(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 134 493**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 03269**

(51) Int Cl[8] : ***H 04 W 8/20*** *(2022.01), H 04 W 12/40, 12/069, 12/106, H 04 L 9/32*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 08.04.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 13.10.23 Bulletin 23/41.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

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

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

(72) **Inventeur(s) :** NOISETTE Yoan, ROZE Stephen et SIMAGIN Kirill.

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

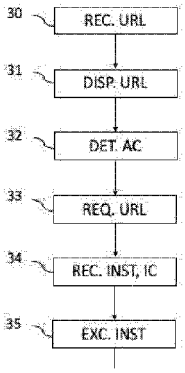
(74) **Mandataire(s) :** CABINET VIDON BREVETS ET STRATEGIE.

(54) Procédé d'activation d'un profil utilisateur dans un équipement terminal, dispositif, système et programme d'ordinateur correspondant.

(57) Procédé d'activation d'un profil utilisateur dans un équipement terminal, dispositif, système et programme d'ordinateur correspondant

L'invention concerne un procédé d'activation d'un profil utilisateur dans un équipement terminal, , ledit procédé comprenant:- la réception (30), au cours d'une session de communication établie entre l'équipement terminal et ledit réseau, d'une information d'identification d'accès à des instructions de code de programme (URL_PRG1) configurées pour commander l'obtention dudit profil utilisateur (UP) dudit réseau et le stockage dudit profil utilisateur dans un module sécurisé (eUICC/eSIM) de l'équipement terminal, lorsqu'elles s'exécutent sur ledit équipement terminal;-suite à la détection (32) d'une sélection par l'utilisateur de l'information d'identification d'accès, l'émission (33) à destination dudit réseau d'une demande d'accès auxdites instructions de code de programme à partir de ladite information d'identification d'accès (URL_PRG1);-la réception (34) en provenance dudit réseau des instructions de code de programme et d'une première information cryptographique (MQ_CP1) signant lesdites instructions de code de programme ;-l'exécution (35) desdites instructions de code de programme,, après vérification que la première information cryptographique (MQ_CP1) signant les instructions de code de programme a été obtenue à partir d'un même certificat de l'opérateur que ledit profil utilisateur (UP).

Figure 3



FR 3 134 493 - A1

Description

Titre de l'invention : Procédé d'activation d'un profil utilisateur dans un équipement terminal, dispositif, système et programme d'ordinateur correspondant

Domaine de l'invention

[0001] Le domaine de l'invention est celui des réseaux de communication, en particulier des réseaux de téléphonie mobile.

[0002] L'invention concerne en particulier l'activation d'un profil utilisateur dans un équipement terminal, suite à la souscription par l'utilisateur à une offre de service fourni par un tel réseau de communication.

[0003] L'invention a de nombreuses applications, notamment, mais non exclusivement, dans le domaine des réseaux de radiocommunication conformes aux normes 3GPP (de l'anglais « 3rd Generation Partnership Project ») de dernières générations ou de générations futures.

Art antérieur

[0004] Dans la plupart des cas, un équipement terminal d'un utilisateur (e.g. un smartphone, une tablette ou un ordinateur équipé d'une connexion cellulaire, etc.) destiné à être connecté à un réseau de radiocommunications est équipé d'une carte à circuit intégré universel ou UICC (de l'anglais, « universal integrated circuit card ») ou SIM (pour « Subscriber Identity Module » en anglais). La carte UICC/SIM contient les données nécessaires à l'équipement utilisateur pour pouvoir établir une connexion avec le réseau en question. Pour de tels équipements, la carte UICC/SIM est traditionnellement une carte physique fournie par l'opérateur lors de la souscription d'un abonnement.

[0005] Une telle carte est ainsi par nature amovible de l'équipement terminal. Ainsi, lors de la résiliation de l'abonnement correspondant, l'utilisateur de l'équipement terminal retire naturellement la carte SIM, devenue inutilisable, de l'équipement en question. C'est par exemple le cas afin de mettre une nouvelle carte SIM correspondant à un nouvel abonnement. Alternativement, si l'utilisateur n'a plus l'usage de l'équipement après la résiliation de son abonnement, l'utilisateur éteint souvent l'équipement terminal (ou ce dernier s'éteint naturellement une fois la batterie déchargée). Ainsi, quand bien même l'utilisateur laisserait la carte SIM maintenant inutilisable dans l'équipement terminal, l'équipement utilisateur n'enverrait aucune requête sur le réseau de l'opérateur désigné via la carte SIM.

[0006] Cependant, de nouveaux équipements terminaux, comme par exemple certains objets connectés, sont équipés d'une technologie de carte ou module eUICC/eSIM embarqué ou intégré (e.g. une eSIM, pour « Embedded Subscriber Identity Module » en anglais).

Cette technologie UICC/SIM intégrée, spécifiée par la GSMA, permet le provisionnement à distance d'un profil de l'utilisateur sur tout équipement terminal doté de cette technologie et ainsi d'activer le service d'un opérateur sans avoir de carte SIM physique. Plus particulièrement, un profil opérationnel contenant les données permettant l'accès au réseau est activé dans le module eUICC ou eSIM embarqué. Le module eUICC/eSIM est intégré directement dans l'équipement utilisateur : smartphone, tablette, montre connectée, etc. Cette évolution répond à la multiplication des formats de cartes SIM (standard, mini-SIM, micro SIM, nano SIM...) et à la diversification des usages.

[0007] Ainsi, la technologie eUICC/eSIM procure de nombreux avantages, parmi lesquels :

- la possibilité de gérer plusieurs abonnements et plusieurs opérateurs sur un même équipement utilisateur,
- le changement d'opérateur facilité puisqu'il n'est plus nécessaire de demander une nouvelle carte SIM, le service d'un opérateur étant activé à distance en téléchargeant les informations directement dans le module électronique ou puce embarqué dans l'équipement terminal,
- la possibilité de souscrire à l'avance à un service de l'opérateur (par exemple, appels à l'international), qu'il suffit ensuite d'activer dans le module électronique, et
- la place libérée dans l'équipement utilisateur, dans lequel il n'est plus nécessaire de prévoir une ouverture extérieure, ce qui permet de renforcer l'étanchéité de l'appareil.

[0008] Pour réaliser le provisionnement à distance du module eUICC/eSIM, le système d'exploitation ou OS (en anglais, « Operation System ») de l'équipement terminal intègre une interface sécurisée ou API (« Application Programming Interface », en anglais) spécifique, elle aussi standardisée, appelée LPA-API. Elle est gérée par une application logicielle LPA (pour « Local Profile Assistant », en anglais), intégrée au système d'exploitation, qui permet l'accès au module eUICC/eSIM, le chargement et la gestion de profils utilisateurs sur ce module. Cette application LPA sert ainsi de pont entre une plateforme de service de l'opérateur, en charge de la gestion des souscriptions appelé SM-DP+ (« Subscription Manager and Data Preparation », en anglais) qui prépare, stocke et fournit les profils utilisateurs et le module eUICC/eSIM de l'équipement utilisateur. Cette plateforme fait partie du réseau de communication de l'opérateur.

[0009] En pratique, la méthode la plus répandue aujourd'hui pour activer un profil utilisateur sur un équipement utilisateur, par exemple suite à la souscription par cet utilisateur d'un nouveau forfait mobile, consiste a lui fournir un QR Code sous forme matérielle, par exemple sur un document papier imprimé (en anglais, « flyer ») ou par mail ou encore via un portail Web. Il doit ensuite le scanner manuellement avec son équipement terminal. Cette opération déclenche alors le chargement automatique du

profil utilisateur sur l'équipement terminal, puis son installation dans le module eSIM. On comprend en effet que l'utilisateur ne peut pas afficher le QR code sur son équipement terminal et le scanner avec ce même équipement terminal.

[0010] En alternative, l'utilisateur peut saisir le QR code à la main dans des options d'administration du module sécurisé eSIM/eUICC.

[0011] Néanmoins, quelle que soit la méthode, l'utilisateur doit réaliser une opération manuelle, sans être forcément bien guidé (pour lancer l'application scanner ou pour trouver les options d'administration dans les paramètres de son équipement terminal. En tout état de cause, cette opération manuelle n'est pas simple et surtout elle reste hors de portée de nombreux utilisateurs de téléphones mobiles. Il en résulte que la finalisation du parcours client peut échouer pour cause d'erreur de manipulation, telle qu'une perte de QR code ou de scan sur un téléphone mobile non compatible ou non connecté à un réseau de données.

[0012] Une alternative consiste a demander à l'utilisateur d'utiliser une application logicielle dédiée, configurée pour charger le profil utilisateur et l'installer dans le module eUICC/eSIM, en effectuant tous les contrôles et opérations requis. Il s'agit généralement d'une application native, au sens où elle est développée spécifiquement (ou « nativement ») pour s'intégrer au système d'exploitation de l'équipement terminal. Une telle application dispose souvent d'une interface utilisateur ergonomique et facile d'utilisation, qui guide l'utilisateur à chaque étape. Un inconvénient majeur de cette solution est qu'elle impose le téléchargement puis l'installation cette application logicielle de l'opérateur. Elle est disponible via un canal de distribution générique, par exemple sur un magasin d'applications logicielles (par exemple Google Play ®), et son installation nécessite l'usage d'un identifiant et d'un mot de passe spécifiques préalablement fournis par l'opérateur. Ainsi cette solution alternative nécessite plusieurs manipulations et opérations de la part de l'utilisateur, ce qui peut être rebutant pour certaines personnes peu familières de ce genre d'applications. En outre, l'effort à produire peut être considéré comme disproportionné par rapport à l'usage de l'application, destiné à être ponctuel.

[0013] Il existe donc un besoin d'une solution plus simple, efficace et flexible pour activer le profil de souscription d'un utilisateur dans son équipement terminal.

Exposé de l'invention

[0014] L'invention répond à ce besoin en proposant un procédé d'activation d'un profil utilisateur dans un équipement terminal, ledit profil utilisateur ayant été généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication lorsqu'il est stocké dans un module sécurisé de l'équipement terminal, ledit

procédé étant caractérisé en ce qu'il est mis en œuvre dans l'équipement terminal et comprend :

- la réception, au cours d'une session de communication établie entre l'équipement terminal et ledit réseau, d'une information d'identification d'accès à des instructions de code de programme configurées pour commander l'obtention dudit profil utilisateur dudit réseau et le stockage dudit profil utilisateur dans ledit module, lorsqu'elles s'exécutent sur ledit équipement terminal;
- suite à la détection d'une sélection par l'utilisateur de l'information d'identification d'accès, l'émission à destination dudit réseau d'une demande d'accès auxdites instructions de code de programme à partir de ladite information d'identification d'accès;
- la réception en provenance dudit réseau des instructions de code de programme et d'une première information cryptographique signant lesdites instructions de code de programme ;
- l'exécution desdites instructions de code de programme, comprenant l'émission d'une commande d'obtention et de stockage dudit profil utilisateur audit module, ledit profil utilisateur étant stockée dans ledit module sécurisé, après vérification que la première information cryptographique signant les instructions de code de programme a été obtenue à partir d'un même certificat de l'opérateur que ledit profil utilisateur.

[0015] L'invention s'appuie ainsi sur une approche tout-à-fait nouvelle et inventive de l'activation du profil d'un utilisateur d'un réseau de communication mobile qui vient de souscrire à un nouvel abonnement. La solution proposée consiste à déclencher le téléchargement et le stockage de ce nouveau profil utilisateur dans le module eUICC/ eSIM de son équipement terminal à partir du simple lancement d'une URL fournie par l'opérateur, par exemple à l'issue d'un parcours de souscription suivi par l'utilisateur.

[0016] De la sorte, l'utilisateur n'a plus besoin d'effectuer une démarche spécifique et supplémentaire comme celle d'installer puis d'ouvrir une application native de gestion des profils utilisateurs, hébergée sur un canal de distribution générique (tel que Google Play par exemple) et nécessitant une authentification par identifiant et mot de passe. Il n'a pas besoin non plus de scanner un QR code.

[0017] Avec l'invention, au contraire, l'utilisateur n'a qu'à « cliquer » sur le lien de l'URL affiché par l'équipement terminal pour déclencher le chargement et l'exécution automatiques d'instructions de code de programme configurées pour commander le chargement du profil utilisateur dans le module e-SIM de l'équipement terminal. De la sorte, l'utilisateur n'a donc plus d'obligation de « sortir » du contexte applicatif dans le cadre duquel il a reçu l'URL. On suppose par exemple qu'il a souscrit à une nouvelle offre de service de l'opérateur en échangeant avec un agent conversationnel (en anglais, « chatbot », c'est-à-dire un programme d'ordinateur configuré pour dialoguer avec un utilisateur, par le biais d'une application logicielle de messagerie instantanée

et, selon l'invention, c'est cette application qui lui affiche directement le lien vers l'URL en question, sur une interface utilisateur déjà active dans le cadre de la session de communication établie.

[0018] En réduisant au minimum les opérations à réaliser par l'utilisateur sur son équipement terminal, la solution de l'invention lui permet donc de finaliser son parcours de souscription de façon beaucoup plus simple et fluide qu'avec celles de l'art antérieur.

[0019] Cette fluidité d'usage n'est pourtant pas obtenue au détriment de la sécurité, puisque le profil utilisateur n'est effectivement stocké dans le module sécurisé qu'après vérification que les instructions de code de programme reçues en vue de leur exécution sur l'équipement terminal, bénéficient du droit d'accès ou privilège (de l'anglais, « carrier privilege ») requis, ce droit d'accès étant accordé exclusivement à l'opérateur du réseau de communication mobile qui a généré le profil utilisateur.

[0020] Selon un autre aspect de l'invention, lesdites instructions de code de programme sont comprises dans une application logicielle, dite application instantanée, et correspondent à une partie des instructions de code de programme d'une autre application logicielle, dite application native, ladite application native n'étant pas exécutée au cours de la session de communication.

[0021] Avantageusement, dans un mode de réalisation, l'invention propose d'appliquer de façon astucieuse le concept d'application logicielle instantanée à la gestion des profils utilisateurs dans un équipement terminal.

[0022] Une application logicielle instantanée est liée à une application logicielle native, au sens où elle comprend une partie des instructions de code de programme de cette application native, cette partie permettant la mise en œuvre d'une partie des fonctionnalités de l'application logicielle native. Une application native est une application mobile qui est développée spécifiquement pour un des systèmes d'exploitation utilisé les équipements terminaux de type téléphone intelligent ou tablette. Ce développement spécifique permet généralement d'utiliser toutes les fonctionnalités disponibles dans le système d'exploitation (telles que le GPS, accéléromètre, appareil photo, etc.) et donc de concevoir des applications généralement plus riches que les applications web. Ces applications natives nécessitent d'être téléchargées depuis un magasin d'applications logicielles, puis installées, mais elles peuvent ensuite être utilisées sans connexion Internet.

En l'espèce, cette partie des instructions de code de programme correspond à la mise en œuvre de la fonctionnalité de chargement/activation du nouveau profil utilisateur généré par le système d'information du réseau de communication de l'opérateur, dans le module eUICC/eSIM de l'équipement terminal de l'utilisateur.

[0023] Or, aujourd'hui, les applications instantanées s'exécutent dans des environnements

ouverts mettant en œuvre des interfaces de communication non sécurisées, par exemple pour permettre à un nouvel utilisateur de tester un jeu vidéo, l'application instantanée ne lui permettant d'accéder qu'à un premier niveau de jeu par exemple.

[0024] L'invention vient ainsi à contrepied de l'usage courant en proposant ici d'adapter le mécanisme d'application instantanée à un environnement fermé, celui d'un module sécurisé de gestion de profils utilisateurs générés par un ou plusieurs opérateurs de réseaux de communications et de d'une interface de communication sécurisée avec ce module. Selon l'invention, l'application instantanée en question hérite des droits d'accès ou privilèges de l'application native dont elle est issue.

[0025] Selon encore un autre aspect de l'invention, le procédé comprend l'émission d'une représentation de l'information d'identification d'accès reçue à l'utilisateur sur une interface utilisateur mise en œuvre au cours de la session de communication et en ce que ladite sélection de l'information d'identification d'accès par l'utilisateur est détectée sur ladite interface utilisateur.

[0026] Par exemple, l'interface est une fenêtre d'interaction affichée sur l'écran tactile de l'équipement terminal. Avantageusement, il s'agit de la fenêtre dans laquelle sont affichés les messages successivement échangés entre l'utilisateur et l'agent conversationnel.

[0027] Selon un autre aspect de l'invention, le procédé comprend :

- l'obtention d'un identifiant de groupe de ladite application instantanée et de ladite première information cryptographique à partir de l'information d'identification d'accès ;
- l'obtention et le chargement des instructions de code de programme de l'application instantanée dans une mémoire de l'équipement terminal, à partir de l'identifiant de groupe de l'application, et
- la vérification que les instructions de programme reçues sont associées à ladite première information cryptographique.

Un avantage est de garantir que l'équipement terminal ne charge pas des instructions de code de programme frauduleuses.

[0028] Selon encore un autre aspect de l'invention, l'exécution des instructions de code de programme déclenche l'obtention auprès d'un premier équipement serveur du réseau de communication d'une information d'identification du profil utilisateur et d'une information d'identification d'accès à un deuxième équipement serveur stockant ledit profil utilisateur, l'envoi desdites informations audit module sécurisé dans un message de commande de chargement dudit profil utilisateur, l'obtention par une interface dudit module sécurisé dudit profil utilisateur et d'au moins une information de description associée, ladite information de description associée comprenant une deuxième information cryptographique, ladite deuxième information cryptographique signant le

profil utilisateur étant utilisée pour vérifier que la première information cryptographique signant les instructions de code de programme a été obtenue à partir du même certificat de l'opérateur que la deuxième information cryptographique.

[0029] Du fait que le module de gestion des profils utilisateur est susceptible de stocker des profils issus de plusieurs opérateurs, il n'est pas censé connaître les systèmes d'information de chacun d'eux. A réception de la commande de chargement d'un nouveau profil utilisateur, il requiert donc auprès d'une plateforme de service de cet opérateur qu'elle lui fournisse l'adresse de l'équipement serveur qui stocke le profil utilisateur et un identifiant du profil en question. Par exemple, ces deux informations sont transmises dans une même chaîne de caractères appelée code d'activation (ou « activation code », en anglais).

[0030] Les informations reçues permettent à l'interface sécurisée de vérifier que les instructions de code de programme qui s'exécutent sur l'équipement terminal et lui ont transmis la commande, sont légitimes et bénéficient du droit d'accès

[0031] L'invention concerne également un dispositif d'activation d'un profil utilisateur dans un équipement terminal, ledit profil utilisateur ayant été généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication lorsqu'il est stocké dans un module sécurisé de l'équipement terminal.

[0032] Ledit dispositif est configuré pour mettre en œuvre au sein de l'équipement terminal :

- la réception, au cours d'une session de communication établie entre l'équipement terminal et ledit réseau, d'une information d'identification d'accès à des instructions de code de programme configurées pour commander l'obtention dudit profil utilisateur dudit réseau et le stockage dudit profil utilisateur dans ledit module, lorsqu'elles s'exécutent sur ledit équipement terminal;
- suite à la détection d'une sélection par l'utilisateur de l'information d'identification d'accès, l'émission à destination dudit réseau d'une demande d'accès auxdites instructions de code de programme à partir de ladite information d'identification d'accès ;
- la réception en provenance dudit réseau des instructions de code de programme et d'une information cryptographique signant lesdites instructions de code de programme ;
- l'exécution desdites instructions de code de programme, configurée pour déclencher l'émission d'une commande d'obtention et de stockage dudit profil utilisateur audit module, ledit profil utilisateur étant stockée dans ledit module sécurisé, après vérification que la première information cryptographique signant les instructions de code de programme ont été obtenues à partir d'un même certificat de l'opérateur que ledit profil utilisateur.

[0033] Le dispositif précité met en œuvre le procédé d'activation selon l'invention dans ses

différents modes de réalisations.

[0034] Avantageusement, ledit dispositif d'activation est mis en œuvre dans un équipement terminal comprenant un module sécurisé de gestion d'au moins un profil utilisateur généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication lorsqu'il est stocké dans ledit module sécurisé.

[0035] L'invention concerne également un système de gestion d'un profil utilisateur généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication, lorsqu'il est stocké dans un module sécurisé de gestion de profils utilisateur d'un équipement terminal, ledit système comprenant un équipement terminal selon l'invention.

[0036] Le système de gestion et le dispositif d'activation présentent au moins les mêmes avantages que ceux conférés par le procédé d'activation précité.

[0037] L'invention concerne enfin un produit programme d'ordinateur comprenant des instructions de code de programme pour la mise en œuvre respective du procédé d'activation précité, lorsqu'il est exécuté par un processeur.

[0038] Un programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

[0039] L'invention vise également au moins un support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'invention tel que décrit ci-dessus.

[0040] Un tel support d'enregistrement peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple un support mobile (carte mémoire) ou un disque dur ou un SSD.

[0041] D'autre part, un tel support d'enregistrement peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens, de sorte que le programme d'ordinateur qu'il contient est exécutable à distance. Les programmes selon l'invention peuvent être en particulier téléchargés sur un réseau par exemple le réseau Internet.

[0042] Alternativement, le ou les supports d'enregistrement peuvent être un ou des circuits intégrés dans lesquels chaque programme est incorporé, le ou les circuits étant adaptés pour exécuter ou pour être utilisé dans l'exécution du procédé précité.

[0043] Selon un exemple de réalisation, la présente technique est mise en œuvre au moyen de composants logiciels et/ou matériels. Dans cette optique, le terme "module" peut correspondre dans ce document aussi bien à un composant logiciel, qu'à un composant matériel ou à un ensemble de composants matériels et logiciels.

[0044] Un composant logiciel correspond à un ou plusieurs programmes d'ordinateur, un ou plusieurs sous-programmes d'un programme, ou de manière plus générale à tout élément d'un programme ou d'un logiciel apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Un tel composant logiciel est exécuté par un processeur de données d'une entité physique (terminal, serveur, passerelle, set-top-box, routeur, etc.) et est susceptible d'accéder aux ressources matérielles de cette entité physique (mémoires, supports d'enregistrement, bus de communication, cartes électroniques d'entrées/sorties, interfaces utilisateur, etc.). Par la suite, on entend par ressources tous ensembles d'éléments matériels et/ou logiciels support d'une fonction ou d'un service, qu'ils soient unitaires ou combinés.

[0045] De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Il peut s'agir d'un composant matériel programmable ou avec processeur intégré pour l'exécution de logiciel, par exemple un circuit intégré, une carte à puce, une carte à mémoire, une carte électronique pour l'exécution d'un micrologiciel (« firmware » en anglais), etc.

[0046] Chaque composante du système précédemment décrit met bien entendu en œuvre ses propres modules logiciels.

[0047] Les différents modes de réalisation mentionnés ci-dessus sont combinables entre eux pour la mise en œuvre de la présente technique.

Brève description des dessins

[0048] D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

[Fig.1] la [Fig.1] représente un système de gestion d'un profil utilisateur d'un équipement terminal dans un réseau de communication, conforme à l'invention dans un mode particulier de réalisation ;

[Fig.2] la [Fig.2] représente un exemple d'architecture d'un équipement terminal hébergeant un dispositif d'activation d'un profil utilisateur conforme à l'invention, dans un mode particulier de réalisation ;

[Fig.3] la [Fig.3] illustre, sous forme d'ordinogramme, les principales étapes d'un procédé d'activation d'un profil utilisateur selon l'invention, dans un mode particulier de réalisation.

[Fig.4] la [Fig.4] illustre, sous la forme d'un diagramme de flux, les messages échangés au sein du système de gestion d'un profil utilisateur selon l'invention, dans un mode particulier de réalisation ; et

[Fig.5] la [Fig.5] représente, de façon schématique, un exemple de fichier listant des informations relatives à des instructions de code de programme accessibles par un dispositif d'activation d'un profil utilisateur conforme à l'invention, dans un mode de réalisation.

[Fig.6] la [Fig.6] représente, de façon schématique, un exemple d'architecture matérielle d'un dispositif d'activation d'un profil utilisateur selon l'invention, dans un mode particulier de réalisation.

Description de l'invention

[0049] L'invention concerne l'activation d'un profil utilisateur généré par un opérateur d'un réseau de communication suite à la souscription par un utilisateur d'un abonnement à un service fourni par ce réseau. Le principe de l'invention consiste à déclencher, sur instruction de l'utilisateur en réponse à un identifiant d'accès à des instructions de code de programme reçues au cours d'une session de communication établie avec le réseau de communication, le chargement et l'exécution automatique de ces instructions de code de programme sur l'équipement terminal, lesdites instructions de code de programme étant configurées pour commander au module sécurisé de gestion des profils de cet équipement terminal d'obtenir le profil utilisateur du réseau de communication et de le stocker dans ce module sécurisé. De la sorte, l'utilisateur n'a pas à sortir du contexte applicatif dans lequel il a obtenu l'identifiant d'accès de la part du réseau de communication et par exemple effectué sa démarche de souscription. La seule opération qu'il doit effectuer est de répondre à une requête d'accès à ces instructions de code de programme, par exemple en cliquant sur un lien vers une adresse de type URL.

[0050] La finalisation du parcours de souscription d'un utilisateur à un service d'un réseau de communication d'un opérateur s'en trouve donc simplifié et fluidifié.

[0051] La [Fig.1] représente, dans son environnement, un système S de gestion d'un profil utilisateur conforme à l'invention, dans un mode particulier de réalisation.

[0052] Un tel système S comprend un équipement terminal UE d'un utilisateur UT, par exemple de type téléphone intelligent (en anglais, « smartphone ») ou ordinateur personnel (en anglais, « laptop ») ou encore tablette, connecté à un réseau de communication RC d'un opérateur par le biais d'un équipement d'accès AP (en anglais, « Access Point »). Ce point d'accès AP1, AP2 peut aussi bien mettre en œuvre une technologie filaire que sans fil, Wi-Fi (AP1) ou radio cellulaire (AP2) par exemple.

[0053] On suppose que l'équipement terminal UE est équipé d'un module sécurisé eUICC/eSIM et que son utilisateur UT a initié une démarche de souscription à une offre de

service de communication fourni par le réseau de communication RC. Pour ce faire, il a établi une session de communication avec une plateforme de gestion de clientèle du réseau de communication RC configurée pour gérer avec l'utilisateur notamment le choix d'une offre commerciale, le paiement, la saisie des informations clients et la création d'un compte client. Par exemple, cette plateforme comprend un serveur Web avec lequel l'utilisateur communique via un navigateur Web de son équipement terminal. En variante, il a initié une discussion avec un agent conversationnel de cette plateforme dans un contexte applicatif de messagerie instantanée.

[0054] Le réseau de communication RC comprend aussi un serveur SMDP+ de gestion des souscriptions configuré pour préparer un profil utilisateur correspondant à l'offre commerciale choisie par l'utilisateur, le stocker et le fournir au module sécurisé eUICC/ eSIM de son équipement terminal.

[0055] En relation avec la [Fig.2], l'équipement terminal UE comprend un module sécurisé eUICC de gestion des profils utilisateurs de réseaux de communications mobiles. Son accès est protégé par une interface API_LPA gérée par une application logicielle LPA. Cette application LPA appartient à une classe d'applications, appelée classe « EUICCManager », autorisées à gérer ce type d'interface. Cette application LPA est configurée pour n'autoriser le stockage d'un profil utilisateur dans le module eSIM que s'il est associé à un certificat de l'opérateur qui l'a généré (« carrier privilege »). Ce certificat de l'opérateur est ajouté par le système d'information du réseau en question au moment de la génération du profil utilisateur, dans un champ d'information appelé privilège de l'opérateur (en anglais, « carrier privilege »), compris dans des métadonnées associées à ce profil utilisateur. En variante, il peut être ajouté au moment de la mise à disposition de ce profil dans l'équipement serveur SMDP+, en vue de son téléchargement par l'équipement terminal UE de l'utilisateur.

[0056] De même, seules les applications logicielles compilées et signées avec ce même certificat de l'opérateur sont autorisées par l'application LPA à piloter le profil utilisateur via l'interface LPA_API) et notamment à réaliser des opérations liées à ce profil utilisateur dans le module eUICC, telles que son chargement, son activation, sa désactivation ou encore sa suppression. Il s'agit donc nécessairement d'applications logicielles dont l'opérateur est propriétaire (en anglais, « carrier application ») et qui sont configurées pour communiquer avec un contrôleur dédié (en anglais « EuiccController ») du système d'exploitation OS de l'équipement terminal UE.

[0057] Ce mécanisme, mis en œuvre par le système d'exploitation OS, notamment Android ®, de l'équipement terminal UE, permet d'accorder des privilèges spéciaux aux opérateurs propriétaires d'applications de cartes de circuit intégré universelle (UICC) et maintenant de module eUICC et leur offre donc un moyen sûr et flexible de gérer leurs applications propriétaire (hébergées sur des canaux de distribution d'applications gé-

nériques (tels que Google Play) tout en conservant des privilèges spéciaux sur les équipements terminaux et sans le besoin de préinstaller ces applications en tant qu'applications système.

[0058] En relation avec la [Fig.2], l'équipement terminal comprend en outre un dispositif 100 d'activation d'un profil utilisateur dans un équipement terminal, ledit profil utilisateur ayant été généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication lorsqu'il est stocké dans un module sécurisé de l'équipement terminal. Selon l'invention, le dispositif 100 est configuré pour mettre en œuvre la réception REC, au cours d'une session de communication établie entre l'équipement terminal UE et ledit réseau RC, d'un identifiant d'accès à des instructions de code de programme, la détection DET d'une sélection par l'utilisateur dudit identifiant, suite à cette détection, l'émission REQ_APP à destination dudit réseau d'une demande d'accès audit code de programme, la réception REC_APP en provenance dudit réseau des instructions de code de programme et d'une information cryptographique signant lesdites instructions de code de programme, l'exécution EXC desdites instructions de code de programme, comprenant l'émission d'une commande d'obtention et de stockage dudit profil utilisateur audit module, ledit profil utilisateur étant stocké dans le module sécurisé suite à la vérification CHK que l'information cryptographique signant les instructions de code de programme ont été obtenues à partir d'un même certificat de l'opérateur que ledit profil utilisateur. Le dispositif 100 met ainsi en œuvre le procédé d'activation d'un profil utilisateur dans un équipement terminal selon l'invention qui sera détaillé ci-après en relation avec la [Fig.3].

[0059] Dans l'exemple de réalisation de la [Fig.2], le dispositif 100 est intégré dans l'équipement terminal UE. Alternativement, le dispositif 100 peut être indépendant de l'équipement terminal UE mais connecté à celui-ci par une liaison quelconque, filaire ou non.

[0060] Le dispositif 100 comprend aussi une mémoire M1, dans laquelle il stocke les informations qu'il reçoit du réseau, comme par exemple l'identifiant d'accès à des instructions de code de programme ou les instructions de code de programme elles-mêmes. Il peut y stocker aussi des informations reçues de l'utilisateur via une interface utilisateur UI, comme par exemple des instructions ou commandes. Avantageusement, le dispositif 100 utilise des ressources de l'équipement terminal UE dans lequel il est embarqué, comme par exemple une interface utilisateur (écran tactile), une mémoire etc.

[0061] En relation avec la [Fig.3], on présente désormais les étapes d'un procédé d'activation d'un profil utilisateur dans un équipement terminal selon un mode de réalisation de l'invention. On suppose ici que cet équipement terminal UE est équipé d'un

module sécurisé de gestion des profils utilisateurs, de type eSIM ou eUICC, et qu'il héberge un dispositif 100 mettant en œuvre le procédé d'activation d'un profil utilisateur de l'invention.

[0062] A titre illustratif, on considère le cas d'un utilisateur UT qui vient de souscrire à une offre de service de l'opérateur du réseau de communication RC. En 30, une information d'identification d'd'accès à des instructions de code de programme est reçu au cours d'une session de communication établie entre l'équipement terminal UE et le réseau de communication RC. Par exemple, cette session de communication est établie avec un équipement du réseau de l'opérateur, au sein d'une application logicielle installée sur l'équipement terminal, par exemple un navigateur web ou une application de messagerie instantanée.

[0063] En 31, l'application logicielle en question demande à l'utilisateur UT via une interface utilisateur UI s'il souhaite accéder à ces instructions de code de programme. Par exemple, l'information d'identification d'accès reçue est une URL que l'application logicielle affiche sur l'écran tactile de l'équipement terminal UE comme un lien hypertexte. En variante, l'affichage prend la forme d'un bouton ou d'une icône à cliquer.

[0064] En 32, suite à la détection d'une action de l'utilisateur qui correspond à une sélection de ladite information d'identification d'accès, une demande d'accès auxdites instructions de code de programme est émise en 33 à destination du réseau de communication RC. Par exemple l'utilisateur UT a cliqué sur le lien ou le bouton affiché sur l'écran tactile de l'équipement terminal UE.

[0065] En 34, les instructions INST de code de programme sont reçues par l'équipement terminal UE ainsi qu'une information cryptographique IC signant lesdites instructions de code de programme.

[0066] En 35, les instructions de code de programme sont exécutées, ce qui déclenche l'émission d'une commande d'obtention et de stockage d'un profil utilisateur UP au module sécurisé eUICC/eSIM de l'équipement terminal UE. Plus précisément, c'est l'interface LPA_API qui obtient ledit profil utilisateur UP auprès du réseau RC et vérifie, à partir de métadonnées associées auprofil utilisateur UP, qu'elles comprennent une marque correspondant au même certificat de l'opérateur que celui qui a servi à signer les instructions de code de programme en cours d'exécution. Une fois cette vérification effectuée, l'interface LPA_API commande le chargement du profil utilisateur UP dans le module sécurisé et valide son activation. En effet, le module sécurisé eSIM/eUICC pouvant stocker plusieurs profils utilisateurs, il est nécessaire d'activer un des profils utilisateurs stockés et, à l'heure actuelle, un seul peut être actif à la fois. Ce n'est qu'à la fin de ce processus de validation que le profil utilisateur UP est mis à disposition de l'équipement terminal pour qu'il puisse accéder au(x) services de

l'opérateur.

[0067] Selon un mode de réalisation de l'invention, les instructions de code de programme en question sont celles d'une application logicielle instantanée INST_APP1. Par définition, l'application logicielle instantanée INST_APP1 est liée ou adossée à une application logicielle native APP1. Plus précisément, les instructions de code de programme de l'application instantanée INST_APP1 correspondent généralement à une sous-partie des instructions de code de programme de cette application native APP1, cette sous-partie permettant la mise en œuvre d'une partie des fonctionnalités de l'application logicielle native APP1. En l'espèce, la fonctionnalité est la gestion (stockage, activation, désactivation, suppression) d'un profil utilisateur dans le module eUICC/eSIM de l'équipement terminal UE. Selon une première option, l'application logicielle native APP1 en question est une application propriétaire de l'opérateur du réseau RC, dédiée à la mise en en œuvre de cette fonctionnalité, c'est-à-dire que l'application instantanée INST_APP1 et son application native APP1 réalisent la même fonctionnalité. En variante, APP1 est une application logicielle plus générique de gestion des offres de service d'un utilisateur qui est enrichie d'autres fonctionnalités que celle de gestion du module eUICC, liées par exemple à un suivi de consommation de l'utilisateur, la possibilité de souscrire à d'autres offres, etc. On comprend qu'un avantage de l'application instantanée INST_APP1 est qu'elle réalise les seules fonctions requises pour l'activation du profil utilisateur UP. Elle reste donc la plus légère possible.

[0068] Contrairement à l'application logicielle native qui nécessite plusieurs actions volontaires consécutives de la part de l'utilisateur pour s'exécuter sur son équipement terminal, à savoir la télécharger depuis un magasin d'application logicielles, puis l'installer sur l'équipement terminal UE et enfin fournir un couple d'identifiant/mot de passe de l'utilisateur pour accéder à un compte de l'utilisateur auprès de l'opérateur, l'application instantanée INST_APP1 bénéficie d'une mise en œuvre allégée : elle peut être téléchargée et exécutée automatiquement sur l'équipement terminal UE dès lors que l'utilisateur UT a sélectionné l'information d'identification d'accès aux instructions de code de programme de cette application instantanée INST_APP1.

[0069] Avantageusement, l'application instantanée INST_APP1 est signée avec le même certificat de l'opérateur (« carrier privilege ») que l'application logicielle native APP1. De la sorte, elle hérite des mêmes droits d'accès ou privilèges que l'application native APP1, ce qui lui permet d'accéder au module eUICC/eSIM de l'équipement terminal, au même titre que l'application native dont elle dépend.

[0070] Selon ce mode de réalisation de l'invention, la réponse à la demande d'accès auxdites instructions de code de programme émise en 33 à destination du réseau de communication RC, permet au dispositif 100 d'obtenir un identifiant de groupe BDL_ID1 de

ladite application instantanée et la première information cryptographique MQ_CP1. Les instructions de code de programme de l'application instantanée INST_APP1 sont obtenue à partir de cet identifiant de groupe, puis chargées dans une mémoire de l'équipement terminal, à partir de l'identifiant de groupe de l'application. La première information cryptographique est utilisée pour vérifier que les instructions de code de programme reçues ont bien été signées avec le certificat de l'opérateur qui a permis d'obtenir cette première information cryptographique.

[0071] En relation avec **la** [Fig.4], on présente désormais les échanges de messages entre l'équipement terminal et le réseau de communication lors de la mise en œuvre du procédé d'activation d'un profil utilisateur qui vient d'être décrit, selon un exemple de de réalisation de l'invention.

[0072] On suppose ici que l'utilisateur UT a souscrit à une offre de service de l'opérateur du réseau RC en échangeant (étapes 1 et 2) avec un agent conversationnel BOT d'une plateforme de gestion de clientèle PGC de ce réseau, par exemple au cours d'une session de communication établie dans une application logicielle de type messagerie instantanée MSG_APP installée sur son équipement terminal UE (interface « MSG »). Des échanges de messages entre l'utilisateur et l'agent conversationnel de la plateforme de gestion de clientèle PGC ont conduit au choix par l'utilisateur UT de cette offre de service donnée, à la fourniture d'informations d'identifications et de paiement et à la création d'un compte client pour cet utilisateur. Toutes les informations fournies par l'utilisateur et collectées par la plateforme de gestion de clientèle PGC par l'intermédiaire de l'agent conversationnel sont enregistrées par le système d'information (non représenté) du réseau de communication RC. Parmi ces informations, on compte en particulier une information relative à un type de support du profil utilisateur dans l'équipement utilisateur UE, qui indique donc que l'équipement terminal UE est équipé d'un module sécurisé eUICC/eSIM plutôt que d'une carte UICC/SIM amovible classique.

[0073] Au cours d'une étape 3, la plateforme de gestion de clientèle PGC commande à une plateforme SMDP+ de gestion des souscription utilisateurs du réseau RC de préparer le profil utilisateur UP correspondant à l'offre de service choisie par l'utilisateur. Une fois ce profil utilisateur UP prêt, la plateforme SMDP+ transmet à la plateforme de gestion de clientèle PGC une information d'identification de correspondance du profil utilisateur avec l'utilisateur MUT_ID (en anglais, « Matching ID ») et une information d'identification d'accès au profil utilisateur, par exemple de type URL (URL_UP). Par exemple, l'information MUT_ID d'identification de correspondance du profil utilisateur à avec l'utilisateur a la forme suivante :

matchingId : exemple "97582923-1490-6110-8712-683344602712",

et l'information URL_UP d'identification d'accès au profil utilisateur UP a la forme

suivante : "sm-v4-009-xxppa-gtm.pr.go-esim.com".

[0074] Ces deux informations MUT_ID, URL_UP sont destinées à être utilisées par la plateforme PGC pour générer une information de code d'activation (en anglais, « activation code ») AC_CD. Par exemple, le code d'activation AC_CD a la forme suivante :
« 1$SMDP.GSMA.COM$04386-AGYFT-A74Y8-3F815$1.3.6.1.4.1.31746 ».

[0075] Cette information de code d'activation AC_CD est destinée à être transmise à l'équipement terminal afin qu'une application de gestion du module sécurisé eSIM/ eUICC en déduise l'information d'identification d'accès URL_UPau profil utilisateur et l'information d'identification de correspondance du profil MUT_ID.

[0076] La génération de ce code d'activation est par exemple décrite dans la spécification technique intitulée « SGP 22 -RSP Technical Specification », Version 2.201, publiée en septembre 2017 par l'association GSMA (de l'anglais, « Global System for Mobile Communications »).

[0077] La plateforme de gestion de clientèle PGC obtient du système d'information du réseau RC, au cours d'une étape 4, une information d'identification d'accès à des instructions de code de programme configurées pour commander le chargement et le stockage du profil utilisateur UP dans le module sécurisé eUICC/eSIM de l'équipement terminal UE. Cette information d'identification d'accès est personnalisée pour l'utilisateur, de sorte qu'il soit le seul à pouvoir accéder aux instructions de code de programme à partir de cette information d'accès. Autrement dit, elle comprend une information d'autorisation de l'utilisateur. Par exemple, cette information d'autorisation est de type jeton TK1 (en anglais, « token ») à usage unique et elle est assortie d'une période de validité, qui doit être suffisamment courte pour des raisons évidentes de sécurité et par exemple égale à 1h. L'information d'identification d'accès reçue est par exemple une URL (URL_PRG) qui pointe sur une ressource stockée dans un équipement serveur web ESW du réseau de communication RC de l'opérateur. A réception de cette URL en 30, par exemple de la part de l'agent conversationnel BOT, l'équipement terminal UE affiche en 31 un lien ou un bouton sur lequel l'utilisateur peut cliquer pour requérir l'accès aux instructions de code de programme. Avantageusement, on suppose ici que l'équipement terminal UE affiche ce lien/bouton cliquable dans une interface utilisateur UI déjà active mise en œuvre par la session de communication avec l'agent conversationnel établie par l'application MSG_APP. De la sorte, l'utilisateur UT n'a pas d'autre action à mener que celle de cliquer sur le lien/ bouton, pour accéder aux instructions de code de programme. En particulier, il n'a pas à sortir du contexte de l'application logicielle MSG_APP qu'il utilise pour communiquer avec l'agent conversationnel BOT.

[0078] Au cours d'une étape 5, on suppose que l'utilisateur clique sur le lien/bouton pour

requérir l'accès aux instructions de code de programme et que cette action, détectée en 32, déclenche l'accès à l'URL par le navigateur Web (interface WEB) de l'équipement terminal qui se lance automatiquement.

[0079] Au cours d'une étape 6, le navigateur WEB de l'équipement terminal UE transmet la requête d'accès à l'URL à une autre application logicielle native de l'équipement terminal qui est l'application cliente d'accès STR_APP à un serveur de gestion, aussi appelé magasin, d'applications logicielles, par exemple de type Google Play ®. Au cours de l'étape 7, l'application cliente STR_APP obtient de l'équipement serveur ESW, à partir de l'URL, un fichier FL comprenant une liste de N programmes informatiques, avec N entier non nul, qui sont stockés dans le magasin d'applications STR. Il s'agit par exemple d'un fichier FL de type fichier /.well-known/AssetLinks.json, qui liste des applications instantanées gérées par l'opérateur du réseau de communication RC. Dans ce fichier FL, comme illustré par la [Fig.5], chaque application instantanée disponible est indexée par une information d'identification d'accès URL_PRGi, typiquement l'URL précédente ou une partie de l'URL précédente, à laquelle sont associées une première information d'identification de groupe BDL_IDi des instructions de code de programme PRGi, par exemple ici une application instantanée (en anglais, « bundle or package ID ») et une première empreinte ou marque MQ_CPi d'un certificat de l'opérateur utilisé pour signer l'application instantanée en question. Par exemple, il s'agit d'un haché de type SHA1 de ce certificat. Dans la suite, on désigne par INST_APP1 l'application logicielle désignée par l'URL URL_PRG1 reçue par l'équipement terminal UE. Dans le fichier FL, elle est associée à l'information d'identification de groupe BDL_ID1 et à la marque ou première information cryptographique MQ_CP1. Dans cet exemple, il s'agit d'une application logicielle instantanée adossée à une application logicielle native APP1 de l'opérateur du réseau de communication RC.

[0080] Au cours d'une étape 8, l'application cliente STR_APP interroge le magasin d'applications logicielles STR à partir de l'URL précédente URL_PRG1 et obtient une deuxième information d'identification de groupe (« Bundle ID ») de l'application logicielle INST_APP1 correspondant à l'URL transmise. Elle vérifie que la deuxième information d'identification de groupe correspond à la première qu'elle a obtenu du fichier /.well-known/AssetLinks.json. Si c'est le cas, elle interroge en 9 le magasin d'applications logicielles STR pour obtenir une deuxième marque de certificat utilisé pour signer l'application logicielle INST_APP1. Elle vérifie que cette deuxième marque correspond à la première obtenue dans le fichier. Si c'est bien le cas, elle lance le téléchargement de l'application logicielle instantanée INST_APP1 du magasin STR sur l'équipement terminal UE qui la reçoit en 34.

[0081] L'application instantanée INST_APP1 s'exécute donc en 35 sur l'équipement

terminal UE. Au cours de cette exécution, elle récupère l'information d'identification d'accès (URL_PRG) initialement obtenue de la plateforme de gestion de clientèle PGC, qui comprend l'information d'autorisation ou jeton TK1 propre à l'utilisateur. Elle utilise en 11 ce jeton TK1 pour obtenir de la plateforme PGC du réseau de communication RC une information qui lui permettra d'accéder au profil utilisateur UP dans le réseau RC. Dans ce mode de réalisation, il s'agit d'une information de code d'activation AC_CD qui a été générée elle-aussi par le système d'information du réseau de communication RC, spécifiquement pour l'utilisateur UT.

[0082] En 12, l'application instantanée INST_APP1 reçoit de la plateforme PGC l' information de code d'activation AC_CD, associée au profil utilisateur de l'utilisateur UT. Elle a été générée pour permettre à l'équipement terminal UE (et en particulier à l'application LPA) d'obtenir au moins l'information d'identification d'accès à un équipement serveur URL_UP du réseau RC qui stocke le profil utilisateur et l'information d'identification ID_UP de ce profil utilisateur (étape 3).

[0083] En 13, l'application INST_APP1 demande l'accès au module sécurisé de gestion des profils utilisateurs eUICC/eSIM à l'application LPA via l'interface sécurisée LPA_API, à l'aide d'une requête comprenant l'information de code d'activation AC_CD. L'application LPA traite la demande d'accès et demande à l'utilisateur une autorisation d'accès, via une interface utilisateur de l'équipement terminal UE, par exemple en lançant automatique une fenêtre d'affichage de type « pop-up ».

[0084] En 14, l'application LPA se connecte à la plateforme de gestion des souscriptions SMDP+, dont elle a récupéré l'adresse (ou information d'identification d'accès URL_UP) à partir de l'information de code d'activation AC_CD et requiert l'obtention du profil utilisateur UP identifié par l'information d'identification ID_UP obtenue elle aussi à partir de l'information de code d'activation. L'application LPA télécharge le profil utilisateur UP. Elle obtient des métadonnées associées à ce profil utilisateur UP. Ces métadonnées comprennent notamment une marque MQ_CP_UP du certificat de l'opérateur utilisé pour signer le profil utilisateur UP.

[0085] En 15, l'application LPA vérifie dans les métadonnées que la marque du certificat correspond à celle de celui utilisé pour signer l'application instantanée INST_APP1. Si c'est bien le cas, l'application LPA valide le chargement ou l'approvisionnement (en anglais, « provisioning ») du module sécurisé eUICC/eSIM à l'aide du profil utilisateur UP. Avantageusement, elle peut vérifier aussi que les métadonnées du profil utilisateur UP comprennent la première information d'identification de groupe de l'application instantanée (Bundle ID). Pour une sécurité encore accrue, l'application LPA peut en outre requérir en 16 de l'utilisateur qu'il saisisse le code PIN d'accès à son module sécurisé eSIM. Par exemple, l'opérateur a préalablement fourni ce code PIN à l'utilisateur, par exemple au cours des échanges avec l'agent conversationnel ou via

l'application instantanée ou encore par un autre canal de communication (Email ou autre).

[0086] En 17, lorsque le cas échéant le code PIN a été saisi avec succès par l'utilisateur sur une interface utilisateur de son équipement terminal, l'application instantanée INST_APP1 active le profil utilisateur UP dans le module sécurisé eUICC/eSIM. Optionnellement, il requiert préalablement l'accord de l'utilisateur.

[0087] On présente désormais, en relation avec la [Fig.6] un exemple de structure matérielle du dispositif 100 permettant de mettre en œuvre les étapes du procédé d'activation d'un profil utilisateur dans un équipement terminal selon l'invention.

[0088] Le dispositif 100 comprend une mémoire vive 103 (par exemple une mémoire RAM), une unité de traitement 102 équipée par exemple d'un processeur μP, et pilotée par un programme d'ordinateur stocké dans une mémoire morte 101 (par exemple une mémoire ROM ou un disque dur). A l'initialisation, les instructions de code du programme d'ordinateur sont par exemple chargées dans la mémoire vive 103 avant d'être exécutées par le processeur de l'unité de traitement 102.

[0089] Cette [Fig.6] illustre seulement une manière particulière, parmi plusieurs possibles, de réaliser le dispositif 100 afin qu'il effectue les étapes du procédé d'activation d'un profil utilisateur (selon l'un quelconque des modes de réalisation et/ou variantes décrit(e)s ci-dessus en relation avec les figures 3 et 4). En effet, ces étapes peuvent être réalisées indifféremment sur une machine de calcul reprogrammable (un ordinateur PC, un processeur DSP ou un microcontrôleur) exécutant un programme comprenant une séquence d'instructions, ou sur une machine de calcul dédiée (par exemple un ensemble de portes logiques comme un FPGA ou un ASIC, ou tout autre module matériel).

[0090] Dans le cas où le dispositif 100 est réalisé avec une machine de calcul reprogrammable, le programme correspondant (c'est-à-dire la séquence d'instructions) pourra être stocké dans un médium de stockage amovible (tel que par exemple un CD-ROM, un DVD-ROM, une clé USB) ou non, ce médium de stockage étant lisible partiellement ou totalement par un ordinateur ou un processeur.

[0091] Dans certains modes de réalisation, le dispositif 100 est inclus dans l'équipement terminal UE.

[0092] L'invention qui vient d'être présentée procure de nombreux avantages. Elle permet notamment à un utilisateur qui vient de souscrire à une offre d'un opérateur d'un réseau de communication mobile, de finaliser de façon simple et fluide son parcours de souscription. En effet, avec l'invention, l'utilisateur n'a pas besoin d'aller chercher une nouvelle application logicielle hébergée dans un magasin d'applications, ni d'entrer ses informations d'accès à un compte client, ni de scanner un QR code. Au contraire, il lui suffit de sélectionner une information d'identification d'accès reçue une fois l'offre

souscrite, via la même session de communication que celle utilisée pour communiquer avec la plateforme de gestion de clientèle de l'opérateur, et de se laisser guider.

[0093] Avec l'invention, les opérations de gestion du profil utilisateur (téléchargement, stockage, activation dans le module eUICC/eSIM) sont intégrées au parcours client et rendues « invisibles » pour l'utilisateur. Avantageusement, ce parcours client peut aussi prendre en charge des vérifications préalables, comme par exemple un test de l'éligibilité de l'équipement terminal, un test de connexion à un réseau de données, etc.

[0094] Ainsi, l'utilisateur n'a plus à gérer la réception ni la manipulation d'un QR code comprenant l'information d'identification d'accès à son profil utilisateur. L'invention contribue donc à simplifier les opérations à effectuer par l'utilisateur (sélectionner/autoriser et à les mettre la portée de tous les publics.

Revendications

[Revendication 1] Procédé d'activation d'un profil utilisateur dans un équipement terminal, ledit profil utilisateur ayant été généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication lorsqu'il est stocké dans un module sécurisé (eUICC/eSIM) de l'équipement terminal, ledit procédé étant caractérisé en ce qu'il est mis en œuvre dans l'équipement terminal et comprend :
- la réception (30), au cours d'une session de communication établie entre l'équipement terminal et ledit réseau, d'une information d'identification d'accès à des instructions de code de programme (URL_PRG1) configurées pour commander l'obtention dudit profil utilisateur (UP) dudit réseau et le stockage dudit profil utilisateur dans ledit module (eUICC/eSIM), lorsqu'elles s'exécutent sur ledit équipement terminal;
- suite à la détection (32) d'une sélection par l'utilisateur de l'information d'identification d'accès, l'émission (33) à destination dudit réseau d'une demande d'accès auxdites instructions de code de programme à partir de ladite information d'identification d'accès (URL_PRG1);
- la réception (34) en provenance dudit réseau des instructions de code de programme et d'une première information cryptographique (MQ_CP1) signant lesdites instructions de code de programme ;
- l'exécution (35) desdites instructions de code de programme, comprenant l'émission d'une commande d'obtention et de stockage dudit profil utilisateur audit module, ledit profil utilisateur étant stockée dans ledit module sécurisé, après vérification que la première information cryptographique (MQ_CP1) signant les instructions de code de programme a été obtenue à partir d'un même certificat de l'opérateur que ledit profil utilisateur (UP).

[Revendication 2] Procédé d'activation d'un profil utilisateur selon la revendication 1, caractérisé en ce que lesdites instructions de code de programme sont comprises dans une application logicielle, dite application instantanée (INST_APP1), et correspondent à une partie des instructions de code de programme d'une autre application logicielle, dite application native (APP1), ladite application native n'étant pas exécutée au cours de la session de communication.

[Revendication 3] Procédé d'activation d'un profil utilisateur selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend l'émission d'une représentation de l'information d'identification d'accès (URL_PRG1) reçue à l'utilisateur sur une interface utilisateur mise en œuvre au cours de la session de communication et en ce que ladite sélection de l'information d'identification d'accès par l'utilisateur est détectée sur ladite interface utilisateur.

[Revendication 4] Procédé d'activation d'un profil utilisateur d'un équipement terminal, selon l'une quelconques des revendications 2 et 3, caractérisé en ce qu'il comprend :
- l'obtention d'un identifiant de groupe (BDL_ID1) de ladite application instantanée et de ladite première information cryptographique (MQ_CP1) à partir de l'information d'identification d'accès (URL_PRG1);
- l'obtention et le chargement des instructions de code de programme de l'application instantanée dans une mémoire de l'équipement terminal, à partir de l'identifiant de groupe de l'application, et
- la vérification que les instructions de programme reçues sont associées à ladite première information cryptographique.

[Revendication 5] Procédé d'activation d'un profil utilisateur dans un équipement terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que l'exécution des instructions de code de programme déclenche l'obtention auprès d'un premier équipement serveur (PGC) du réseau de communication (RC) d'une information d'identification du profil utilisateur (ID_UP) et d'une information d'identification d'accès (URL_UP) à un deuxième équipement serveur (SMDP+) stockant ledit profil utilisateur, l'envoi desdites informations audit module sécurisé dans un message de commande de chargement dudit profil utilisateur, l'obtention par une interface (LP_API) dudit module sécurisé dudit profil utilisateur (UP) et d'au moins une information de description associée, ladite information de description associée comprenant une deuxième information cryptographique (MQ_CP_UP), ladite deuxième information cryptographique signant le profil utilisateur étant utilisée pour vérifier que la première information cryptographique signant les instructions de code de programme a été obtenue à partir du même certificat de l'opérateur que la deuxième information cryptographique.

[Revendication 6] Dispositif (100) d'activation d'un profil utilisateur dans un équipement terminal, ledit profil utilisateur ayant été généré par un réseau de com-

munication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication lorsqu'il est stocké dans un module sécurisé (eUICC/eSIM) de l'équipement terminal, ledit dispositif étant configuré pour mettre en œuvre au sein de l'équipement terminal :
- la réception (REC), au cours d'une session de communication établie entre l'équipement terminal et ledit réseau, d'une information d'identification d'accès à des instructions de code de programme configurées pour commander l'obtention dudit profil utilisateur dudit réseau et le stockage dudit profil utilisateur dans ledit module (eUICC/eSIM), lorsqu'elles s'exécutent sur ledit équipement terminal;
- suite à la détection (DET) d'une sélection par l'utilisateur de l'information d'identification d'accès, l'émission (REQ_APP) à destination dudit réseau d'une demande d'accès auxdites instructions de code de programme à partir de ladite information d'identification d'accès ;
- la réception (REC_APP) en provenance dudit réseau des instructions de code de programme et d'une information cryptographique (IC) signant lesdites instructions de code de programme ;
- l'exécution (EXC) desdites instructions de code de programme, configurée pour déclencher l'émission d'une commande d'obtention et de stockage dudit profil utilisateur audit module, ledit profil utilisateur étant stockée dans ledit module sécurisé, après vérification (CHK) que la première information cryptographique signant les instructions de code de programme ont été obtenues à partir d'un même certificat de l'opérateur que ledit profil utilisateur.

[Revendication 7] Equipement terminal (UE)comprenant un module (eUICC/eSIM) de gestion d'au moins un profil utilisateur généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication lorsqu'il est stocké dans ledit module sécurisé (eUICC/eSIM), caractérisé en ce qu'il comprend un dispositif (100) d'activation d'un profil utilisateur selon la revendication 6.

[Revendication 8] Système (S) de gestion d'un profil utilisateur généré par un réseau de communication mobile d'un opérateur et comprenant des informations permettant l'accès de l'utilisateur à au moins un service dudit réseau de communication, lorsqu'il est stocké dans un module sécurisé de gestion de profils utilisateur d'un équipement terminal (UE), caractérisé en ce

qu'il comprend un équipement terminal (UE) d'un utilisateur, un dispositif (100) d'activation d'un profil utilisateur selon la revendication 6, un premier équipement serveur (PGC) du réseau de communication configuré pour gérer l'accès par l'équipement terminal (UE) à des instructions de code de programme configurées pour commander l'obtention dudit profil utilisateur dudit réseau et le stockage dudit profil utilisateur dans ledit module (eUICC/eSIM) et un deuxième équipement serveur (SMDP+) configuré pour gérer l'accès de l'équipement utilisateur audit profil utilisateur (UP).

[Revendication 9] Produit programme d'ordinateur comprenant des instructions de code de programme pour la mise en œuvre d'un procédé d'activation selon l'une quelconque des revendications 1 à 5, lorsqu'il est exécuté par un processeur.

[Fig. 1]

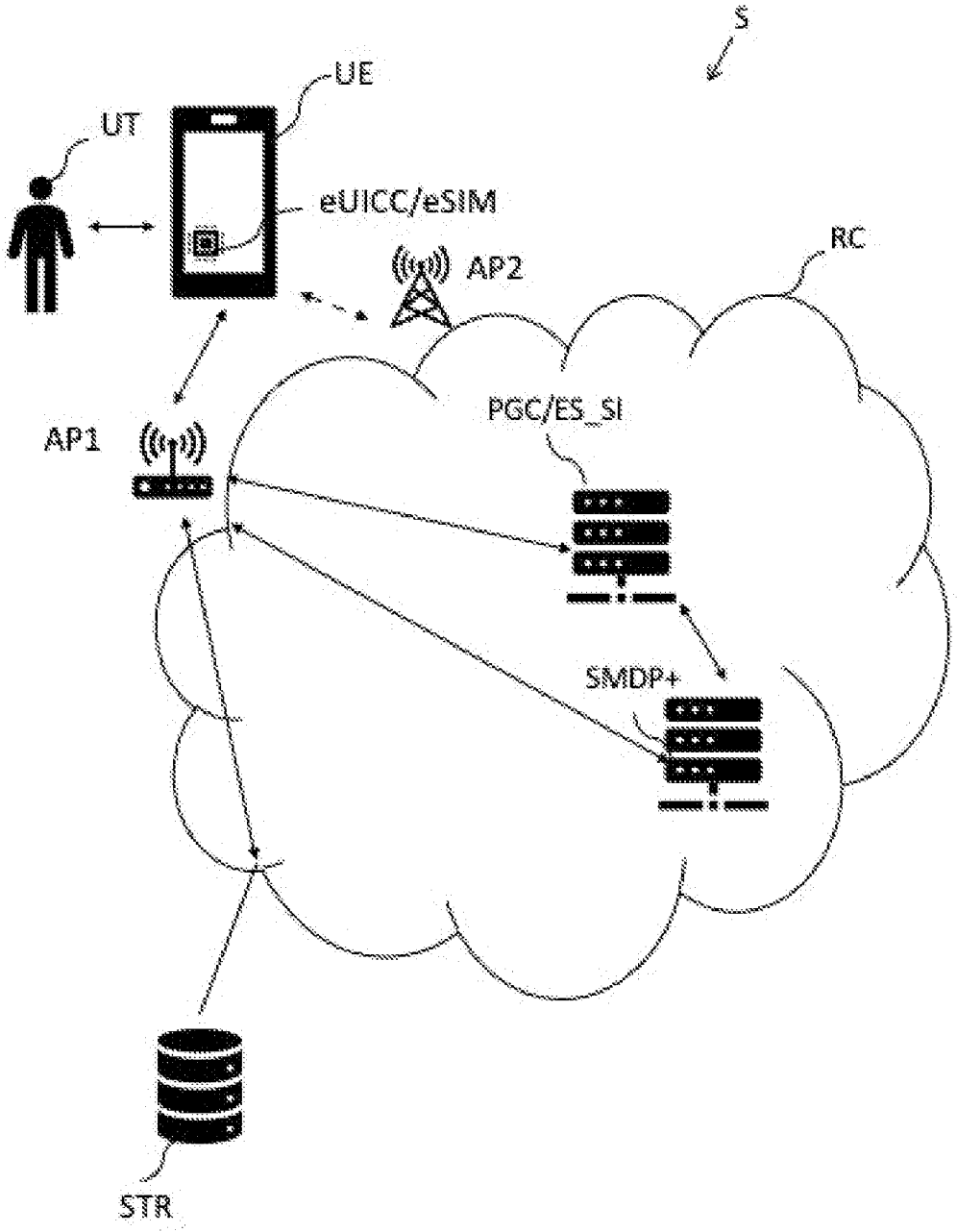


Fig. 1

[Fig. 2]

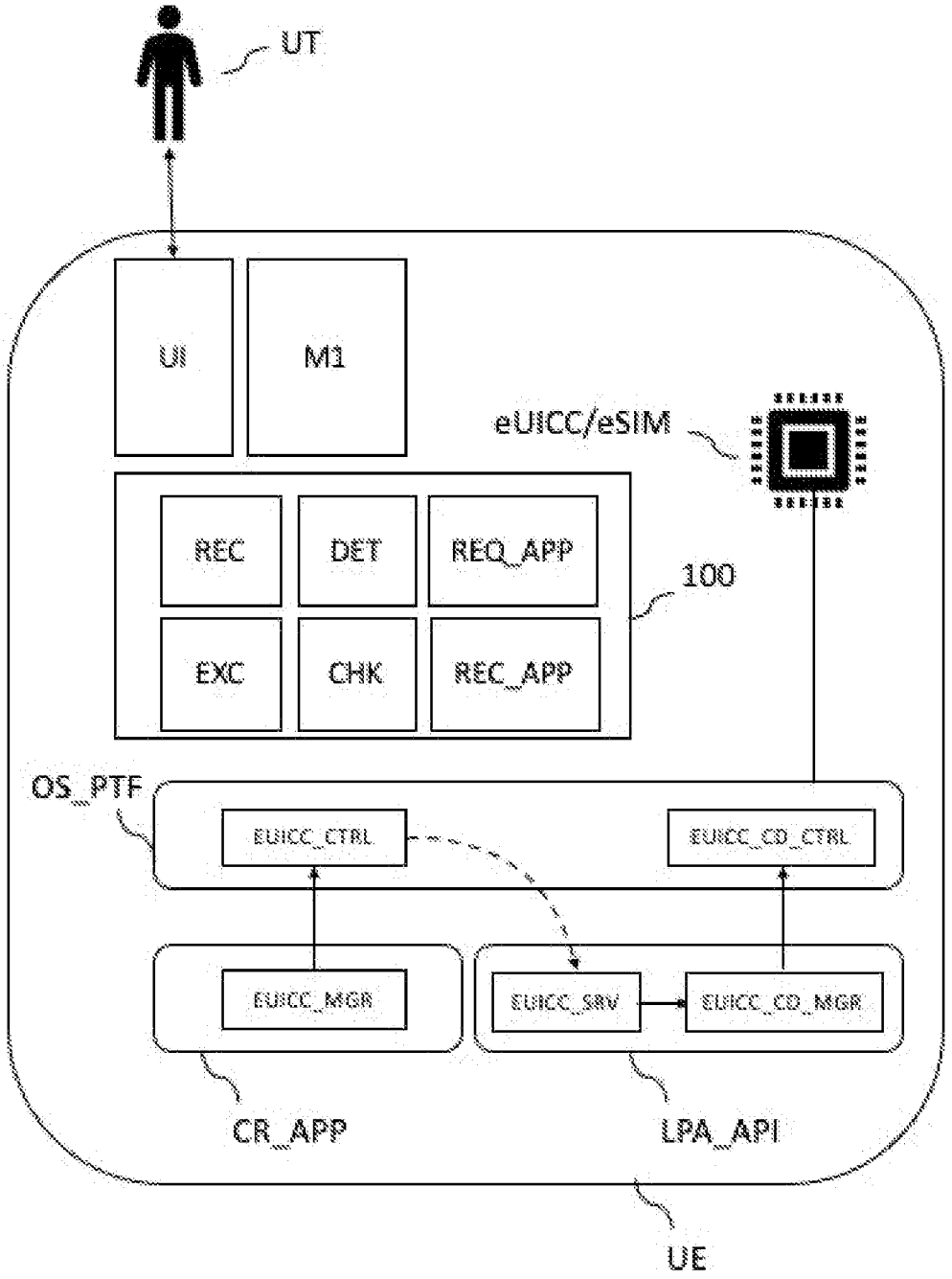

UT
UI
M1
eUICC/eSIM
REC
DET
REQ_APP
EXC
CHK
REC_APP
100
OS_PTF
EUICC_CTRL
EUICC_CD_CTRL
EUICC_MGR
EUICC_SRV
EUICC_CD_MGR
CR_APP
LPA_API
UE

Fig. 2

[Fig. 3]

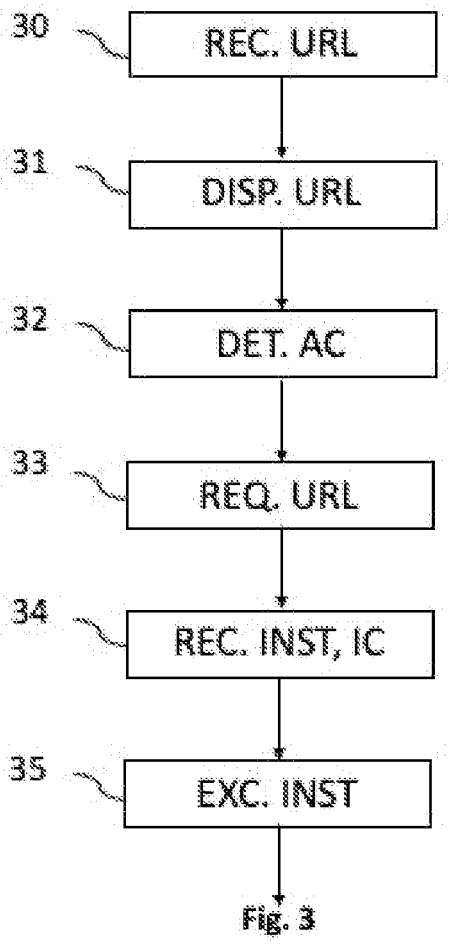

30
REC. URL
31
DISP. URL
32
DET. AC
33
REQ. URL
34
REC. INST, IC
35
EXC. INST

Fig. 3

[Fig. 4]

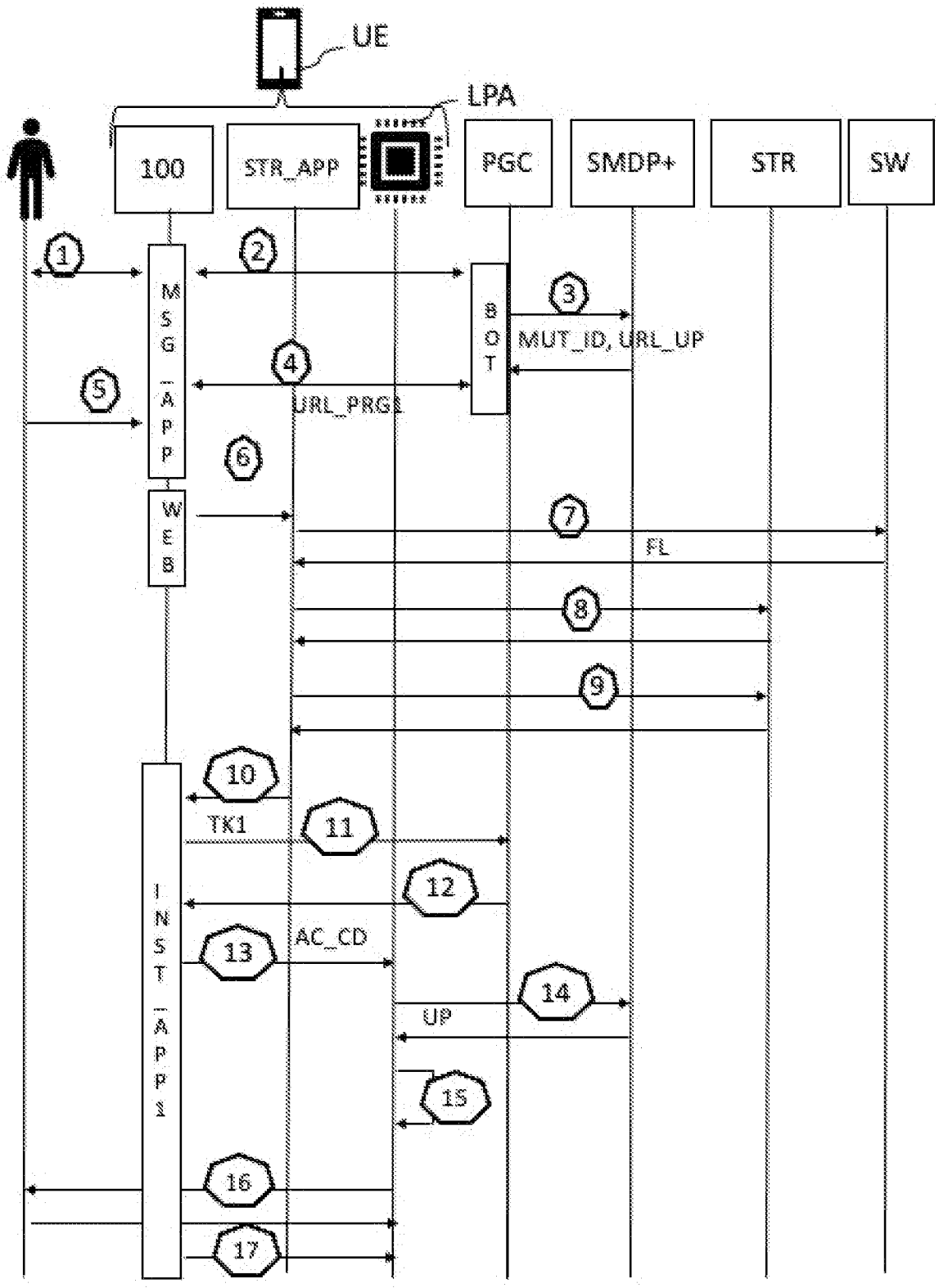

UE
LPA
100
STR_APP
PGC
SMDP+
STR
SW
MSG IAPP
BOT
WEB
INST IAPPS
MUT_ID, URL_UP
URL_PRG
FL
TK1
AC_CD
UP
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

Fig. 4

[Fig. 5]

URL_PRG1	BDL_ID1	MQ_CP1
URL_PRG2	BDL_ID2	MQ_CP2
URL_PRG3	BDL_ID3	MQ_CP3
...	...	...
URL_PRGN	BDL_IDN	MQ_CPN

FL

Fig. 5

[Fig. 6]

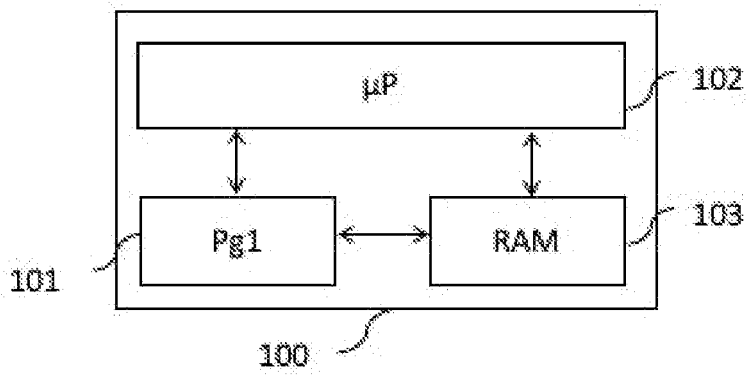


Fig. 6

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 906605
FR 2203269

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2020/112854 A1 (NAMIRANIAN BABAK [US]) 9 avril 2020 (2020-04-09) * alinéa [0024] - alinéa [0039] *	1-9	H04W8/20 H04W12/40 H04W12/069 H04W12/106
A	US 2018/302781 A1 (LEE HYE-WON [KR] ET AL) 18 octobre 2018 (2018-10-18) * alinéa [0078] - alinéa [0085] *	1-9	H04L9/32
A	US 2021/289360 A1 (PARK JUNG SIK [KR] ET AL) 16 septembre 2021 (2021-09-16) * alinéa [0101] - alinéa [0135] *	1-9	
A	US 2019/327605 A1 (FAN SHUNAN [CN] ET AL) 24 octobre 2019 (2019-10-24) * alinéa [0084] - alinéa [0126] *	1-9	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W

Date d'achèvement de la recherche	Examinateur
22 novembre 2022	Vadursi, Michele

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2203269 FA 906605

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **22-11-2022**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2020112854 A1	09-04-2020	CN 111010691 A	14-04-2020
		EP 3634021 A1	08-04-2020
		US 2020112854 A1	09-04-2020
US 2018302781 A1	18-10-2018	CN 108141747 A	08-06-2018
		EP 3337204 A1	20-06-2018
		KR 20170041597 A	17-04-2017
		US 2018302781 A1	18-10-2018
		WO 2017061800 A1	13-04-2017
US 2021289360 A1	16-09-2021	CN 109691151 A	26-04-2019
		CN 114697948 A	01-07-2022
		EP 3512224 A1	17-07-2019
		KR 20180028729 A	19-03-2018
		US 2019208405 A1	04-07-2019
		US 2021289360 A1	16-09-2021
		WO 2018048278 A1	15-03-2018
US 2019327605 A1	24-10-2019	CN 108353462 A	31-07-2018
		EP 3413685 A1	12-12-2018
		EP 3726868 A1	21-10-2020
		EP 3968677 A1	16-03-2022
		ES 2898302 T3	07-03-2022
		US 2019327605 A1	24-10-2019
		US 2020196131 A1	18-06-2020
		WO 2017147873 A1	08-09-2017