'un appareil électronique (10) comprenant un module d'authentification (40) et un module sécurisé (30), comprenant les étapes suivantes :

- émission (E44) par le module d'authentification (40) d'un résultat de reconnaissance (R) à destination du module sécurisé (30) selon un processus permettant l'authentification du module d'authentification (40) par le module sécurisé (30) ;

- génération (E50) d'un jeton d'authentification (TOK) par le module sécurisé (30) par signature, au moyen d'une clé privée (SE_Auth_SK) mémorisée dans le module sécurisé (30), de données comprenant des données représentatives d'au moins une caractéristique du module d'authentification (40) ;

- émission (E52) du jeton d'authentification généré (TOK).

2. Procédé d'authentification selon la revendication 1, dans lequel lesdites données représentatives sont reçues (E16 ; E120) par le module sécurisé (30) en provenance du module d'authentification (40) avec une signature associée et dans lequel la signature est vérifiée (E18 ; E122) au moyen d'une clé (OT_PK) mémorisée dans le module sécurisé (30).

3. Procédé d'authentification selon la revendication 1 ou 2, dans lequel le processus permettant l'authentification du module d'authentification (40) par le module sécurisé (30) utilise une clé privée du module d'authentification (App_SK).

4. Procédé d'authentification selon la revendication 3, dans lequel le processus permettant l'authentification du module d'authentification (40) par le module sécurisé (30) comprend les étapes suivantes :

- transmission (E26 ; E126) d'un défi (SE_Ch) du module sécurisé (30) au module d'authentification (40) ;

- génération (E42) d'une réponse (SIG2) par le module d'authentification par application au défi (SE_Ch) d'un algorithme de signature utilisant la clé privée du module d'authentification (App_SK) ;

- transmission (E44) de la réponse (SIG2) du module d'authentification (40) au module sécurisé (30) ;

- vérification (E48) de la réponse (SIG2) par le module sécurisé (30) au moyen de la clé publique (App_PK) associée à la clé privée du module d'authentification (App_SK).

5. Procédé d'authentification selon la revendication 4, dans lequel ladite clé publique (App_PK) est reçue (E14 ; E118) par le module sécurisé (30) avec une signature associée et dans lequel la signature est vérifiée (E18 ; E122) par le module sécurisé (30) au moyen d'une clé (OT_PK) mémorisée dans le module sécurisé (30).

6. Procédé d'authentification selon l'une des revendications 3 à 5, dans lequel le résultat de reconnaissance (R) est émis (E44) signé au moyen de la clé privée du module d'authentification (App_SK).

7. Procédé d'authentification selon l'une des revendications 3 à 6, comprenant une étape de déchiffrement (E32 ; E114), par le module d'authentification (40), de la clé privée du module d'authentification (App_SK) à partir d'une version chiffrée de la clé privée du module d'authentification ($[App\_SK]^{AEK}$).

8. Procédé d'authentification selon la revendication 7, dans lequel ladite version chiffrée ($[App\_SK]^{AEK}$) est mémorisée dans une mémoire non-volatile de l'appareil électronique (10) et dans lequel la clé privée du module d'authentification (App_SK) obtenue par l'étape de déchiffrement (E32 ; E114) est mémorisée dans une mémoire vive de l'appareil électronique (10).

9. Procédé d'authentification selon l'une des revendications 7 ou 8, dans lequel l'étape de déchiffrement (E32 ; E114) met en œuvre un algorithme cryptographique de déchiffrement utilisant une clé (AEK) dérivée à partir de données reçues (OT_App_K ; OT_Apps) et de données (App_AEK_Deriv) mémorisées dans l'appareil électronique (10).

10. Procédé d'authentification selon l'une des revendications 1 à 9, dans lequel le module d'authentification (40) comprend un capteur d'authentification (16) et dans lequel le résultat de reconnaissance (R) est déterminé par le module d'authentification (40) par comparaison entre des données acquises par le capteur d'authentification (16) et des données mémorisées par le module d'authentification (40).

11. Procédé d'authentification selon l'une des revendications 1 à 10, dans lequel le module d'authentification (40) est mis en œuvre au moins en partie par une application d'authentification (24) exécutée par un processeur (12) de l'appareil électronique (10).

12. Procédé d'authentification selon l'une des revendications 1 à 11,

dans lequel l'appareil électronique (10) est un téléphone mobile.

13. Procédé d'authentification selon l'une des revendications 1 à 11, dans lequel l'appareil électronique (10) est une tablette numérique.

14. Procédé d'authentification selon l'une des revendications 1 à 11, dans lequel l'appareil électronique (10) comprend un élément de maintien sur une partie du corps de l'utilisateur.

15. Procédé d'authentification selon l'une des revendications 1 à 14, dans lequel le module sécurisé (30) et le module d'authentification (40) échangent des données au moyen d'un protocole de type ISO 7816 ou SPI ou HCI/SWP.

16. Module sécurisé (30) comprenant au moins une mémoire mémorisant une clé privée (SE_Auth_SK) et un processeur programmé pour mettre en œuvre les étapes suivantes :

- réception (E46), en provenance d'un module d'authentification (40), d'un résultat de reconnaissance (R) selon un processus permettant l'authentification du module d'authentification (40) par le module sécurisé (30) ;

- génération (E50) d'un jeton d'authentification (TOK) par signature, au moyen de ladite clé privée (SE_Auth_SK), de données comprenant des données représentatives d'au moins une caractéristique du module d'authentification (40) ;

- émission (E52) du jeton d'authentification généré (TOK).

17. Module sécurisé selon la revendication 16, dans lequel le processeur est programmé pour recevoir (E16 ; E120) lesdites données représentatives en provenance du module d'authentification (40) avec une signature associée et pour vérifier la signature (E18 ; E122) au moyen d'une clé (OT_PK) mémorisée dans le module sécurisé (30).

18. Module sécurisé selon la revendication 16 ou 17, dans lequel le processeur est programmé pour mettre en œuvre le processus permettant l'authentification du module d'authentification (40) par le module sécurisé (30) selon les étapes suivantes :

- émission (E26 ; E126) d'un défi (SE_Ch) à destination du module d'authentification (40) ;

- réception (E46) d'une réponse (SIG2) en provenance du module d'authentification (40) ;

- vérification (E48) de la réponse au moyen d'une clé publique (App_PK) associée à une clé privée du module d'authentification (App_SK).

19. Module sécurisé selon la revendication 18, dans lequel le processeur est programmé pour vérifier une signature (E18 ; E122) de ladite clé publique (App_PK) au moyen d'une clé (OT_PK) mémorisée dans le module sécurisé (30).

20. Appareil électronique (10) comprenant un module d'authentification (40), un module sécurisé (30) selon l'une des revendications 16 à 19, et une unité de commande (12) mémorisant une application (20) exécutable par un processeur de l'unité de commande (12).

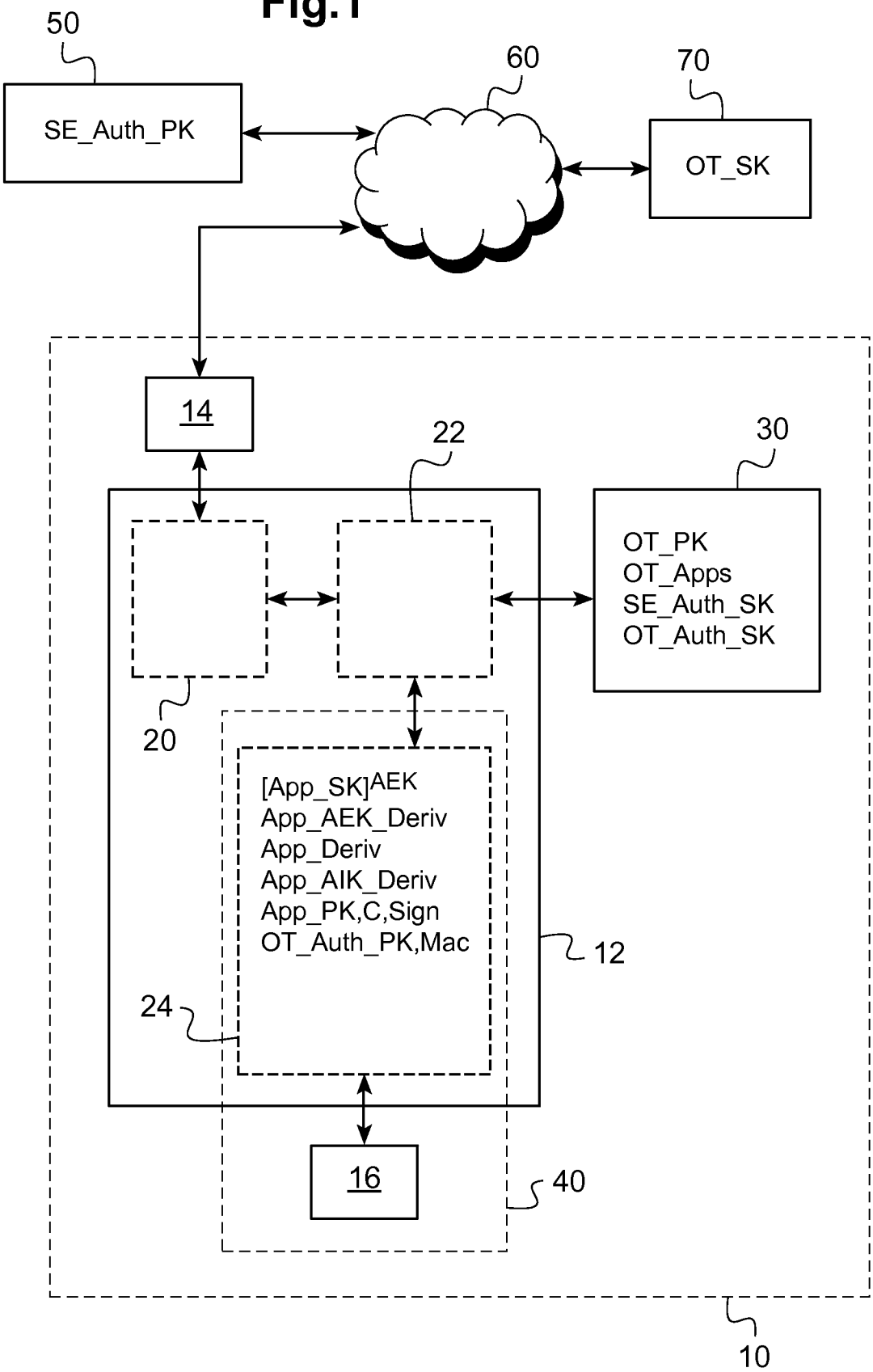
21. Appareil électronique (10) selon la revendication 20, dans lequel l'application est une application de paiement ou une application d'accès.

22. Système comprenant un serveur (50) et un appareil électronique (10) selon la revendication 20 ou 21, dans lequel l'appareil électronique (10) est conçu pour émettre le jeton d'authentification généré (TOK) à destination du serveur (50) et dans lequel le serveur (50) est conçu pour recevoir le jeton d'authentification émis (TOK) et pour vérifier le jeton d'authentification reçu (TOK).

23. Système selon la revendication 22, dans lequel le serveur (50) est conçu pour recevoir des données (ID) relatives au module d'authentification (40) en provenance d'un autre serveur (70).

24. Système selon la revendication 22 ou 23, dans lequel le serveur (50) est conçu pour émettre un message d'autorisation ou d'information (MOK) à destination de l'application (20) en cas de vérification du jeton d'authentification reçu.

Fig.1


50
SE_Auth_PK
60
70
OT_SK
14
22
30
OT_PK
OT_Apps
SE_Auth_SK
OT_Auth_SK
20
[App_SK]AEK
App_AEK_Deriv
App_Deriv
App_AIK_Deriv
App_PK,C,Sign
OT_Auth_PK,Mac
12
24
16
40
10

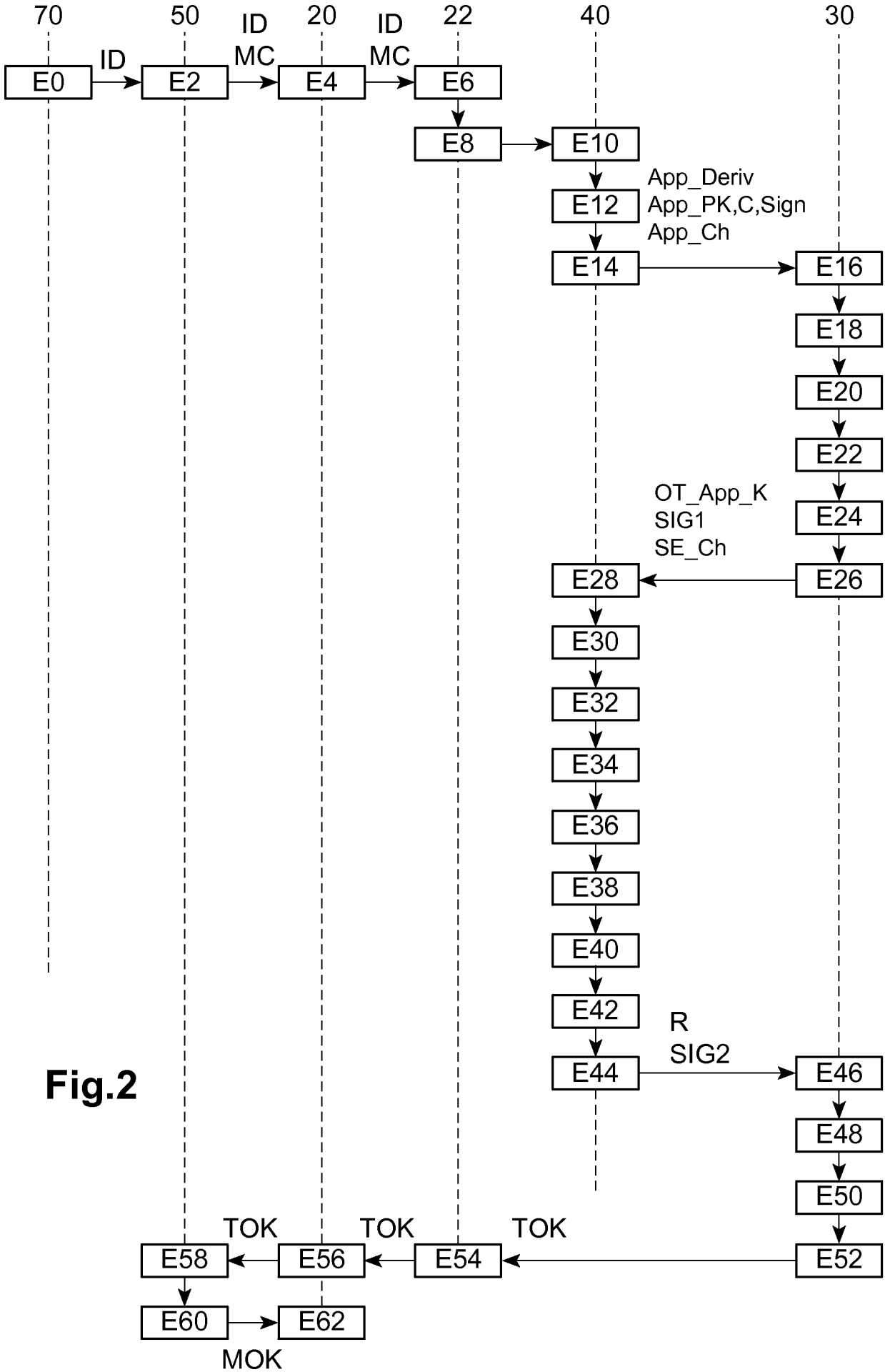
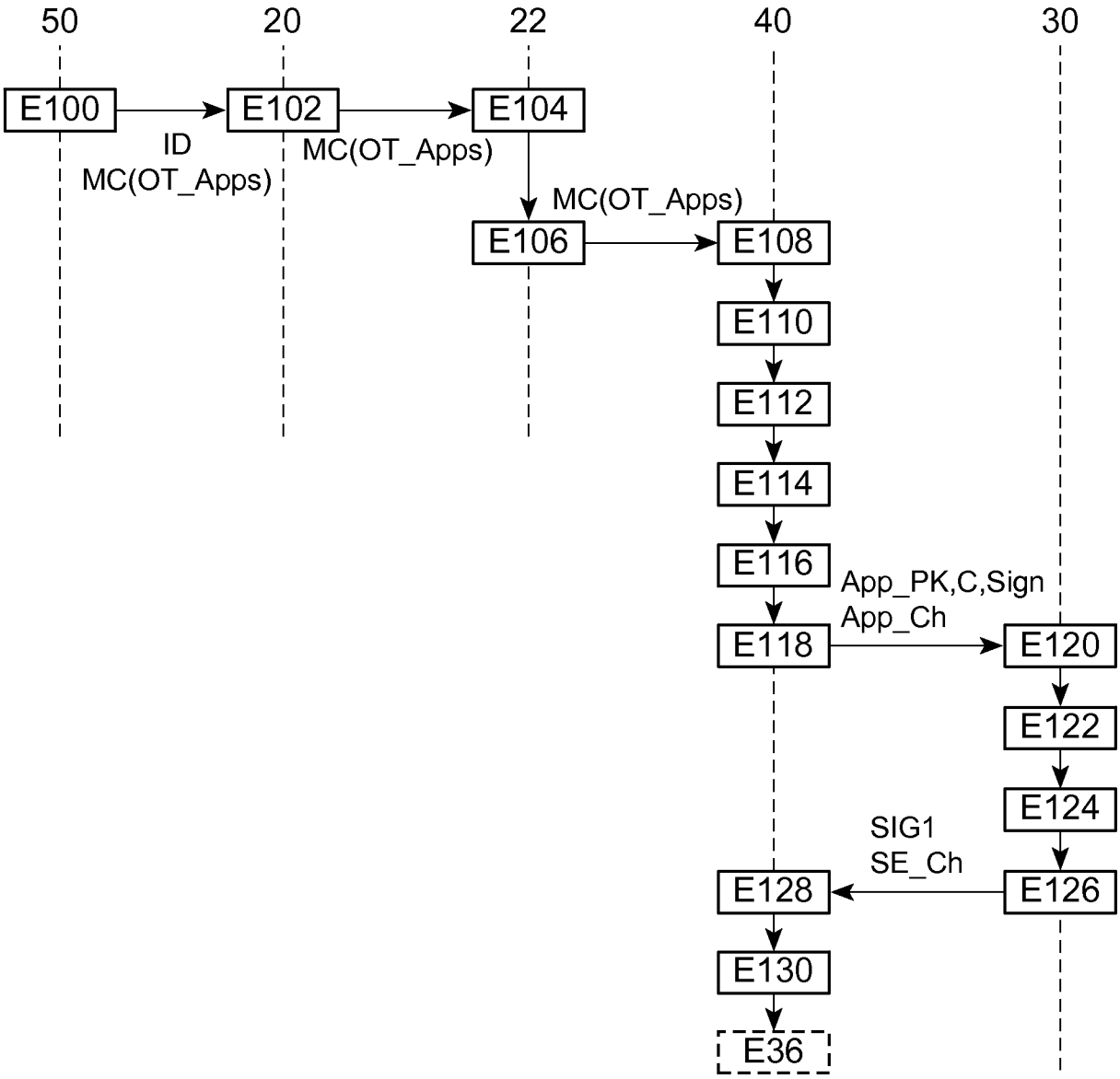

70
50
20
22
40
30
ID
ID
MC
ID
MC
E0
E2
E4
E6
E8
E10
E12
E14
E16
E18
E20
E22
E24
E26
E28
E30
E32
E34
E36
E38
E40
E42
E44
E46
E48
E50
E52
E54
E56
E58
E60
E62
App_Deriv
App_PK,C,Sign
App_Ch
OT_App_K
SIG1
SE_Ch
R
SIG2
TOK
TOK
TOK
MOK

Fig.2

Fig.3


50
20
22
40
30
E100
E102
E104
ID
MC(OT_Apps)
MC(OT_Apps)
MC(OT_Apps)
E106
E108
E110
E112
E114
E116
App_PK,C,Sign
App_Ch
E118
E120
E122
E124
SIG1
SE_Ch
E128
E126
E130
E36

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/053605

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 H04L29/06
ADD. G06F21/83

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 H04L

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

Electronic data base consulted during the international search (name of data base and, where 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.
X	EP 2 128 783 A1 (FUJITSU LTD [JP]) 2 December 2009 (2009-12-02) paragraph [0009] - paragraph [0020] paragraph [0024] - paragraph [0056] paragraph [0068] - paragraph [0073] figures 1,2,5,7,8 -----	1-24
X	US 2014/289833 A1 (BRICENO MARC [US] ET AL) 25 September 2014 (2014-09-25) paragraph [0089] - paragraph [0107] paragraph [0118] - paragraph [0128] paragraph [0151] - paragraph [0162] paragraph [0381] - paragraph [0405] figures 1,13,15,21,23,24,34,46A,50 ----- -/--	1-24

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
7 March 2016	15/03/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Sauzon, Guillaume

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/053605

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/195815 A1 (TAVEAU SEBASTIEN LUDOVIC JEAN [US] ET AL) 10 July 2014 (2014-07-10) paragraph [0007] - paragraph [0013] paragraph [0029] - paragraph [0034] paragraph [0043] - paragraph [0046] figures 2,4,6 -----	1-24

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2015/053605

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2128783 A1	02-12-2009	CN 101636740 A	27-01-2010
		EP 2128783 A1	02-12-2009
		KR 20100005037 A	13-01-2010
		US 2010082982 A1	01-04-2010
		WO 2008114390 A1	25-09-2008
US 2014289833 A1	25-09-2014	CN 105229596 A	06-01-2016
		EP 2976706 A2	27-01-2016
		US 2014289833 A1	25-09-2014
		WO 2014153462 A2	25-09-2014
US 2014195815 A1	10-07-2014	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/053605

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/32 H04L29/06
ADD. G06F21/83

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 H04L

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

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 2 128 783 A1 (FUJITSU LTD [JP]) 2 décembre 2009 (2009-12-02) alinéa [0009] - alinéa [0020] alinéa [0024] - alinéa [0056] alinéa [0068] - alinéa [0073] figures 1,2,5,7,8 -----	1-24
X	US 2014/289833 A1 (BRICENO MARC [US] ET AL) 25 septembre 2014 (2014-09-25) alinéa [0089] - alinéa [0107] alinéa [0118] - alinéa [0128] alinéa [0151] - alinéa [0162] alinéa [0381] - alinéa [0405] figures 1,13,15,21,23,24,34,46A,50 ----- -/--	1-24

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

[X] 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	Date d'expédition du présent rapport de recherche internationale
7 mars 2016	15/03/2016

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Sauzon, Guillaume

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/053605

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2014/195815 A1 (TAVEAU SEBASTIEN LUDOVIC JEAN [US] ET AL) 10 juillet 2014 (2014-07-10) alinéa [0007] - alinéa [0013] alinéa [0029] - alinéa [0034] alinéa [0043] - alinéa [0046] figures 2,4,6 -----	1-24

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2015/053605

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 2128783 A1	02-12-2009	CN 101636740 A	27-01-2010
		EP 2128783 A1	02-12-2009
		KR 20100005037 A	13-01-2010
		US 2010082982 A1	01-04-2010
		WO 2008114390 A1	25-09-2008
US 2014289833 A1	25-09-2014	CN 105229596 A	06-01-2016
		EP 2976706 A2	27-01-2016
		US 2014289833 A1	25-09-2014
		WO 2014153462 A2	25-09-2014
US 2014195815 A1	10-07-2014	AUCUN	