(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 144 733**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 14570**

(51) Int Cl[8] : ***H 04 W 4/60*** *(2023.01), H 04 W 4/50, 8/18, 12/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.12.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 05.07.24 Bulletin 24/27.

(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) :** *THALES Société anonyme* — FR et *THALES DIS FRANCE SA Société anonyme* — FR.

(72) **Inventeur(s) :** MINGARDON Sylvaine, SCHOLLER Franck et ANSLOT Michel.

(73) **Titulaire(s) :** THALES Société anonyme, THALES DIS FRANCE SA Société anonyme.

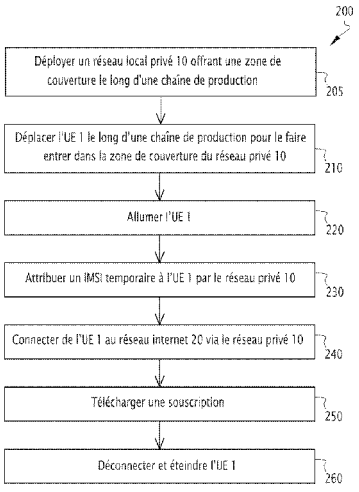
(74) **Mandataire(s) :** Lavoix.

(54) Procédé amélioré de provisionnement d'un équipement utilisateur avec un profil de souscription d'un opérateur final.

(57) Procédé amélioré de provisionnement d'un équipement utilisateur avec un profil de souscription d'un opérateur final

Ce procédé de provisionnement d'un équipement utilisateur avec une information d'un opérateur final, l'équipement utilisateur – UE étant muni d'une carte du type circuit intégré universelle embarquée – eUICC et d'un module radio, est caractérisé par: déployer (205) un réseau de téléphonie mobile privé, connecté à un réseau IP hébergeant un serveur mémorisant ladite information; attribuer (230) dynamiquement, par un équipement de gestion d'identifiants du réseau de téléphonie mobile privé, au moins un identifiant d'abonnement temporaire (IMSI) à l'eUICC résidant dans l'UE; connecter (240) l'UE au réseau IP via le réseau de téléphonie mobile privé en utilisant ledit au moins un identifiant d'abonnement temporaire; télécharger (250) ladite information auprès du serveur; et, déconnecter (260) l'UE.

Figure pour l'abrégé: Figure 3



FR 3 144 733 - A1

Description

Titre de l'invention : Procédé amélioré de provisionnement d'un équipement utilisateur avec un profil de souscription d'un opérateur final

[0001] La présente invention est relative aux procédés permettant le provisionnement d'un équipement utilisateur avec la souscription d'un opérateur dit « final ».

[0002] Un équipement équipé d'une interface de radiocommunication doit posséder une souscription auprès un opérateur final d'un réseau de téléphonie mobile pour pouvoir se connecter à ce réseau de téléphonie mobile afin d'accéder ensuite, en fonction des droits qui lui sont octroyés, aux services souhaités.

[0003] Pour charger cette souscription, l'équipement doit, dans une phase initiale, se connecter à l'internet pour accéder à un serveur de profils, dans lequel l'opérateur final aura préalablement déposé la souscription associée à l'utilisateur de l'équipement. Un tel serveur de profils est par exemple un serveur SM-DP/SM-SR (« Subscription Manager Data Preparation / Secure Routing » ou « Gestionnaire de souscriptions – préparation des données / routage sécurisé » en français) utilisé dans le monde de l'internet des objets – IoT (« Internet of Things ») ou son évolution un serveur SM-DP+, comme cela est décrit dans les spécifications de l'association « GSMA » SGP.21 et SGP.31.

[0004] Cependant, pour cette phase initiale, notamment lorsqu'il n'est équipé d'aucune autre interface (le WIFI n'étant pas disponible sur les terminaux IoT), l'équipement doit utiliser son interface air pour accéder à l'internet. Il doit par conséquent utiliser les services d'un réseau de radiocommunication public intermédiaire géré par un opérateur intermédiaire.

[0005] Actuellement, un fichier d'amorçage, ou fichier de « bootstrap » en anglais, est fourni à l'équipement pour lui permettre d'effectuer cette connectivité initiale avec un réseau public intermédiaire.

[0006] Une telle solution présente néanmoins différents inconvénients.

[0007] Il est ainsi nécessaire d'avoir des accords d'itinérance (« roaming ») entre l'opérateur final et l'opérateur intermédiaire du réseau public autorisant la connectivité initiale.

[0008] Pour un équipement susceptible d'être utilisé dans différents pays et/ou n'importe où dans un pays, il faut alors multiplier les accords d'itinérance pour permettre à l'utilisateur de l'équipement de charger et activer une souscription, au moment où il vient de prendre possession de l'équipement et souhaite l'initialiser pleinement. Or, il s'avère difficile d'obtenir une telle variété d'accords. Cela est très couteux et reste difficile à opérer.

[0009] De plus, le fait de disposer d'un accord d'itinérance n'est parfois pas suffisant, puisque l'équipement peut, au moment où l'utilisateur souhaite l'initialiser, se situer dans une zone blanche, c'est à dire une zone non couverte du réseau public de l'opérateur intermédiaire avec lequel l'opérateur final à cet accord d'itinérance.

[0010] Il faut par ailleurs que le fichier d'amorçage soit enregistré dans l'équipement avant son achat par l'utilisateur final. C'est donc au fabricant d'enregistrer le fichier d'amorçage dans un équipement destiné à être utilisé avec une souscription d'un opérateur final particulier.

[0011] Le fabricant dépend par conséquent du fournisseur de ce fichier d'amorçage. Comme le fichier d'amorçage dépend de l'opérateur final (et éventuellement pour un opérateur final des différents opérateurs intermédiaires avec lesquels il a des accords d'itinérance), cela pose un problème de logistique important au fabricant, qui doit savoir quel fichier d'amorçage enregistrer dans un lot d'équipements destiné à être vendu sur un marché particulier.

[0012] Tout cela représente une gestion complexe d'un point de vue opérationnel et sécuritaire et par conséquent un coût supplémentaire uniquement pour réaliser cette connectivité initiale.

[0013] En particulier, une telle façon de faire n'est pas envisageable dans la pratique pour le déploiement d'équipements dans le cadre de l'internet des objets - IoT (« internet of things »), où l'on cherche à disséminer dans l'environnement un grand nombre d'équipements à faible coût ayant la capacité de se connecter à l'internet pour échanger des données.

[0014] L'utilisation d'un fichier d'amorçage est donc problématique.

[0015] Il y a donc un besoin de simplifier le procédé permettant le provisionnement d'un équipement avec une souscription d'un opérateur final.

[0016] Le but de la présente invention est de répondre à ce besoin.

[0017] Pour cela l'invention a pour objet un procédé de provisionnement d'un équipement utilisateur avec une information d'un opérateur final, l'équipement utilisateur – UE étant muni d'une carte du type circuit intégré universelle embarquée – eUICC et d'un module radio, caractérisé en ce qu'il consiste à : déployer un réseau de téléphonie mobile privé, connecté à un réseau IP hébergeant un serveur mémorisant ladite information ; attribuer dynamiquement, par un équipement de gestion d'identifiants du réseau de téléphonie mobile privé, au moins un identifiant de profil temporaire à l'eUICC résidant dans l'UE ; connecter l'UE au réseau IP via le réseau de téléphonie mobile privé en utilisant ledit au moins un identifiant de profil temporaire ; télécharger ladite information auprès du serveur ; et déconnecter l'UE.

[0018] Suivant des modes particuliers de réalisation, le procédé comporte une ou plusieurs des caractéristiques suivantes, prises isolément ou suivant toutes les combinaisons

techniquement possibles :

[0019] - attribuer dynamiquement, par un équipement de gestion d'identifiants du réseau de téléphonie mobile privé, au moins un identifiant d'abonnement à l'eUICC consiste à transmettre, par l'équipement de gestion d'identifiants, au travers du réseau de téléphonie mobile privé auquel l'UE demande à s'attacher en mettant en œuvre un protocole standard d'attachement d'un terminal itinérant sur un réseau de téléphonie mobile, un identifiant d'abonnement temporaire dans un champ d'un message échangé conformément audit protocole standard d'attachement, la mise en œuvre du protocole standard d'attachement se terminant par un rejet de la demande d'attachement, un profil temporaire spécifique pour l'eUICC ayant été créé par l'équipement de gestion d'identifiants (64) et transmis à un serveur de profils d'abonnés - HSS du réseau de téléphonie mobile privé, ledit profil temporaire intégrant l'identifiant d'abonnement temporaire attribué à l'eUICC.

[0020] - connecter l'UE au réseau public via le réseau de téléphonie mobile privé en utilisant ledit au moins un identifiant d'abonnement temporaire (t-IMSI) consiste à émettre, par l'UE , une nouvelle demande d'attachement au réseau de téléphonie mobile privé en mettant en œuvre le protocole standard d'attachement en utilisant l'identifiant d'abonnement temporaire.

[0021] - la nouvelle demande d'attachement met en œuvre une procédure d'authentification entre l'eUICC et l'équipement de gestion d'identifiants.

[0022] - l'eUICC et l'équipement de gestion d'identifiants échangent des paramètres de chiffrement permettant de calculer, de part et d'autre, des accréditations, ledit profil temporaire intégrant lesdites accréditations.

[0023] - l'équipement de gestion d'identifiants reconnaît l'eUICC à qui fournir un identifiant d'abonnement temporaire à partir d'un paramètre d'identification de l'eUICC reçu de l'eUICC et présent dans une liste de paramètres d'identification d'eUICCs mémorisée par l'équipement de gestion d'identifiants.

[0024] - l'information à télécharger est un profil de souscription, le serveur étant un serveur de profils du type SM-DP.

[0025] L'invention a également pour objet un système pour la mise en œuvre d'un procédé de provisionnement d'un équipement utilisateur avec une information d'un opérateur final conforme au procédé précédent, comportant : un équipement utilisateur – UE, l'UE étant muni d'une carte du type circuit intégré universelle embarquée – eUICC et d'un module radio pour se connecter ; un réseau public hébergeant un serveur mémorisant ladite information ; et un réseau de téléphonie mobile privé, le réseau de téléphonie mobile privé comportant : une connexion filaire ou non filaire au réseau public ; un serveur de profils d'abonné – HSS ; un équipement de gestion d'identifiants, l'équipement de gestion d'identifiants étant propre à : attribuer à

l'eUICC un identifiant d'abonnement temporaire ; à transmettre à l'eUICC l'identifiant d'abonnement temporaire ; à créer un profil temporaire spécifique de l'eUICC ; et à mettre à jour le serveur de profils d'abonné – HSS avec ledit profil temporaire, ledit profil temporaire intégrant l'identifiant d'abonnement temporaire attribué à l'eUICC.

[0026] L'invention a également pour objet un réseau de téléphonie mobile privé adapté pour être intégré dans le système précédent.

[0027] De préférence, ce réseau est déployé à partir d'un ordinateur intégrant les différentes fonctionnalités d'un réseau de téléphonie mobile et adapté pour couvrir une zone géographique limitée.

[0028] L'invention a également pour objet une chaîne de production d'un équipement utilisateur – UE comportant un poste de configuration des UEs fabriquées, ledit poste intégrant le réseau de téléphonie mobile privé précédent.

[0029] L'invention a finalement pour objet un produit programme d'ordinateur comportant des instructions logicielles qui, lorsqu'elles sont exécutées par un ordinateur, confèrent audit ordinateur la possibilité de fonctionner conformément au réseau de téléphonie mobile privé précédent, l'ordinateur ayant des moyens matériels adaptés pour constituer une station de base du réseau de téléphonie mobile privé et une connexion filaire ou non filaire à un réseau IP.

[0030] L'invention et ses avantages seront mieux compris à la lecture de la description détaillée qui va suivre d'un mode de réalisation particulier, donné uniquement à titre d'exemple non limitatif, cette description étant faite en se référant aux dessins annexés sur lesquels :

[0031] [Fig.1] La [Fig.1] est une représentation schématique d'une installation intégrant un système selon l'invention permettant la mise en œuvre du procédé selon l'invention ;

[0032] [Fig.2] La [Fig.2] et une représentation schématique sous forme de bloc t'es un mode de réalisation préférée du procédé salon l'invention ;

[0033] [Fig.3] La [Fig.3] est un chronogramme des messages échangées dans l'installation de la [Fig.1] pour la réalisation de l'étape principale du procédé de la [Fig.3] ; et,

[0034] [Fig.4] La [Fig.4] est une représentation schématique d'une chaîne de production équipée du système selon l'invention.

[0035] La présente invention consiste à déployer un réseau privé sur un lieu de production. Ce réseau privé est géré par le fabricant. Ce réseau privé est connecté à l'internet par une liaison filaire ou en variante par une liaison sans fil, par exemple Wi-Fi. Ce réseau privé comporte un serveur propre à attribuer automatiquement des identifiants temporaires à un équipement arrivant en bout de chaîne de fabrication .

[0036] Ces identifiants temporaires sont provisionnés dans l'équipement, qui doit pour cela être équipé d'une carte eUICC, comme par exemple une carte eSIM (« embedded SIM ») ou l'équivalent, comme par exemple une carte iSIM (« integrated SIM »), conve-

nablement programmée. L'ensemble des identifiants temporaires provisionnés comporte au moins un iMSI, puisque c'est le seul identifiant qu'il convient a minima d'ajouter si l'on souhaite effectuer un changement de souscription.

[0037] Une fois l'IMSI du réseau privé provisionné dans la carte eSIM, l'équipement peut s'attacher et s'identifier au réseau privé, pour ensuite se connecter à l'internet et télécharger directement la souscription adaptée auprès d'un serveur de profils de l'opérateur final.

[0038] Le système selon l'invention est donc une solution complètement dynamique, qui offre une connectivité initiale temporaire à un équipement en bout de chaîne de fabrication.

[0039] On s'affranchit ainsi de l'utilisation d'un fichier d'amorçage et de la nécessité d'utiliser un réseau public intermédiaire. Cela permet également de simplifier drastiquement la logistique associée. Tout ceci concourt par conséquent à la diminution des coûts. De plus, cela permet de laisser la gestion de la sécurité au seul fabricant.

[0040] Une mode de réalisation préféré de l'invention va être présenté en relation avec les figures.

[0041] La [Fig.1] représente une installation comportant un équipement utilisateur – UE (« User Equipment ») 1, un réseau de radiocommunication privé 10, et le réseau IP 20 (c'est-à-dire une réseau de communication mettant en œuvre le protocole internet – IP (« Internet Protocol »).

[0042] Le réseau IP 20 est par exemple un réseau public, comme le réseau Internet. Il comporte un serveur 22 provisionné avec des informations relatives à une souscription au réseau de téléphonie mobile d'un opérateur final sur lequel l'équipement utilisateur UE 1 est destiné à fonctionner. Le serveur 22 est par exemple un serveur du type SM-DP stockant un profil associé à une souscription.

[0043] Le réseau 10 est un réseau privé de téléphonie mobile du type 3G, 4G ou 5G ou futur telle que définit par le 3GPP (« 3rd Generation Partnership Project »). Dans ce qui suit, sera plus particulièrement pris pour exemple le cas d'un réseau du type 4G, mais l'homme du métier sait comment appliquer l'enseignement de la présente description au cas d'un autre type d'infrastructure de téléphonie mobile, notamment une infrastructure du type 5G.

[0044] Le réseau 10 offre un service de téléphonie mobile dans une région géographique limitée (de l'ordre de quelques mètres) couvrant par exemple la chaine de fabrication ou l'usine de fabrication de l'UE 1. On peut parler de microsystème de radiocommunication.

[0045] Le réseau 10 est géré par le fabricant de l'UE 1, qui opère également la chaine de fabrication de l'UE 1.

[0046] Le réseau 10 comporte un réseau d'accès radio 11, ou RAN (« Radio Access

Network »), intégrant de préférence un unique point d'accès 12, ou eNB (« e-Node B » en 4G). Un eNB permet à un équipement utilisateur de se connecter au moyen d'une liaison radio sans fil au réseau 10. Par exemple, l'UE1 est connecté (ou cherche à établir une connexion) au travers de la liaison 81 avec l'eNB 12 du RAN 11.

[0047] Le réseau 10 comporte un réseau cœur 15, ou ePC (« evolved Packet Core » en 4G), comportant notamment :

[0048] - une passerelle de service 14, ou SGW (« Serving Gateway »), qui s'occupe, au niveau plan de données, de l'acheminement des flux « utiles » (les communications voix, le trafic de données applicatives, etc.) entre le RAN 11 et le ePC 15.

[0049] - un serveur MME (« Mobile Management Entity ») 16, qui gère, au niveau plan de contrôle, les sessions (authentification, autorisations,…).

[0050] - une passerelle 19, ou PGW (« Paquet Data Network Gateway ») responsable des échanges des flux « utiles » avec le réseau internet 20. La passerelle 19 peut comporter ou consister en une carte réseau Ethernet connectée par un câble au réseau internet 20 (liaison 86 de la [Fig.1]) ;

[0051] - un serveur d'abonnés, ou serveur HSS (« Home Subscriber Server ») 18, propre à offrir un service d'abonnés. Le HSS 18 comporte une base de données des profils des abonnés, avec leurs droits et leurs caractéristiques ;

[0052] - un module de gestion d'identifiants 64, qui sera décrit en détail ci-dessous.

[0053] Sur la [Fig.1], différentes liaisons ont été représentées :

[0054] - la liaison 82 est une liaison de flux de données entre l'eNB 12 et le SGW 14,

[0055] - la liaison 83 est une liaison de flux de données entre le SGW 14 et le PGW 19.

[0056] - la liaison 84 est une liaison de flux de contrôle entre le SGW 14 et le MME 16.

[0057] - la liaison 85 est une liaison de flux de contrôle entre le eNB 12 et le MME 16.

[0058] - la liaison 70 est une liaison de flux de contrôle entre le MME 16 et le HSS 18.

[0059] L'UE 1 utilise le réseau 10 pour télécharger un profil temporaire, qui lui permettra ensuite de se connecter à l'internet 20, en particulier à un serveur SMDP 22 afin de télécharger un profil définitif associé à une souscription au réseau de téléphonie mobile géré par un opérateur final.

[0060] L'UE 1 comporte un moyen de calcul, tel qu'un processeur 2, un moyen de mémorisation, tel qu'une mémoire 3, une carte eUICC 4 et un module radio 5. Ces composants sont connectés par un bus de données adapté 6.

[0061] La mémoire 3 comporte les instructions de programmes d'ordinateur qui, lorsqu'elles sont exécutées par le processeur 2 permettent la mise en œuvre de certaines fonctionnalités. En particulier, la mémoire 3 comporte les instructions d'un programme 31 permettant la mise en œuvre par l'UE 1 de certaines des étapes du procédé selon l'invention.

[0062] Le module radio 5 est connu en tant que tel. Il stocke deux identifiants :

[0063] - l'IMEI (« International Mobile Equipment Identity »), qui est un identifiant du module radio 5 de l'UE 1. C'est une information qui est fixe ; et,

[0064] - l'IPadd, qui est l'adresse IP (« Internet Protocol ») attribuée à l'UE 1 au cours de la mise en œuvre du procédé selon l'invention.

[0065] L'équipement utilisateur UE 1 comporte une carte de circuit intégré universelle embarquée - eUICC (« Embedded Universal Integrated Circuit Card ») 4.

[0066] De manière générale, un carte eUICC (comme une carte eSIM) est une carte SIM (« Subscriber Identity Module ») qui présente la capacité de pouvoir être re-programmée à distance via l'interface radio (programmation « Over The Air » - OAT) par une machine du réseau à laquelle l'UE se connecte, tel qu'un serveur SM-DP+ (« Subscription Manager – Data Preparation »). En variante, une carte iSIM est utilisée. Il s'agit d'une carte eUICC intégré au processeur de l'équipement.

[0067] De la sorte, un utilisateur peut mémoriser plusieurs profils sur l'UE qu'il utilise, chaque profil correspondant à des souscriptions avec des opérateurs finaux différents et/ou, pour un même opérateur final, pour des services différents (comme l'échange de données, les appels longue distance, etc.)

[0068] Dans le présent procédé, l'utilisation d'une carte eUICC est nécessaire car l'identifiant principal que le présent procédé permet d'attribuer dynamiquement à l'équipement est l'identifiant IMSI (« International Mobile Subscriber Identity »). Or, une carte SIM (« subscriber identity/identification module ») classique mémorise un IMSI qu'il n'est pas possible de modifier.

[0069] L'eUICC 4 comporte un moyen de calcul, tel qu'un processeur 42, et un moyen de mémorisation, tel qu'une mémoire 43.

[0070] La mémoire 43 comporte les instructions de programmes d'ordinateur qui, lorsqu'elles sont exécutées par le processeur 42 permettent la mise en œuvre de certaines fonctionnalités. En particulier, la mémoire 43 comporte les instructions d'un programme 41 permettant la mise en œuvre par l'eUICC 4 de certaines des étapes du procédé selon l'invention.

[0071] Par ailleurs, la mémoire 43 stocke différentes informations.

[0072] Avant la mise en œuvre du procédé selon l'invention, la mémoire 43 comporte un ensemble d'informations pré-provisionnées, notamment :

[0073] - un EID (« eUICC ID »), qui est un identifiant de l'eUICC 4 ;

[0074] - une MK, qui est une clé maîtresse (« Master Key »), partagée avec le service d'attribution dynamique d'identifiants du module 64 ;

[0075] - des MK1 et MK2, qui sont des clés diversifiées caractéristiques de l'eUICC 4 ;

[0076] - un Cer, qui est un certificat constituant une signature de l'eUICC 4 ; et,

[0077] - une IPsmdp, qui est l'adresse IP du serveur SM-DP+ auquel l'UE 1 cherche à se connecter pour télécharger un profil définitif.

[0078] Au cours ou après la mise en œuvre du procédé selon l'invention, la mémoire 43 comporte, en outre :

[0079] - un IMSI (« international mobile subscriber identity »), qui est un identifiant normalement attribué par un opérateur aux cartes SIM des UEs dont les utilisateurs ont une souscription auprès de cet opérateur ;

[0080] - un Ki (« Subscriber Authentication Key ») et un OPc (« derived operator code »), qui sont un exemple d'ensemble d'informations permettant une authentification réciproque entre un abonné et un opérateur. Un tel ensemble de clés est dénommé accréditations (« credentials »).

[0081] Il est à noter que l'IMSI, et éventuellement le Ki et l'OPc, sont chargés sur l' l'eUICC 4 et chargés dans le HSS 18.

[0082] D'autres informations, identifiants ou paramètres existent. Ils ne sont pas mentionnés car ils ne sont pas modifiés par le présent procédé. Si certains d'entre eux sont utilisés au cours de la mise en œuvre du présent procédé, ils prennent une valeur prédéfinie ou une valeur par défaut.

[0083] Le module de gestion d'identifiants 64 est constitué par un calculateur pour réaliser certaines des étapes du procédé selon l'invention de manière à fournir un service d'attribution dynamique d'identifiants et, une fois ces identifiants attribués à un équipement utilisateur, un service de gestion des communications.

[0084] L'équipement de gestion d'identifiants 64 est par exemple fondé sur une architecture du type SDN (« Software Defined Network »). Elle comporte alors une composante de contrôle réseau 50 et une composante applicative d'orchestration de services, ou orchestrateur 60.

[0085] La composante de contrôle réseau 50 comporte par exemple :

[0086] - un module d'autorisation et d'authentification, dit module AAA (« Authentication, Authorization, Accounting/Auditing ») 57, pour la mise en œuvre de mécanismes d'authentification sur la base de certificats, tel que par exemple le mécanisme EAP-TLS (« Extensible Authentication Protocol - Transport Layer Security »). Ce module est relié à l'orchestrateur 60 par une liaison 72, par exemple du type API REST.

[0087] - un serveur d'attribution dynamique d'identifiants, dit serveur « TIC » 51, participant à l'attribution et à l'utilisation d'une IMSI temporaire (t-IMSI) pour un équipement utilisateur. Le serveur TIC 51 est relié à l'orchestrateur 60 par une liaison 72, par exemple du type API REST. Le serveur TIC 51 est relié, via la liaison 70, au MME 16.

[0088] Le serveur TIC 51 peut être identifié comme un centre d'authentification - AuC («Authentication Center »).

[0089] Le serveur TIC 51 comporte par exemple un module SP 52 ayant pour fonction d'identifier des UEs abonnés au service d'attribution dynamique d'identifiants et de

mettre en œuvre le protocole de transfert d'un t-ISMI temporaire, ainsi qu'avantageusement un module SG 53 ayant pour fonction de simplifier la gestion des clefs et des droits des UEs abonnés au service.

[0090] La composante d'orchestration de services 60 a pour fonction de synchroniser les différents services, notamment l'attribution et la gestion des identifiants temporaires.

[0091] Dans une variante particulièrement avantageuse, le réseau 10 ne comporte pas de serveur HSS 18 séparé. C'est le module 64 qui réalise les fonctions d'un serveur HSS. Il est à noter que les fonctions d'un serveur HSS sont simplifiées dans la mesure où il n'y a pas de gestion de la mobilité à prévoir sur le réseau 10, puisque ce réseau ne comporte avantageusement qu'un eNB et qu'un MME.

[0092] L'orchestrateur 60 gère les différents modules de la composante de contrôle réseau 50. L'orchestrateur 60 est relié aux différentes fonctionnalités du plan de contrôle. Dans le présent mode de réalisation, l'orchestrateur 60 est ainsi relié au serveur TIC 51 (liaison 72), au serveur HSS 18 (liaison 71), à la passerelle PGW 19 (liaison 73 sur la [Fig.1], par exemple du type interface SGi Radius). C'est l'orchestrateur qui synchronise et assure la cohérence lors de la mise en place des services.

[0093] De plus, l'orchestrateur 60 est relié au HSS 18 par une liaison 71, par exemple du type API REST.

[0094] La composante d'orchestration de services 60 tient à jour une base de données 65.

[0095] La base de données 65 comporte les données nécessaires à l'attribution d'identifiants temporaires à un abonné au service et, une fois un identité temporaire attribuée à un UE, le contrôle de la communication entre cet UE et le destinataire que constitue le serveur SM-DP 22.

[0096] En particulier, la base de données 65 comporte :

[0097] - une Liste_EID, qui est une liste des EIDs des UEs abonnés au service et les certificats Cer de chacun de ces UEs ;

[0098] - la clé maîtresse MK du service d'attribution dynamique d'identifiants ;

[0099] Et, pour chaque UE 1 utilisant effectivement le réseau 10 à un instant donné, la base de données 65 comporte en outre :

[0100] - l'EID de cet UE ;

[0101] - l'IMEI courante de cet UE ;

[0102] - l'IMSI courante de cet UE ;

[0103] - les clés diversifiées MK1, MK2 de cet UE ;

[0104] - les credentiels Ki et OPc de cet UE ; et,

[0105] - l'adresse IP, IPadd, attribuée à cet UE.

[0106] La [Fig.2] représente le cas d'usage envisagé pour la présente invention, à savoir une chaîne de fabrication, en l'occurrence d'un véhicule automobile, dont le dernier poste consiste à configurer l'équipement utilisateur, en l'occurrence un ordinateur de bord du

véhicule automobile fabriqué le long de cette chaine.

[0107] La chaîne de fabrication 100 comporte une succession de postes conduisant à la fabrication d'un véhicule automobile 90. Par exemple, la chaîne de fabrication 100 comporte un poste 102 d'assemblage de tôlerie pour la fabrication de la caisse, un poste 104 de peinture de la caisse, un poste 106 d'assemblage du châssis et des organes moteurs, un poste 108 de montage de la caisse sur le châssis, un poste 110 d'installation d'équipements dans l'habitacle, et un une étape 112 d'implantation de l'ordinateur de bord.

[0108] Selon l'invention, la chaîne de fabrication 100 comporte, en outre, un poste 120 de configuration de l'ordinateur de bord, en tant qu'équipement utilisateur 1, de chaque véhicule passant à travers ce poste 120.

[0109] Le poste 120 comporte de préférence un ordinateur 122 permettant de déployer le réseau de radiocommunication privé 10 de la [Fig.1]. Il comporte notamment une antenne 124, qui est l'antenne du eNB 12 du RAN 11 du réseau 10. Il est programmé pour réaliser les fonction de l'ePC 15 de la [Fig.1]. L'ordinateur 122 est programmé pour mettre en œuvre au moins les fonctionnalités minimales d'un réseau cœur, ainsi que les fonctionnalités permettant la mise en œuvre du procédé selon l'invention.

[0110] Cette antenne 12 permet de définir une zone de couverture élémentaire du réseau 10, ou cellule 126, présentant une extension géographique réduite, mais suffisante pour permettre aux véhicules se déplaçant le long de la chaîne de production, à l'intérieur de ladite cellule, d'avoir le temps de télécharger un profil de souscription.

[0111] L'ordinateur 122 est par ailleurs connecté au réseau internet (non représenté sur la [Fig.2]) par une liaison filaire 128. En variante, il s'agit d'une liaison sans fil, par exemple Wi-Fi.

[0112] L'équipement utilisateur 1 est allumé lorsque le véhicule qu'il équipe entre dans le poste 120 (c'est à dire à l'intérieur de la cellule 126). L'UE1 établit une connexion 81 avec l'eNB 12 (via l'antenne 124). La mise en œuvre du procédé selon l'invention est réalisée alors que le véhicule se déplace à travers la cellule 126. Lorsqu'il sort du poste 120, l'ordinateur de bord du véhicule 90 est provisionné avec un profil de souscription d'un opérateur final de téléphonie mobile. De la sorte, lorsque le véhicule 90 sera vendu, son nouveau propriétaire pourra immédiatement se connecter au réseau de téléphonie mobile de cet opérateur final de manière à accéder sans attendre et facilement aux services fournis par cet opérateur final. Eventuellement, cette première connexion au réseau de l'opérateur final consistera à redéfinir les droits et services effectivement ouverts à ce nouveau propriétaire du véhicule 90, c'est-à-dire charger un autre profil de souscription.

[0113] Si le cas d'un véhicule automobile a été présenté, le présent procédé peut s'appliquer à n'importe quel dispositif destiné à pouvoir se connecter à un réseau de téléphonie

mobile, comme par exemple un téléphone, une tablette, un ordinateur personnel, des dispositifs intelligents pour la domotique, la sécurité des infrastructures, la télémesure médicale, etc.

[0114] Comme représenté sur la [Fig.3], le procédé 200 consiste, dans une étape 205 à déployer le réseau local privé 10 le long d'une chaîne de fabrication.

[0115] Avant la mise en œuvre du procédé selon l'invention, l'eUICC de l'UE 1 est vierge, au sens où elle ne comporte aucun profil lui permettant de s'attacher, par son interface air, à un réseau de téléphonie mobile.

[0116] De plus, le serveur HSS 18 ne comporte aucun profil relatif à l'UE 1.

[0117] Puis dans une étape 210, le procédé consiste à déplacer l'UE 1 le long de la chaîne de production pour qu'elle entre dans la zone de couverture du réseau privé 10, à savoir la cellule 126.

[0118] Dans une étape 220, UE 1 est allumé.

[0119] Le fait d'allumer l'UE 1 initie la mise en œuvre de la première phase du procédé conduisant, à l'étape de 230, à l'attribution d'identifiants temporaires à l'UE 1.

[0120] Une fois que l'UE 1 dispose d'identifiants temporaires, dans une étape 240, UE 1 se connecte au réseau internet 20, via le réseau 10.

[0121] Dans une seconde phase du procédé, qui correspond à l'étape 250, l'UE 1 se connecte au serveur 22 pour télécharger un profil associé à une souscription préalablement préparée par l'opérateur final.

[0122] Une fois l'UE 1 provisionné avec un profil de souscription, l'UE 1 est éteint.

[0123] Ainsi, suite à la mise en œuvre du présent procédé, une fois entre les mains de son utilisateur final, UE 1 pourra se connecter directement au réseau, privé ou public, géré par l'opérateur final ou géré par un opérateur avec lequel l'opérateur final aura un accord d'itinérance.

[0124] En se reportant à la [Fig.4], les étapes 230 et 240 du procédé 200 vont être détaillées.

[0125] Le procédé 200 permet l'attribution dynamique d'un identifiant d'abonnement IMSI à l'équipement UE 1, en s'appuyant sur un mécanisme d'échange de données cachées dans les champs des messages classiquement échangés lors de l'enrôlement d'un équipement utilisateur auprès d'un réseau de téléphonie mobile, tel que le premier réseau 10. Ce mécanisme est par exemple décrit dans la demande de brevet EP 3 506 668.

[0126] Plus précisément, sur la [Fig.4], après avoir été mis sous tension à l'étape 220, l'étape 230 consiste à un enrôlement de l'UE 1 auprès du service d'attribution dynamique d'identifiants afin de fournir à l'UE 1 un profil temporaire.

[0127] L'UE 1 va d'abord utiliser un premier IMSI, IMSI1, généré aléatoirement pour s'enrôler auprès du réseau 10. Cet IMSI va être identifié par le réseau 10 comme appartenant à son réseau privé et le serveur TIC 51 va en profiter pour récupérer l'EID de

l'UE 1, et lui renvoyer un IMSI temporaire, t-IMSI.

[0128] De manière détaillée :

[0129] Etape 302 : suite à la mise sous tension de l'UE1, la carte eUICC 4 ne détecte aucun IMSI définitif dans sa mémoire 43 et calcule alors, de façon aléatoire, un premier IMSI, IMSI1. Par exemple, ce premier IMSI est calculé sur la base de l'EID. En variante, est pré-enregistré sur la carte eUICC 4 un IMSI origine.

[0130] Etape 303: Pour s'enrôler sur le réseau 10, l'UE 1 demande à la carte eUICC 4 un IMSI.

[0131] Etape 304 : la carte eUICC 4 renvoie l'IMSI1, calculée à l'étape 301.

[0132] Etape 305 : l'UE 1 cherchant à se connecter au réseau 10, émet une requête d'attachement vers le MME 16. Cette requête d'attachement comporte l'IMSI1.

[0133] Etape 306 : suite à la réception de la requête d'attachement, le MME 16 constate que l'IMSI1 est dans une première gamme de valeurs prédéfinie (par exemple entre 0 et 50). En conséquence, le MME 16 émet une requête vers le serveur TIC 51.

[0134] Etape 307 : en réponse à cette requête, le serveur TIC 51 demande à la carte eUICC 4 son EID pour pouvoir l'identifier comme l'un des abonnés au service d'attribution dynamique d'identifiants. Cette demande est masquée dans une requête d'authentification classique. Plus précisément :

[0135] Etape 308 : une requête d'authentification est transmise du serveur TIC 51 vers le MME 16.

[0136] Etape 309 : une requête d'authentification est transmise du MME 16 vers l'UE 1.

[0137] Etape 310 : une requête d'authentification est transmise de l'UE 1 vers la carte eUICC 4.

[0138] Etape 311 : suite à la réception de la requête d'authentification, la carte eUICC 4 lit l'EID présent dans sa mémoire 43 et, de préférence, le crypte en utilisant la clé maîtresse MK associée au service d'attribution dynamique d'identifiants. La clé MK est une clé privée, qui est partagée avec le réseau 10 et préalablement provisionnée sur les UEs.

[0139] Etape 312 : la carte eUICC 4 répond à la requête d'authentification de l'UE 1 en lui passant l'EID chiffré.

[0140] Etape 313 : l'UE 1 répond à la requête d'authentification du MME 16 par un message classique d'échec de l'authentification. Ce message comporte l'EID chiffré.

[0141] Etape 314 : le MME 16 transmet le message d'échec d'authentification au serveur TIC 51.

[0142] Etape 315 : Le serveur TIC 51 utilise la clé maîtresse MK du module 64 pour décrypter l'EID de l'eUICC 4.

[0143] Le serveur TIC 51 vérifie que l'EID est présent dans la liste Liste_EID contenant les EIDs des abonnés au service. Si l'EID reçu n'est pas dans la liste des EIDs, l'étape 230

se termine. En revanche, si l'EID reçu est valide, le serveur TIC 51 sélectionne un IMSI temporaire, t-MSI, dans une seconde gamme de valeurs (par exemple entre 1000 et 3000).

[0144] En variante, au cas où le fabricant ne souhaite pas provisionner ses EIDs dans l'équipement 64, l'utilisation d'un paramètre supplémentaire permettra d'identifier un équipement utilisateur du fabricant, ce paramètre devant alors être provisionné dans ses équipement et dans la base de données 65 de l'équipement 64, à laquelle accède le serveur TIC 51.

[0145] Le serveur TIC 51 calcule les accréditations (Ki et OPc) associées au t-IMSI sélectionné, un nombre aléatoire RAND, ainsi qu'une durée de connectivité temporaire de X minutes.

[0146] Le serveur TIC 51 de l'équipement 64 chiffre le t-IMSI, le Ki, l'OPc et la durée de connectivité temporaire au moyen de la clé maitresse MK et transmet à la carte eUICC 4 ces informations cryptées, ainsi que le nombre aléatoire RAND, et un résultat de chiffrement XRES. Cette transmission s'effectue en masquant ces informations dans une nouvelle demande d'authentification adressée à la carte eUICC 4. Plus précisément :

[0147] Etape 316 : une requête d'authentification est ainsi transmise du serveur TIC 51 vers le MME 16.

[0148] Etape 317 : le MME 16 conserve le XRES et retransmet la requête d'authentification vers l'UE 1.

[0149] Etape 318 : la requête d'authentification est retransmise de l'UE 1 vers la carte eUICC 4.

[0150] Etape 319 : la carte eUICC 4 calcule un résultat RES à partir du nombre aléatoire RAND et des informations cryptées, notamment le t-IMSI.

[0151] Etape 320 : la carte eUICC TAC 4 répond à la requête d'authentification de l'UE 1 par un message intégrant le résultat RES du calcul de l'étape 319.

[0152] Etape 321 : l'UE 1 répond à la requête d'authentification du MME 16 par un message intégrant le résultat RES.

[0153] Etape 322 : le MME compare le RES et le XRES.

[0154] Etape 323 : ces grandeurs étant identiques, le MME 16 retransmet la réponse d'authentification vers le serveur TIC 51.

[0155] Etape 324 : en réponse, le serveur TIC 51 renvoie un message d'erreur d'authentification vers le MME 16.

[0156] Etape 325 : le MME 16 rejette la demande d'attachement de l'UE 1.

[0157] Du point de vue du MME 16, c'est-à-dire du réseau 10, il n'y a donc eu qu'un échange de messages d'authentification ayant conduit à un échec d'authentification, alors que le module 64 a pu récupérer l'EID de la carte eUICC 4 et cette dernière un

IMSI temporaire.

[0158] Etape 326 : le serveur TIC 51 calcule, à partir du t-IMSI venant d'être attribué à la carte eUICC 4, de la clé maîtresse MK, et du nombre aléatoire RAND envoyé à la carte eUICC 4, un Ki1 et un OPc1.

[0159] Le serveur TIC 51 transmet ces accréditations (Ki1 et un OPc1) à l'orchestrateur 60 pour qu'il provisionne, via la liaison 71, le HSS 18 avec le profil temporaire de ce nouvel abonné qu'est la carte eUICC 4 de l'UE 1. L'équipement 64 fournit au HSS le t-IMSI, le Ki1 et l'OPc1. Il indique également et de préférence les ressources informatiques ou de télécommunication afin de répondre aux besoins de ce nouvel abonné.

[0160] Etape 327 : parallèlement, la carte eUICC 4 mémorise le t-IMSI à la place de e-IMSI1.

[0161] L'eUICC 4 calcule les Ki1 et OPc1, avec le t-IMSI, la clé maîtresse MK et le nombre aléatoire RAND reçu du serveur TIC 51.

[0162] Finalement, la carte eUICC 4 commande un redémarrage du module radio 5 afin d'initier un attachement au réseau 10 mais avec le t-IMSI.

[0163] Avantageusement, la carte eUICC 4 contrôle que cette nouvelle connexion restera temporaire et ne se prolongera pas au-delà de la durée de connectivité temporaire de X minutes prévue.

[0164] Etape 328 : la carte eUICC 4 rafraichit les informations du module radio 5 de l'UE 1 en lui indiquant le t-IMSI.

[0165] Etape 329 : l'UE 1 cherchant à se connecter au réseau 10, émet une requête d'attachement vers le MME 16. Cette requête d'attachement intègre le t-IMSI.

[0166] Etape 330 : Suite à la réception de la requête d'attachement, constatant que le t-IMSI est dans la seconde gamme de valeurs, le MME 16 demande au serveur HSS 18 d'authentifier l'UE 1. Cette demande comporte le t-IMSI.

[0167] Etape 331 : le serveur HSS 18, maintenant convenablement provisionné avec le profil temporaire de l'UE 1, répond par un message de demande d'authentification avec les paramètres RAND, XRES et AUTN nécessaires à une authentification mutuelle à réaliser au niveau du MME 16.

[0168] Etape 332 : sur réception du message de demande d'authentification, le MME 16 mémorise certains de ces paramètres, tandis qu'il retransmet les autres dans un message d'authentification vers l'UE 1.

[0169] Etape 333 : le message d'authentification reçu par l'UE1, est retransmis à la carte eUICC 4.

[0170] Etape 334 : après vérification positive du RAND/AUTN, la carte eUICC 4 calcule un RES.

[0171] Etape 335 : la carte eUICC 4 transmet le RES calculé à l'UE 1.

[0172] Etape 336 : l'UE 1 retransmet le RES au MME 16.

[0173] Etape 337 : le MME compare le RES et le XRES, et, ces deux grandeurs étant effectivement identiques, le MME 16 accepte l'attachement de l'UE 1.

[0174] Etape 338 : de manière conventionnelle, une fois l'attachement accepté, le MME 16 transmet au HSS 18 une information de localisation de l'UE 1 et le HSS 18 répond aux MME 16 par un message d'accuser-réception.

[0175] Etape 240 : l'UE 1 étant maintenant attaché au réseau 10 avec son profil temporaire, l'UE 1 reçoit du réseau 10 une adresse IP, IPadd, de manière à pouvoir se connecter au réseau internet 20, via le réseau 10.

[0176] L'UE 1 peut alors télécharger (étape 250) le profil de souscription prévu par l'opérateur final en interrogeant le serveur SM-DP 22 dont il connaît l'adresse IP, IPsmdp.

[0177] Une fois le profil téléchargé, la connexion temporaire entre l'UE 1 et le réseau 10 est libérée, par exemple à l'expiration de la durée de connexion. La carte eUICC 4 se détache alors automatiquement du réseau 10. Après cette période, le t-IMSI et Ki1 sont dé-provisionnés du HSS. La valeur du t-IMSI pourra donc être réutilisée pour un autre équipement utilisateur.

[0178] L'UE 1 est alors éteinte (étape 260).

[0179] De nombreuses variantes du mode de réalisation préféré précédemment décrit sont envisageables.

[0180] Une fois qu'il possède une connexion à l'internet, l'UE 1 peut télécharger toute information d'un opérateur final autre qu'un profil de souscription, comme par exemple un code d'activation (« activation code »). Un code d'activation comporte par exemple une adresse du serveur de profils et un identifiant de mise en correspondance pour retrouver la souscription de l'utilisateur utilisant le code d'activation. L'utilisateur doit ainsi d'abord acquérir un code d'activation, pour ensuite se connecter à un serveur de profil et recevoir le profil d'abonné correspondant.

[0181] On pourrait ne pas mettre en œuvre de filtrage sur les l'EIDs, de sorte que le service d'attribution dynamique d'identifiant soit ouvert à tout équipements dans la zone de couverture du réseau 10. Cependant, cela présente un risque de diaphonie entre deux postes de configuration d'équipements utilisateurs dans une usine dont les zones de couverture se recouvrirait partiellement. Le filtrage sur l'EID permet donc de s'assurer que c'est bien l'équipement utilisateur voulu qui est configuré.

[0182] De manière similaire, on pourrait s'affranchir d'un chiffrement avec une clé partagée si l'on estime que cela offre un niveau de sécurité suffisant.

[0183] De manière similaire, on pourrait se limiter à la transmission d'un IMSI temporaire (t-IMSI) sans les accréditations. Cependant, il est préférable de calculer des accréditations afin de provisionner de manière adaptée une fonction HSS, qui permet de s'assurer qu'un profil temporaire unique est attribué à un équipement utilisateur

unique.

[0184] La solution proposée va au-delà d'un simple profil de test, comme un profil « Rhodes and Schwartz », adapté pour permettre un accès à un réseau privé. En effet, un tel profil de test ne permettrait pas deux attachements en parallèle de deux équipements utilisateurs différents, puisqu'ils partagerait les mêmes informations d'identification. Cela ne permettrait donc pas la configuration de plusieurs équipement utilisateurs simultanément, ce qui reste un besoin élémentaire d'une mise en œuvre sur une chaîne de production.

[0185] Par ailleurs, lorsque un nouveau terminal cherche à s'enrôler en indiquant son EID à l'équipement 64, la vérification de cet EID est celui d'un abonné pouvant bénéficier du service peut comporter une étape de contrôle effectuée manuellement par un opérateur, via une interface homme-machine connectée à l'équipement 64.

[0186] Au lieu de fonder cette vérification sur l'EID, on pourrait la réaliser sur un autre paramètre d'identification de la carte, comme le certificat Cer ou un identifiant provisionné à cette fin dans le terminal par le fabricant.

[0187] La solution pourra aussi être mise en œuvre sans serveur TIC sur le réseau privé, en utilisant des IMSIs / KIs pré-chargés dans les cartes eUICC des équipements utilisateurs et dans le HSS du réseau local.

[0188] Au lieu de calculer de part et d'autre une paire d'accréditations Ki1 et OPc1 à partir d'une paire d'accréditations Ki et OPc1, seul l'OPc pourrait être échangé entre le réseau et le terminal, et le Ki dérivé par le terminal d'une part et par le réseau d'autre part (en utilisant l'OPc, la clé MK et le nombre RAND).

[0189] La présente invention permet de gérer localement et dynamiquement la souscription d'un équipement utilisateur sur son site de production. En variante, le procédé peut être mis en œuvre par un revendeur de l'équipement utilisateur. Par exemple, un concessionnaire de véhicule automobile ou un vendeur de téléphones mobiles dans un pays particulier, de manière à ce que l'équipement utilisateur concerné accède à des fichiers de souscription adaptés à ce pays et aux opérateurs finaux gérant des réseaux offrant une couverture dans ledit pays.

[0190] Par temporaire, on entend des informations ayant une validité limitée dans le temps (i.e. à courte durée de vie), typiquement le temps nécessaire pour qu'un équipement utilisateur puise être enrôlé sur le réseau privé puis télécharger l'intégralité du fichier de souscription.

[0191] L'invention permet donc de simplifier la gestion du provisionnement d'informations dans des cartes eUICCs.

[0192] Dans un mode de réalisation simple, aucun pré-enregistrement n'est nécessaire au niveau de l'équipement utilisateur, ni au niveau du serveur TIC. Le provisionnement du HSS est dynamique via le serveur TIC. Ceci permet une simplicité d'utilisation

pour le fabricant (ou l'entité qui déploie le réseau privé), alors que cela ne constitue pas son cœur de métier.

Revendications

[Revendication 1] Procédé de provisionnement d'un équipement utilisateur avec une information d'un opérateur final, l'équipement utilisateur – UE (1) étant muni d'une carte du type circuit intégré universelle embarquée – eUICC (4) et d'un module radio (5), caractérisé en ce que le procédé consiste à :

- déployer (205) un réseau de téléphonie mobile privé (10), connecté à un réseau IP (20) hébergeant un serveur (22) mémorisant ladite information ;
- attribuer (230) dynamiquement, par un équipement de gestion d'identifiants (64) du réseau de téléphonie mobile privé (10), au moins un identifiant d'abonnement temporaire (t-IMSI) à l'eUICC (4) résidant dans l'UE (1) ;
- connecter (240) l'UE (1) au réseau IP (20) via le réseau de téléphonie mobile privé (10) en utilisant ledit au moins un identifiant d'abonnement temporaire (t-IMSI) ;
- télécharger (250) ladite information auprès du serveur (22) ; et,
- déconnecter (260) l'UE (1).

[Revendication 2] Procédé selon la revendication 1, dans lequel attribuer dynamiquement, par un équipement de gestion d'identifiants (64) du réseau de téléphonie mobile privé (10), au moins un identifiant d'abonnement (IMSI) à l'eUICC (4) consiste à transmettre, par l'équipement de gestion d'identifiants (64), au travers du réseau de téléphonie mobile privé (10) auquel l'UE (1) demande à s'attacher en mettant en œuvre un protocole standard d'attachement d'un terminal itinérant sur un réseau de téléphonie mobile, un identifiant d'abonnement temporaire (t-IMSI) dans un champ d'un message échangé conformément audit protocole standard d'attachement, la mise en œuvre du protocole standard d'attachement se terminant par un rejet de la demande d'attachement, un profil temporaire spécifique pour l'eUICC (4) ayant été créé par l'équipement de gestion d'identifiants (64) et transmis à un serveur de profils d'abonnés - HSS (18) du réseau de téléphonie mobile privé (10), ledit profil temporaire intégrant l'identifiant d'abonnement temporaire attribué à l'eUICC (4).

[Revendication 3] Procédé selon la revendication 2, dans lequel connecter l'UE (1) au

réseau IP (20) via le réseau de téléphonie mobile privé (10) en utilisant ledit au moins un identifiant d'abonnement temporaire (t-IMSI) consiste à émettre, par l'UE (1), une nouvelle demande d'attachement au réseau de téléphonie mobile privé (10) en mettant en œuvre le protocole standard d'attachement en utilisant l'identifiant d'abonnement temporaire.

[Revendication 4] Procédé selon la revendication 3, dans lequel la nouvelle demande d'attachement met en œuvre une procédure d'authentification entre l'eUICC (4) et l'équipement de gestion d'identifiants (64).

[Revendication 5] Procédé selon l'une quelconque des revendications 1 à 4, dans lequel l'eUICC (4) et l'équipement de gestion d'identifiants (64) échangent des paramètres de chiffrement permettant de calculer, de part et d'autre, des accréditations, ledit profil temporaire intégrant lesdites accréditations.

[Revendication 6] Procédé selon l'une quelconque des revendications 1 à 5, dans lequel l'équipement de gestion d'identifiants (64) reconnaît l'eUICC (4) à qui fournir un identifiant d'abonnement temporaire à partir d'un paramètre d'identification de l'eUICC (EID) reçu de l'eUICC et présent dans une liste de paramètres d'identification d'eUICCs mémorisée par l'équipement de gestion d'identifiants (64).

[Revendication 7] Procédé selon l'une quelconque des revendications précédentes, dans lequel l'information à télécharger est un profil de souscription, le serveur étant un serveur de profils du type SM-DP.

[Revendication 8] Système pour la mise en œuvre du procédé de provisionnement d'un équipement utilisateur avec une information d'un opérateur final, selon l'une quelconque des revendications précédentes, comportant :
- un équipement utilisateur – UE (1), l'UE (1) étant muni d'une carte du type circuit intégré universelle embarquée – eUICC (4) et d'un module radio (5) pour se connecter ;
- un réseau IP (20) hébergeant un serveur (22) mémorisant ladite information ; et,
- un réseau de téléphonie mobile privé (10),
le réseau de téléphonie mobile privé (10) comportant :
- une connexion filaire ou non filaire au réseau IP (20) ;
- un serveur de profils d'abonné – HSS (18) ;
- un équipement de gestion d'identifiants (64), l'équipement de gestion d'identifiants (64) étant propre à : attribuer à l'eUICC (4) un identifiant d'abonnement temporaire (t-IMSI) ; à transmettre à l'eUICC (4) l'identifiant d'abonnement temporaire ; à créer un profil temporaire

spécifique de l'eUICC (1) ; et à mettre à jour le serveur de profils d'abonné – HSS avec ledit profil temporaire, ledit profil temporaire intégrant l'identifiant d'abonnement temporaire attribué à l'eUICC.

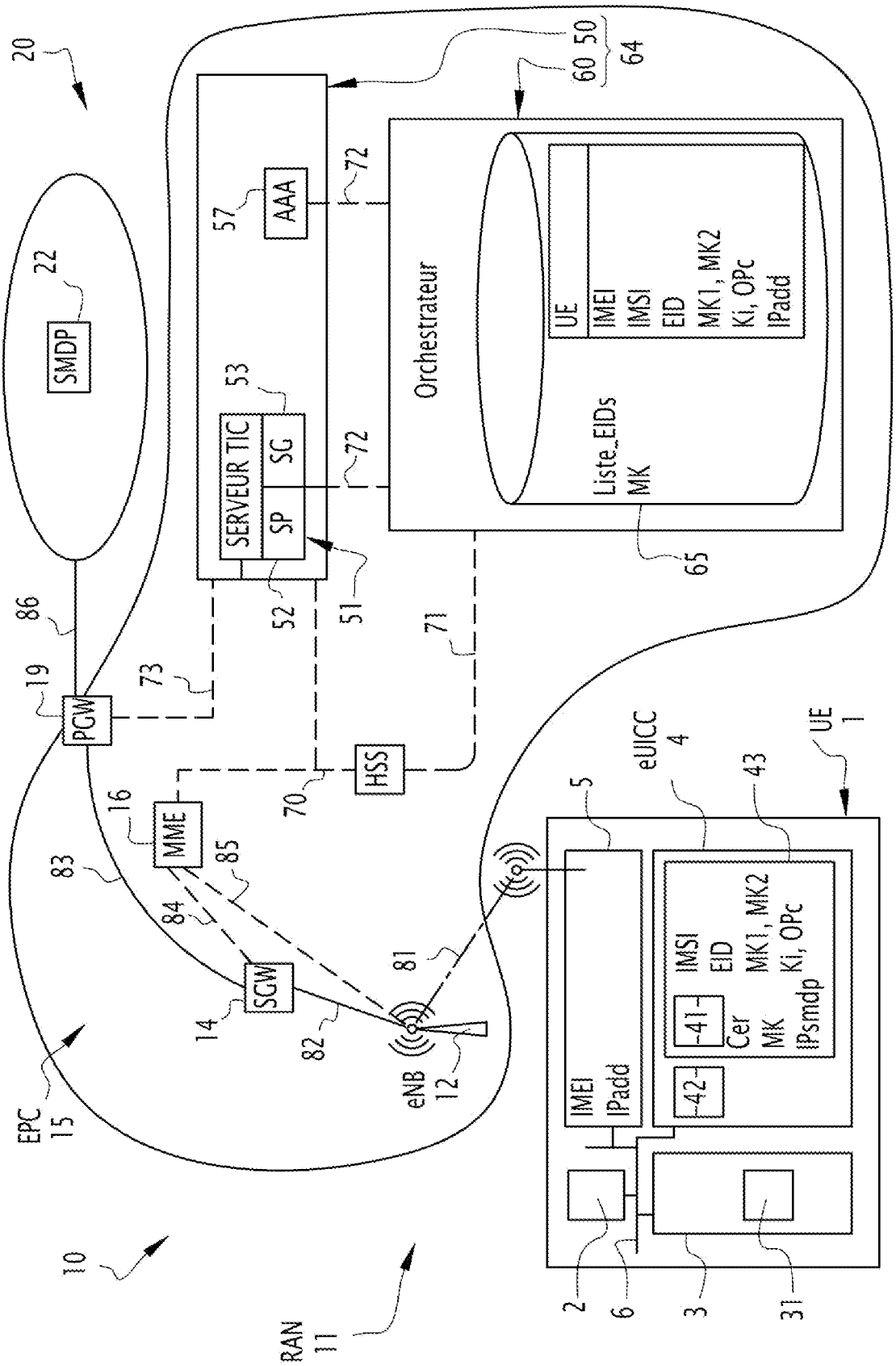
[Revendication 9] Réseau de téléphonie mobile privé (10) adapté pour être intégré dans un système selon la revendication 8.

[Revendication 10] Réseau de téléphonie mobile privé (10) selon la revendication 9, déployé à partir d'un ordinateur intégrant les différentes fonctionnalités d'un réseau de téléphonie mobile et adapté pour couvrir une zone géographique limitée.

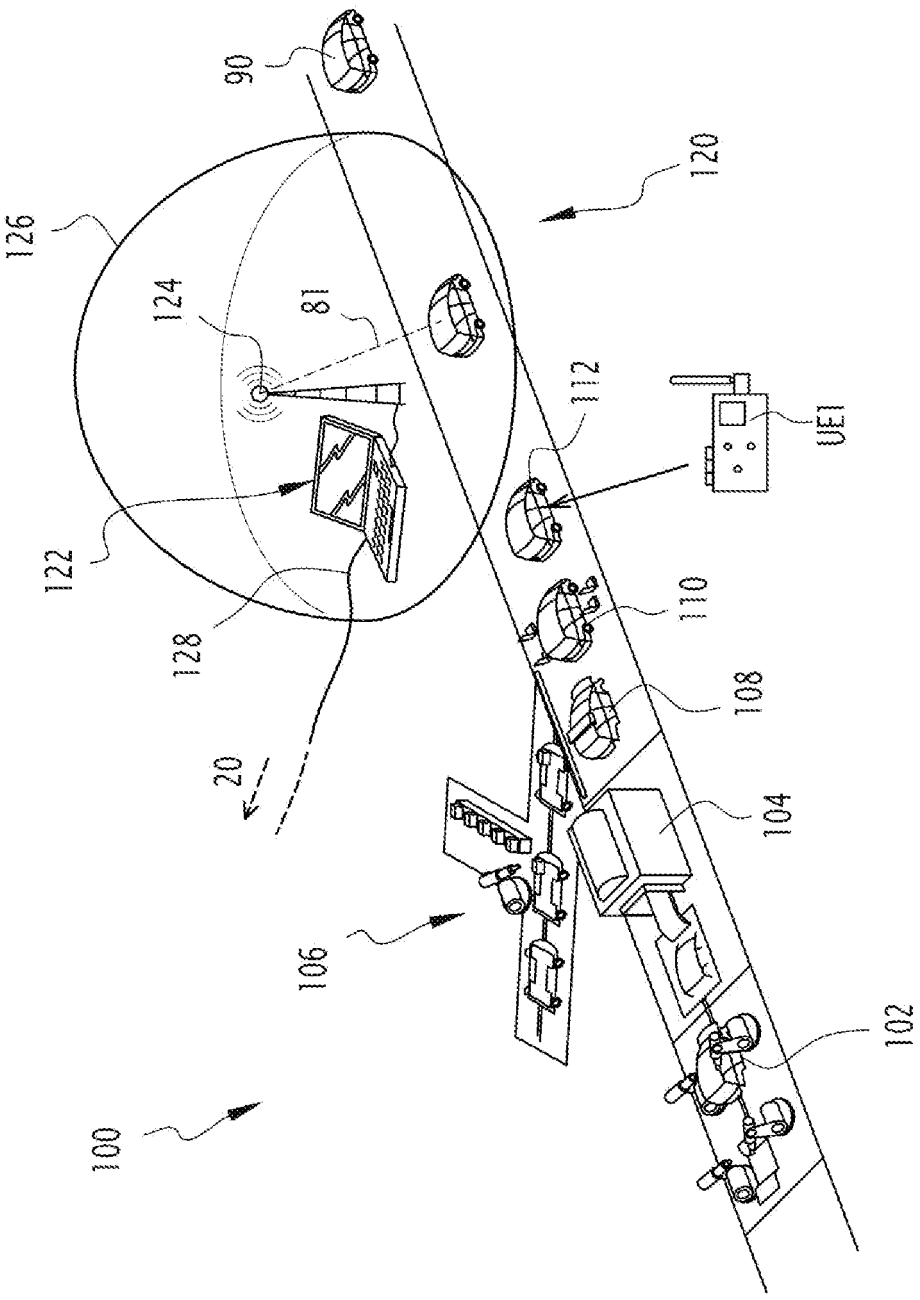
[Revendication 11] Chaîne de production d'équipement utilisateur – UE (1) comportant un poste de configuration des UEs (1) fabriquées, ledit poste intégrant un réseau de téléphonie mobile privé (10) selon la revendication 9 ou la revendication 10.

[Revendication 12] Produit programme d'ordinateur comportant des instructions logicielles qui, lorsqu'elles sont exécutées par un ordinateur, confèrent audit ordinateur la possibilité de fonctionner conformément au réseau de téléphonie mobile privé de la revendication 9 ou de la revendication 10, l'ordinateur ayant des moyens matériels adaptés pour constituer une station de base du réseau de téléphonie mobile privé et une connexion filaire ou non filaire à un réseau IP (20).

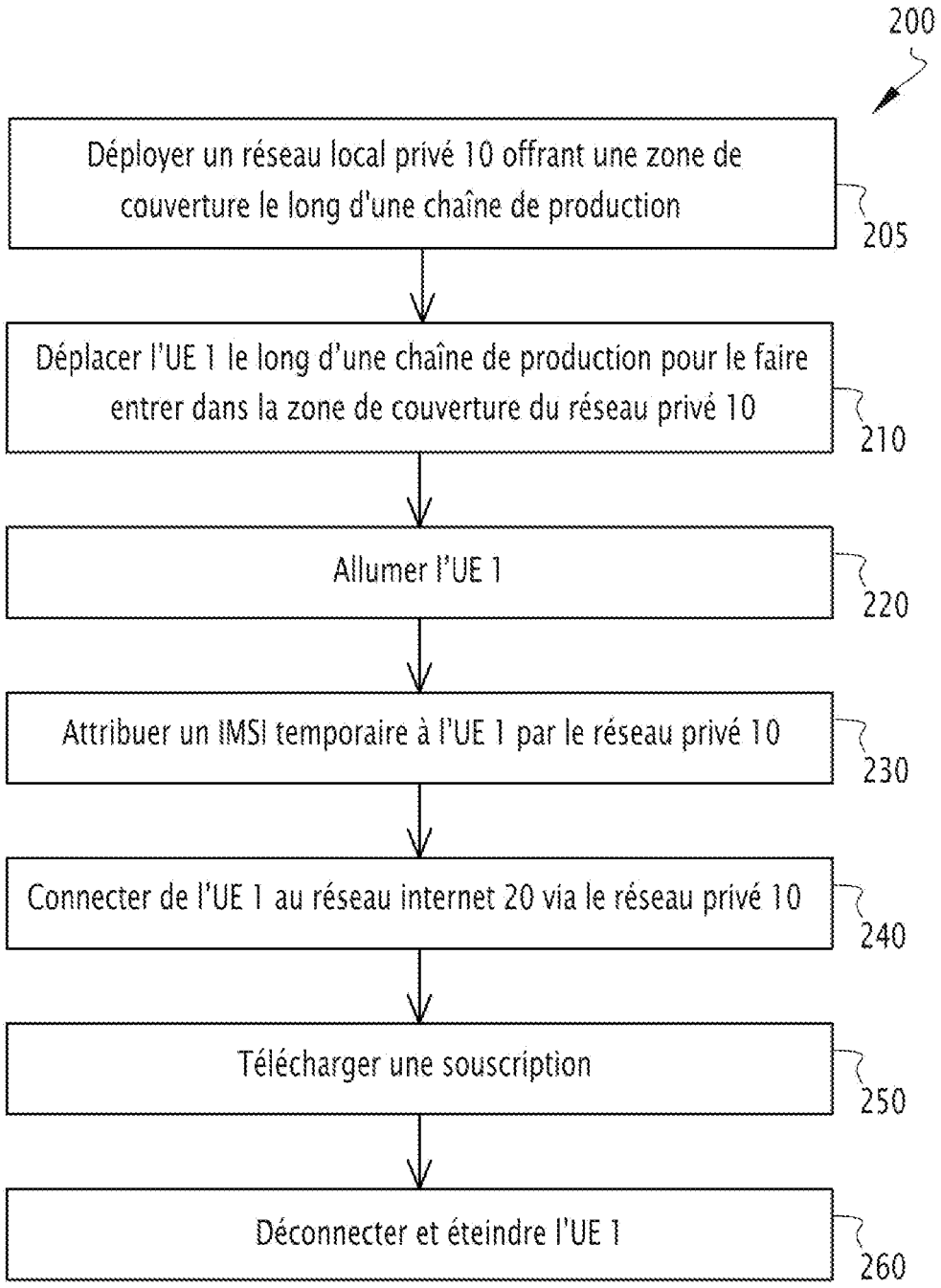
[Fig. 1]


20
60 50
64
22
SMDP
57
AAA
72
53
SERVEUR TIC
SG
SP
72
Orchestrateur
UE
IMEI
IMSI
EID
MK1, MK2
Ki, OPc
IPadd
Liste_EIDs
MK
65
52
51
71
86
19
PGW
73
HSS
70
16
MME
83
85
84
14
SGW
82
81
eNB
12
EPC
15
10
RAN
11
5
eUICC
4
43
UE
1
IMEI
IPadd
IMSI
EID
MK1, MK2
Ki, OPc
41
Cer
MK
IPsmdp
42
2
6
3
31

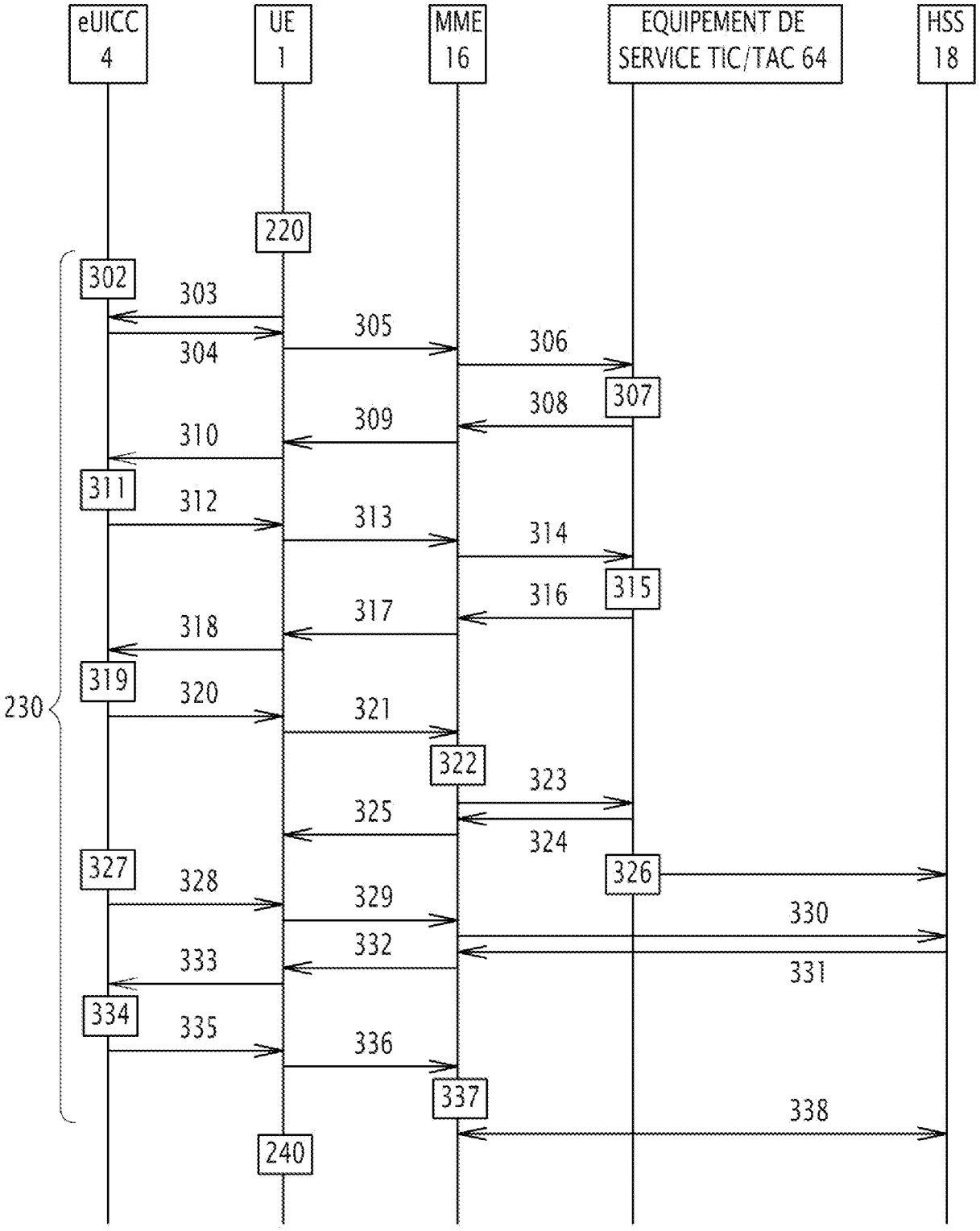
[Fig. 2]



[Fig. 3]


200
Déployer un réseau local privé 10 offrant une zone de couverture le long d'une chaîne de production
205
Déplacer l'UE 1 le long d'une chaîne de production pour le faire entrer dans la zone de couverture du réseau privé 10
210
Allumer l'UE 1
220
Attribuer un IMSI temporaire à l'UE 1 par le réseau privé 10
230
Connecter de l'UE 1 au réseau internet 20 via le réseau privé 10
240
Télécharger une souscription
250
Déconnecter et éteindre l'UE 1
260

[Fig. 4]


eUICC 4
UE 1
MME 16
EQUIPEMENT DE SERVICE TIC/TAC 64
HSS 18
220
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
240
230

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 916891
FR 2214570

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 2021/314765 A1 (ANSLOT MICHEL [FR] ET AL) 7 octobre 2021 (2021-10-07) * alinéa [0007] - alinéa [0237] * * figures 1-12 *	1-12	H04W 12/06 H04W 4/50 H04W 4/60 H04W 8/18
X	US 2020/236529 A1 (ANSLOT MICHEL [FR] ET AL) 23 juillet 2020 (2020-07-23) * alinéa [0001] - alinéa [0104] * * figures 1-3 *	1-12	
A	US 2021/258781 A1 (ANSLOT MICHEL [FR] ET AL) 19 août 2021 (2021-08-19) * alinéa [0001] - alinéa [0117] * * figures 1A-3C *	1-12	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W H04L

Date d'achèvement de la recherche	Examinateur
18 août 2023	Ghomrasseni, Z

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 2214570 FA 916891

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 **18-08-2023**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2021314765 A1	07-10-2021	BR 112019016200 A2	24-03-2020
		BR 112019016201 A2	07-04-2020
		CN 110447251 A	12-11-2019
		CN 110463237 A	15-11-2019
		CN 110622535 A	27-12-2019
		EP 3358867 A1	08-08-2018
		EP 3358868 A1	08-08-2018
		EP 3358869 A1	08-08-2018
		EP 3358870 A1	08-08-2018
		EP 3577921 A1	11-12-2019
		EP 3577922 A1	11-12-2019
		EP 3577923 A1	11-12-2019
		EP 3577924 A1	11-12-2019
		ES 2867388 T3	20-10-2021
		ES 2873829 T3	04-11-2021
		JP 6775090 B2	28-10-2020
		JP 6803481 B2	23-12-2020
		JP 6812565 B2	13-01-2021
		JP 6911156 B2	28-07-2021
		JP 2020505879 A	20-02-2020
		JP 2020507291 A	05-03-2020
		JP 2020508017 A	12-03-2020
		JP 2020511097 A	09-04-2020
		KR 20190131481 A	26-11-2019
		KR 20190134603 A	04-12-2019
		KR 20190134604 A	04-12-2019
		KR 20190139203 A	17-12-2019
		US 2019349766 A1	14-11-2019
		US 2020015069 A1	09-01-2020
		US 2020021973 A1	16-01-2020
		US 2020236538 A1	23-07-2020
		US 2021314765 A1	07-10-2021
		US 2021392489 A1	16-12-2021
		US 2023164542 A1	25-05-2023
		WO 2018141665 A1	09-08-2018
		WO 2018141889 A1	09-08-2018
		WO 2018141895 A1	09-08-2018
		WO 2018141896 A1	09-08-2018
		WO 2018141897 A1	09-08-2018
US 2020236529 A1	23-07-2020	CN 111373779 A	03-07-2020
		EP 3457728 A1	20-03-2019
		EP 3682657 A1	22-07-2020
		JP 7096881 B2	06-07-2022
		JP 2020533919 A	19-11-2020
		KR 20200053593 A	18-05-2020

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2214570 FA 916891

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 **18-08-2023**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
		US 2020236529 A1	23-07-2020
		WO 2019053009 A1	21-03-2019
US 2021258781 A1	19-08-2021	BR 112021003272 A2	18-05-2021
		CN 112655231 A	13-04-2021
		EP 3614706 A1	26-02-2020
		EP 3841769 A1	30-06-2021
		JP 7096947 B2	06-07-2022
		JP 2021534691 A	09-12-2021
		US 2021258781 A1	19-08-2021
		WO 2020038847 A1	27-02-2020

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82