(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 143 939***

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

(21) **N° d'enregistrement national :** **22 13627**

(51) Int Cl[8] : ***H 04 W 8/18*** *(2023.01), G 06 K 19/07*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.12.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 21.06.24 Bulletin 24/25.

(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) :** *IDEMIA France SAS* — FR.

(72) **Inventeur(s) :** DOS SANTOS Elder, DUMOULIN Jérôme et WOZNIAK Tomasz.

(73) **Titulaire(s) :** IDEMIA France SAS.

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

(54) MISE A JOUR DE PROFIL DANS UNE CARTE EUICC.

(57) L'invention concerne la mise à jour de profils d'abonné au sein d'eUICCs dans le cadre des procédures standardisées SGP.02 et SGP.22. Le terminal hôte de l'eUICC ou cette dernière reçoit (20), d'un serveur SM-DP, un package de profil partiel comportant des éléments de profil de mise à jour pour un profil cible. L'eUICC traite (22) le package de profil partiel pour mettre à jour les éléments de profil au sein dudit profil. Selon l'invention, le package de profil partiel est reçu du serveur SM-DP via une fonction de mise à jour d'éléments de profil distincte de la fonction LoadProfileElements de SGP.22 et de la fonction DownloadAndInstallation de SGP.02. Par exemple, les commandes ou segments TLV contenant les éléments de profil au sein du package de profil lié peuvent présenter un type différent de '86' (réservé pour les fonctions classiques ci-dessus), typiquement '90'.
(Figure 2)

FR 3 143 939 - A1

Description

Titre de l'invention : MISE A JOUR DE PROFIL DANS UNE CARTE EUICC

DOMAINE DE L'INVENTION

[0001] La présente invention concerne la gestion de profils d'abonné au sein d'éléments sécurisés, tels des eUICC (pour embedded UICC – ou UICC intégrée).

[0002] CONTEXTE DE L'INVENTION

[0003] Un terminal utilisateur sans fil, tel un téléphone portable, comporte traditionnellement un élément sécurisé utilisé pour s'authentifier sur le ou les réseaux de communication, typiquement de téléphonie mobile. De tels éléments sécurisés incluent les cartes de circuit intégré universelles UICC (pour « Universal Integrated Circuit Card »), notamment les cartes SIM (pour « Subscriber Identity Module » – ou module d'identité d'abonné), et leur version intégrée connue sous l'appellation eUICC (pour embedded UICC – ou UICC intégrée) aussi appelée eSIM. Un module eUICC est un élément matériel sécurisé, généralement de petite taille, pouvant être intégré dans un terminal mobile hôte afin de mettre en œuvre les fonctions d'une carte SIM traditionnelle.

[0004] Les eUICCs peuvent comprendre plusieurs abonnements ou profils correspondant chacun à un opérateur différent. Chaque profil comprend des données de souscription, par exemple un identifiant IMSI (pour « International Mobile Subscriber Identity »), des clés cryptographiques et des algorithmes, spécifiques à un abonnement fourni par un opérateur de téléphonie mobile.

[0005] Les cartes eUICC offrent une plus grande flexibilité dans la gestion des abonnements, et notamment dans la fourniture et la gestion à distance des profils. Les cartes eUICC sont en effet reprogrammables et permettent donc, dans le temps, de charger, supprimer et mettre à jour plusieurs profils d'abonné (ou profils de communication) au sein de la même carte eUICC. Chaque profil d'abonné est contenu dans un conteneur sécurisé (noté ISD-P pour « Issuer Security Domain Profile » qui ne peut contenir qu'un seul profil) qui contient, comme une carte SIM classique, les données permettant, lorsque le profil est actif, de s'authentifier auprès d'un réseau correspondant de téléphonie mobile pour accéder à un service (par exemple de voix ou de données).

[0006] En changeant le profil d'abonné actif dans la carte eUICC, il est possible de changer d'opérateur ou de modifier l'accès à des services associés.

[0007] La spécification « SGP.22 - RSP Technical Specification – Version 2.3 – 30 June 2021 », ci-dessous « SGP.22 », décrit notamment une solution technique de fourniture

et gestion à distance des eUICCs dans des terminaux grand public (« Consumer Devices »). Les procédures décrites sont typiquement à l'initiative du terminal (incluant l'eUICC).

[0008] La spécification « SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification - Version 4.2 – 07 July 2022 », ci-dessous « SGP.02 », décrit une solution technique de fourniture et gestion à distance des eUICCs intégrées aux terminaux M2M (« machine to machine »). Les procédures décrites sont typiquement à l'initiative d'un serveur, dénommé SM-DP ou SM-DP+ (pour « Subscription Manager Data Preparation »).

[0009] Des procédures typiques de gestion des eUICC comme décrites dans ces spécifications incluent, entre autres, le chargement et l'installation de profil, l'activation de profil, la désactivation de profil, la suppression de profil et d'ISD-P.

[0010] Un inconvénient de ces spécifications est qu'elles ne permettent pas la mise à jour de profils déjà installés, si ce n'est par une couteuse double procédure de suppression d'un profil existant et de chargement et installation d'un nouveau profil incorporant la mise à jour.

[0011] Des solutions classiques palliant ce manque s'appuient sur des plateformes OTA (« Over-the-air ») de l'opérateur mobile, envoyant des messages SMS à l'eUICC (via le terminal) pour mettre à jour le profil dans l'eUICC. Il est donc nécessaire que ce profil soit actif afin d'offrir la connectivité OTA, en plus de la mise en place de telles plateformes.

[0012] Le document US 2018/294949 propose une solution alternative qui s'affranchit de la plateforme OTA pour s'appuyer sur le serveur traditionnel SM-DP. Elle nécessite cependant une forte adaptation des protocoles standardisés dans la spécification SGP.22.

Résumé de l'invention

[0013] Il existe donc un besoin de solutions techniques adaptées à la fois au mode « Consumer » et au mode « M2M », qui soient plus en adéquation avec les procédures standardisées dans SGP.02 et SGP.22.

[0014] A cet effet, l'invention concerne un procédé de mise à jour d'une carte de circuit intégré universelle, eUICC, intégrée à un terminal hôte et comportant un profil, le procédé comprenant les étapes suivantes :

[0015] recevoir, d'un serveur de préparation de données de gestion d'abonnement SM-DP, un package de profil partiel comportant un ou plusieurs éléments de profil de mise à jour, et

[0016] traiter, par l'eUICC, le package de profil partiel pour mettre à jour le ou les éléments de profil au sein dudit profil,

[0017] caractérisé en ce que le package de profil partiel est reçu via une fonction (ou commande) de mise à jour d'éléments de profil distincte de la fonction LoadProfileElements définie dans la spécification SGP.22 « RSP Technical Specification – Version 2.3 – 30 June 2021 » et de la fonction DownloadAndInstallation définie dans la spécification SGP.02 « Remote Provisioning Architecture for Embedded UICC Technical Specification - Version 4.2 – 07 July 2022 » ou via une fonction (ou commande) de chargement distincte de la fonction LoadBoundProfilePackage définie dans la spécification SGP.22. L'emploi de fonctions distinctes des fonctions classiques pour le chargement et l'installation d'un profil permet à l'eUICC d'identifier, sans équivoque, que le package de profil reçu concerne une mise à jour de profil et non une opération classique d'installation de profil. L'eUICC peut alors mettre en œuvre une routine dédiée à la mise à jour de profil.

[0018] L'usage d'une fonction dédiée permet de conserver le reste des protocoles traditionnels de chargement des éléments de profil jusqu'à l'ISD-P, comme définis dans les spécifications SGP.02 et SGP.22. Par exemple, le package de profil partiel peut être transmis dans un package de profil lié (ou Bound Profile package dans SGP.22).

[0019] Des caractéristiques optionnelles de modes de réalisation de l'invention sont définies dans les revendications dépendantes.

[0020] Dans un mode de réalisation, le package de profil partiel est codé, au sein d'un package de profil lié reçu du serveur SM-DP, sous forme de commandes (ou segments) type-longueur-valeur, TLV, dont le type est différent de '86'. Cela permet, au serveur SM-DP, d'indiquer directement à l'ISD-P cible une mise à jour en conservant le protocole classique d'installation, à savoir, pour le mode « Consumer », la séquence d'une commande TLV en clair correspondant à la fonction InitialiseSecureChannel, suivie de commandes TLV '87' correspondant à la fonction ConfigureISDP, suivies de commandes TLV '88' correspondant à la fonction StoreMetadata, suivies de commandes TLV '87' optionnelles correspondant à la fonction ReplaceSessionKeys, suivies des commandes TLV de mise à jour codant le package de profil partiel (ses PEs de mise à jour).

[0021] Dans un autre mode de réalisation, le package de profil partiel est reçu du serveur SM-DP par un assistant local de profil du terminal hôte, LPAd, qui transfère le package de profil partiel à l'eUICC à l'aide d'une fonction de chargement distincte de la fonction LoadBoundProfilePackage définie dans la spécification SGP.22 « RSP Technical Specification – Version 2.3 – 30 June 2021 ».

[0022] Selon un mode de réalisation, l'assistant LPAd détermine qu'un package de profil reçu est un package de profil partiel par la détection d'un indicateur de mise à jour dans au moins l'un parmi :

[0023] des métadonnées de profil (Profile Metadata) en clair au sein d'un package de profil

lié codant ledit package de profil partiel reçu,

[0024] un code entré par un utilisateur du terminal hôte et initiant une opération d'obtention du package de profil reçu,

[0025] un événement obtenu d'un serveur distant et initiant une opération d'obtention du package de profil reçu.

[0026] Dans un autre mode de réalisation, à détection de la fonction de mise à jour ou de chargement distincte, l'eUICC exécute une routine de mise à jour du profil à partir du package de profil partiel reçu, distincte d'une routine d'installation d'un profil dans l'eUICC. Aussi, l'eUICC, ici l'ISD-P cible, adopte un fonctionnement différent (de celui pour l'installation de profil) à détection de la fonction dédiée à la mise à jour de profil.

[0027] Dans un autre mode de réalisation, la routine de mise à jour du profil met en œuvre une ou plusieurs règles parmi :

[0028] lorsqu'un élément de profil non vide dudit package est déjà présent dans ledit profil de l'eUICC, mettre à jour l'élément de profil de l'eUICC déjà présent avec le contenu dudit élément de profil du package de profil partiel,

[0029] lorsqu'un élément de profil non vide dudit package est absent dudit profil de l'eUICC, ajouter l'élément de profil du package de profil partiel audit profil de l'eUICC,

[0030] lorsqu'un élément de profil vide dudit package de profil partiel est déjà présent dans ledit profil de l'eUICC, supprimer l'élément de profil déjà présent dudit profil de l'eUICC.

[0031] L'invention concerne aussi une carte de circuit intégré universelle, eUICC, intégrable à un terminal hôte et comportant un profil, l'eUICC comprenant un processeur configuré pour recevoir, d'un serveur de préparation de données de gestion d'abonnement SM-DP, un package de profil partiel comportant un ou plusieurs éléments de profil de mise à jour, et traiter le package de profil partiel pour mettre à jour le ou les éléments de profil au sein dudit profil, caractérisé en ce que

[0032] le package de profil partiel est reçu via une fonction de mise à jour d'éléments de profil distincte de la fonction LoadProfileElements de SGP.22 et de la fonction DownloadAndInstallation de SGP.02 ou via une fonction (ou commande) de chargement distincte de la fonction LoadBoundProfilePackage de SGP.22.

[0033] Les caractéristiques décrites ci-dessus en lien avec le procédé sont transposables à la carte eUICC.

[0034] Un système peut comprendre une telle carte eUICC et un terminal hôte intégrant ladite carte eUICC.

[0035] L'invention vise aussi un support d'informations lisible par un microprocesseur, comprenant des instructions d'un programme d'ordinateur pour mettre en œuvre le

procédé défini plus haut, lorsqu'elles sont chargées et exécutées par le micro-processeur.

[0036] Ce 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.

[0037] Le support d'information peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comprendre un moyen de stockage, tel qu'une ROM, par exemple une ROM de microcircuit, ou encore un moyen d'enregistrement magnétique, par exemple un disque dur, ou encore une mémoire flash.

[0038] D'autre part, le support d'information 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. Le programme peut en particulier être téléchargé sur une plateforme de stockage d'un réseau de type Internet, de type communication, ou bien de type télécommunication.

[0039] Alternativement, le support d'information peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du ou des procédés en question.

BREVE DESCRIPTION DES FIGURES

[0040] D'autres particularités et avantages de l'invention apparaîtront encore dans la description ci-après, illustrée par les figures ci-jointes qui en illustrent des exemples de réalisation dépourvus de tout caractère limitatif. Sur les figures :

- la [Fig.1] illustre, de façon schématique, une structure d'un système pour la gestion de profils dans une eUICC intégrée à un terminal hôte utilisateur, tel qu'il ressort de la norme SGP.22 (mode Consumer) ;
- la [Fig.1a] illustre la communication d'un package de profil à installer en mode Consumer avec un assistant LPAd dans le terminal utilisateur ;
- la [Fig.2] illustre, à l'aide d'un ordinogramme, une réalisation de l'invention selon certains modes de réalisation ;
- la [Fig.3] illustre un package de profil et les différents états d'un tel package entre sa génération et son chargement dans l'eUICC, tels que définis dans SGP.22 (mode Consumer) ;
- la [Fig.4] illustre, à l'aide d'un ordinogramme, un exemple de routine de mise à jour d'un profil mis en œuvre par un ISD-P cible lors du traitement d'un package de profil partiel reçu, selon des modes de réalisation de l'invention ; et

- la [Fig.5] et la [Fig.5a] **illustrent des échanges de message pour la mise à jour d'un profil d'eUICC selon des modes de réalisation de l'invention.**

DESCRIPTION DETAILLEE DE L'INVENTION

[0041] La présente invention s'intéresse à la gestion d'éléments sécurisés tels que des eUICC, et notamment à la gestion de profils d'abonnés dans ces eUICC.

[0042] Un élément sécurisé, dénoté SE, est un composant ou plate-forme matérielle inviolable (typiquement une puce) utilisée dans un terminal hôte et capable d'héberger, de façon sûre, des applications et des données en conformité avec des règles et des exigences de sécurité fixées par des autorités de confiance.

[0043] Parmi les trois facteurs de forme d'un SE, l'UICC définit une puce physique qui contient l'application authentifiant un utilisateur dans un réseau de téléphonie mobile pour accéder à des services (voix, données, etc.). A cet effet, elle contient des applications telles que l'application USIM (Universal Subscriber Identity Module – ou module d'identité d'abonné universel) détenant les informations d'identification de l'abonné et permettant son authentification dans le réseau mobile.

[0044] Une eUICC est une puce UICC qui est intégrée, de façon amovible ou soudée, dans un terminal hôte. Il a été envisagé des mécanismes permettant de gérer, de façon sécurisée, différents abonnements au sein de la même carte eUICC comme décrits dans les spécifications SGP.02 pour le mode M2M et SGP.22 pour le mode Consumer.

[0045] La [Fig.1] illustre, de façon schématique, une structure d'un système pour la gestion de profils dans une eUICC intégrée à un terminal hôte utilisateur, tel qu'il ressort de la norme SGP.22 (mode Consumer). Le mode M2M s'appuie sur une architecture similaire dans laquelle cependant les modules LPA (intermédiaires principalement dédiés à des interactions avec l'utilisateur final) ne sont pas mis en œuvre puisque les opérations sont initiées par les serveurs.

[0046] Un réseau de téléphonie mobile 100 est illustré, correspondant par exemple à un opérateur de téléphonie mobile MNO (pour « Mobile Network Operator »). De façon connue, plusieurs réseaux peuvent coexister, correspondant à plusieurs opérateurs et ainsi plusieurs profils sur les terminaux utilisateurs.

[0047] Le réseau de téléphonie mobile 100 comporte une unité de routage sécurisé SM-SR 110 d'un serveur de gestion d'abonnement SM (non représenté pour une meilleure lisibilité), une unité de préparation de données SM-DP 120 d'un (même) serveur de gestion d'abonnement et des serveurs 130 propres à l'opérateur MNO gérant ce réseau de téléphonie mobile. Les fonctions principales, bien connues, de ces unités/serveurs sont décrites par la suite. Bien que les serveurs SM-SR et SM-DP soient représentés séparés, ils peuvent être mis en œuvre au sein d'un même serveur (dénoté SM-DP+). La présente invention s'applique également à d'autres architectures de réseau de té-

léphonie mobile.

[0048] Un serveur SM-DP+ 120 comprend, de façon simplifiée, une fonction de génération de package de profil 121 (Profile Package Binding) et une fonction de fourniture de package de profil 122 (Profile Package Delivery). Dans le cas d'un serveur SM-DP accompagné d'un serveur SM-SR, la fonction de fourniture de package de profil est réalisée par le serveur SM-SR.

[0049] Un terminal utilisateur 200, par exemple un téléphone portable, un smartphone, un ordinateur, une tablette, etc., comporte une carte eUICC 300 pour accéder de façon sécurisée aux services du réseau mobile 100.

[0050] Sur la figure, seul un terminal utilisateur 200 embarquant une carte eUICC est représenté. Bien entendu, le réseau de téléphonie mobile inclut généralement une pluralité de tels terminaux mobiles équipés de cartes eUICC (ou SIM, UICC). La présente description s'intéresse aux cartes eUICC à titre d'exemple. D'une façon générale, la présente invention peut être mise en œuvre dans tout type d'élément sécurisé SE contenant une pluralité de profils d'abonné, par exemple des éléments sécurisés embarqués, ou « eSE ».

[0051] Le terminal utilisateur 200 comporte un système d'exploitation OS apte à contrôler une interface de communication (non représentée) avec le réseau mobile et à réaliser l'interfaçage entre cette interface de communication et la carte eUICC 300, ainsi qu'une interface utilisateur (clavier, écran, etc.) 210 permettant à un utilisateur (dans le mode Consumer notamment) d'interagir.

[0052] Dans un mode de réalisation relatif au mode Consumer, l'OS comporte un assistant local de profil, LPAd, 220 offrant des services de gestion des profils. A titre d'exemple, ces services peuvent inclure un service de découverte locale de profil (LDS pour « Local Discovery Service ») pour connaître les profils P présents dans l'eUICC 300 et leur état actif ou inactif, un service de chargement de profil local (LPD pour « Local Profile Download ») pour réaliser les opérations séquentielles de chargement ou mise à jour d'un profil P et un service d'interface utilisateur local (LUI pour « Local User Interface ») pour récupérer/acquérir les actions de management de profils initiées localement par l'utilisateur (chargement, activation, désactivation, ...).

[0053] Dans un autre mode de réalisation relatif au mode « Consumer », l'assistant local de profil est embarqué dans l'eUICC. Il est alors dénommé LPAe (référence 330 en pointillés).

[0054] La carte eUICC 300 comprend un système d'exploitation OS_{eUICC} (stocké en mémoire non-volatile type morte ou flash par exemple) couplé à une mémoire non volatile MEM. Le système d'exploitation met en œuvre des fonctions (non représentées) dans le domaine télécom (Telecom framework) et pour la gestion des profils, typiquement un interpréteur de package de profile (Profile Package Interpreter) et un moteur de

politique de profil (Profile Policy Enabler). D'autres composants classiques présents dans la carte eUICC sont ici non représentés pour des raisons de clarté : interface (et contrôleur associé) de communication avec le terminal hôte, mémoire vive, bus de donnés, processeur, etc.

[0055] Conformément aux standards susvisés, la carte eUICC 300 comprend, en mémoire non volatile MEM, plusieurs domaines de sécurité pour la gestion de la carte et de profils d'abonné, chaque domaine de sécurité étant identifié par un AID (Application Identifier) unique:

[0056] un domaine de sécurité d'autorité de contrôle de l'eUICC 305 (ECASD pour « Embedded UICC Controlling Authority Security Domain ») responsable du stockage sécurisé d'informations d'identification (credentials) nécessaires aux domaines de sécurité de l'eUICC ;

[0057] un domaine racine ou privilégié de sécurité d'émetteur 310 (ISD-R pour « Issuer Security Domain – Root ») défini, à la fabrication de l'eUICC, comme représentatif du propriétaire de la carte 300 et donc accessible (via un jeu de clés cryptographiques particulier) uniquement par lui. Dans le mode Consumer, l'ISD-R 310 comporte des services LPA aptes à établir un dialogue avec l'assistant LPAd 220 ou LPAe 330 ;

[0058] un ou plusieurs domaines de sécurité de profil 320 (ISD-P pour « Issuer Security Domain – Profile ») généralement dédiés chacun à un opérateur MNO. Chaque domaine ISD-P est un conteneur sécurisé (protégé par un jeu de clés cryptographiques notamment) prévu pour stocker, de façon sécurisée, un unique profil d'abonné P associé à une souscription de service auprès de l'opérateur MNO correspondant et pour permettre son accès. L'un des ISD-P peut comprendre un profil initial par défaut (dit « provisioning profile ») permettant une connectivité réseau avec l'unité SM-SR 110. Le profil d'abonné est identifié par un identifiant unique ICCID (pour « Integrated Circuit Card IDentifier »).

[0059] L'ISD-P comporte une routine utilisée pour le téléchargement et l'installation du profil en collaboration avec l'interpréteur de package de profil pour le décodage et l'interprétation d'un package de profil à installer, reçu dans un canal sécurisé (par exemple selon SCP03t). Un package de profil est notamment conforme à la spécification Trusted Connectivity Alliance : « eUICC Profile Package : Interoperable Format Technical Specification », Version 3.2, dite « spécification TCA » dans la suite du document.

[0060] De façon connue, un profil de communication P comporte des données de souscription (par exemple un identifiant IMSI, des clés cryptographiques, des algorithmes d'authentification et application NAA d'accès au réseau, etc.) et peut comporter en outre un système de fichiers, des applications App, et/ou des règles d'exécution prédéterminées.

[0061] Selon les standards susvisés, un profil est composé de composants de profil (Profile Components) incluant :

[0062] un MNO-SD (domaine de sécurité de l'opérateur) comportant des clés OTA de l'opérateur pour permettre l'établissement d'un canal OTA sécurisé,

[0063] des domaines de sécurité supplémentaires (SSD) et d'un domaine de sécurité CASD,

[0064] d'applications/applets (App),

[0065] d'au moins une application d'accès réseau (NAA pour « Network Access Application »),

[0066] d'un système de fichier (File system),

[0067] de métadonnées de profil (Profile Metadata) incluant notamment des paramètres de connectivité (Connec Param) et des règles de politique de profil (POL1 par exemple). Ces métadonnées peuvent notamment inclure un identifiant ICCID (pour « Integrated Circuit Card Identifier » ou identifiant de carte à circuit intégré) qui identifie de manière unique le profil.

[0068] Bien qu'il soit illustré un unique profile P (ISD-P), la carte eUICC 300 peut comprendre une pluralité de domaines de sécurité ISD-P et ainsi une pluralité de profils chacun pouvant être à l'état actif ou inactif. Chaque profil ou ISD-P correspondant est identifié par un ICCID.

[0069] Le domaine de sécurité racine ISD-R est privilégié en ce qu'il est notamment apte à créer ou supprimer des domaines de sécurité ISD-P dans la mémoire non volatile MEM, et à activer ou désactiver des profils P chargés dans les ISD-P 320 de l'eUICC.

[0070] De façon connue des spécifications susvisées, cette gestion est réalisée par l'échange de messages (commandes, réponses) entre l'unité SM-SR 110 (ou le SM-DP+) et le domaine racine ISD-R 310. Les différentes fonctions et commandes de gestion de l'eUICC 300 sont définies dans ces documents SGP.02 pour le mode M2M et SGP.22 pour le mode Consumer. La communication entre l'unité SM-SR 110 et l'ISD-R 310 peut être portée par le protocole http et être assurée et/ou protégée par le protocole SCP80, SCP81 ou CAT-TP.

[0071] Le chargement, la mise à jour ou la suppression de façon sécurisée des profils dans les domaines sécurisés ISD-P 320 est réalisée par l'échange de messages (commandes, réponses) entre l'unité SM-DP 120 et chaque domaine sécurisé ISD-P concerné de l'eUICC 300. L'unité SM-DP 120 prépare notamment les packages de profil à charger dans l'eUICC, puis les envoie au domaine ISD-P 320 concerné, via l'unité SM-SR 110 et l'ISD-R 310. A nouveau des messages APDU sont utilisés. La communication entre l'unité SM-DP 120 et l'ISD-P 320 (via le SM-SR 110) peut être portée par le protocole http et être protégée par le protocole SCP02 ou SCP03 ou SCP03t, elle-même « tunnelée » ou encapsulée dans le lien SM-SR – ISD-R protégé par le protocole SCP80, SCP81 ou CAT-TP.

[0072] La [Fig.1a] illustre la communication d'un package de profil à installer en mode Consumer avec un assistant LPAd 220 dans le terminal utilisateur 200. Une connexion sécurisée, libellée ES9+ dans SGP.22, est établie entre la fonction de fourniture de package de profil 122 et l'assistant LPAd 220 (ou LPAe 330 dans la variante où celui-ci est implémenté). Une seconde connexion sécurisée, libellée ES8+ dans SGP.22, est établie entre la fonction de fourniture de génération de profil 121 et l'eUICC 300, plus précisément l'ISD-R 310. La seconde connexion est « tunnelée » au sein de la connexion ES9+ et d'une troisième connexion entre l'assistant LPA et l'ISD-R 310. Les mécanismes de sécurisation des connexions par clé sont décrits dans SGP.22.

[0073] Le package de profil ainsi communiqué à l'ISD-R est transmis, dans l'eUICC, à l'ISD-P cible pour installation du profil. L'ISD-P cible est identifié par l'ICCID présent dans les métadonnées de profil.

[0074] Des mécanismes similaires sont mis en œuvre dans le mode M2M où la communication avec le SM-DP+ ou SM-SR est réalisée, à l'initiative de ce dernier, directement avec l'ISD-P cible.

[0075] Lorsqu'un profil d'abonné P ainsi chargé est activé par le SM-SR 110 ou SM-DP+ (ou en variante par l'utilisateur via un menu sur le terminal utilisateur 200), il est équivalent à une UICC : il permet à l'utilisateur de s'identifier sur le réseau mobile 100 de l'opérateur MNO auquel il a souscrit l'abonnement correspondant au profil afin d'accéder à des services.

[0076] L'opérateur MNO 130 peut aussi accéder directement, par OTA (Over The Air – par exemple par SMS), au profil P actif (et notamment à certaines actions prévues par l'opérateur dans ce profil) pour réaliser des actions de diverses natures (notamment la gestion à distance d'un composant du profil 320, par exemple une mise à jour de données ou d'offre ou de règles d'exécution, etc.). De façon réciproque, des applications dans le profil P actif peuvent être configurées pour transmettre des données au MNO 130. Ces échanges sont illustrés sur la [Fig.1] par une flèche double sens entre le MNO 130 et le profil P.

[0077] La mise à jour d'un profil dans l'eUICC (peu importe le composant de profil visé) est essentielle pour une bonne gestion des eUICCs. La communication OTA est l'unique accès permettant une mise à jour des données de profil. La communication classique depuis le serveur SM-DP 120, pour une mise à jour de profil, requiert en effet une suppression de profil suivi d'une installation d'un nouveau profil mis à jour, ce qui entraîne des communications inutiles.

[0078] La communication OTA présente cependant certains inconvénients : d'une part, elle n'est possible que pour un profil actif ; d'autre part, elle requiert l'utilisation d'une plateforme OTA dédiée, ce qui peut s'avérer coûteux pour l'opérateur.

[0079] L'invention permet de réutiliser le serveur SM-DP 120 (ou SM-DP+) tradition-

nellement dédié au chargement et à l'installation de nouveaux profils pour mettre à jour un profil dans l'eUICC. Elle permet de réutiliser les procédures existantes de chargement et installation de profil en limitant leur modification pour signaler qu'il s'agit d'une mise à jour. Elle s'appuie ainsi toujours sur le format de la spécification TCA des packages de profil en limitant son adaptation dans certains modes de réalisation.

[0080] La [Fig.2] illustre, à l'aide d'un ordinogramme, une réalisation de l'invention selon certains modes de réalisation. Ceux-ci définissent de nouvelles commandes envoyées par le serveur SM-DP pour charger des éléments de profil (PE pour « Profile Element ») de mise à jour, qui sont similaires aux commandes classiques de chargement d'éléments de profil d'un nouveau profil à installer. Ainsi, en identifiant ces nouvelles commandes, l'eUICC 300 est en mesure de distinguer les packages de profil reçus concernant une mise à jour de profil de ceux concernant une opération classique d'installation de profil. L'eUICC peut alors mettre en œuvre une routine dédiée à la mise à jour de profil.

[0081] Le serveur SM-DP 120 génère et stocke un package de profil de mise à jour pour l'eUICC concernée, par exemple celle de la [Fig.1]. Un package de profil de mise à jour est typiquement « partiel » en ce qu'il comporte un nombre généralement réduit d'éléments de profil PE (ceux à mettre à jour) par rapport à ceux repris dans la spécification TCA.

[0082] Un package de profil partiel comporte typiquement la différence (en termes de PEs) entre un profil installé et un profil cible souhaité.

[0083] La [Fig.3] illustre un package de profil et les différents états d'un tel package entre sa génération et son chargement dans l'eUICC, tels que définis dans SGP.22 (mode Consumer).

[0084] Le contenu d'un package de profil 30a est défini dans la spécification TCA susvisée et s'applique tant au mode Consumer qu'au mode M2M. Il comporte une collection d'éléments de profil (PE) qui sont décrits, et peuvent ainsi être traités par l'eUICC, indépendamment les uns des autres. Chaque PE est encodé comme une donnée TLV (type ou tag [étiquette], longueur, valeur) et comporte un entête contenant un identifiant de PE (OID pour « Object Identifier »), un drapeau indiquant si le PE est obligatoire, un type de PE et une longueur de PE.

[0085] Un élément de profil de type entête de profile 31a (Profile Header ou PH) est présent avant tout autre PE pour fournir des indications sur le contenu du profil. Les autres PE 32a (PE_1, PE_2, PE_n) décrivent par exemple les composants de profil évoqués plus haut (NAA, système de fichiers, applications, SSD, etc.). A titre illustratif, les éléments de profil suivants (liste non exhaustive) sont décrits dans la spécification TCA : PE-MF, PE-CD, PE-TELECOM, PE-USIM, PE-OPT-USIM, PE-SecurityDomain, PE-

Application, PE-PINCodes. Dans le cadre de l'invention, un package de profil partiel comporte de tels PEs correspondants aux PEs à mettre à jour sur le profil cible déjà installé dans l'eUICC. Un élément de profil de fin 33a (PE End) termine le package.

[0086] La fonction 121 du SM-DP+ 120 génère ainsi un package de profil non protégé 30a constitué d'une séquence de PE TLVs.

[0087] La même fonction 121 encode ces PE TLVs à l'aide de clés (clés de session convenues avec l'eUICC ou en variante des clés aléatoires de protection par profil) en utilisant une méthode encodage-puis-MAC (Encrypt-then-MAC method), incluant donc également le calcul d'un MAC (code d'authentification de message). La spécification SGP.22 se base sur la méthode SCP03t. Un package de profil protégé 30b est ainsi obtenu, qui est découpé en segments 31b de taille fixée, chaque segment étant identifié par un type '86' selon SGP.22.

[0088] La même fonction 121 du SM-DP+ 120 conduit alors une opération visant à lier le package protégé 30b à l'eUICC particulière, grâce à un accord préalable de clés entre l'eUICC et le SM-DP+ 120. Pour ce faire, un package de profil lié 30c (ou « Bound Profile Package ») est généré pour comprendre comme suit (dans cet ordre) :

[0089] une commande TLV en clair 31c, pour l'accord de clé correspondant à la fonction InitialiseSecureChannel de la procédure de chargement et d'installation d'un profil. Cette fonction permet au SM-DP+ d'ouvrir une nouvelle session RSP (pour « Remote SIM Provisioning ») avec l'eUICC 300,

[0090] un jeu de commandes TLV encodées 32c (par exemple selon SCP03t) relatives à des données de configuration de l'ISD-P. Elles correspondent à la fonction ConfigureISDP de la procédure de chargement et d'installation d'un profil. Ces commandes ConfigureISDP sont identifiables par un type '87',

[0091] un jeu de commandes TLV en clair 33c relatives à des métadonnées (Profile Metadata) concernant le profil en question aux fins du gestion locale du profil. Il s'agit par exemple de données en texte simple destinées à un affichage, par l'assistant LPA, à l'utilisateur, mais également de données telles que l'ICCID du profil, des services et applications obligatoires, etc.. Elles correspondent à la fonction StoreMetadata de la procédure de chargement et d'installation d'un profil. Ces commandes StoreMetadata sont identifiables par un type '88',

[0092] un jeu optionnel de commandes TLV encodées 34c (par exemple selon SCP03t) relatives à des clés de session SCP03t. Elles correspondent à la fonction ReplaceSessionKeys de la procédure de chargement et d'installation d'un profil. Ces commandes ReplaceSessionKeys sont identifiables par un type '87' et visent à remplacer les clés de session SCP03t par un nouveau jeu de clés,

[0093] suivi des segments 31b du package de profil protégé 30b, identifiés par le type '86' selon SGP.22 dans la procédure de chargement et d'installation d'un nouveau profil.

Ces segments définissent des commandes TLV correspondant à la fonction LoadProfileElements de la procédure classique de chargement et d'installation en mode « Consumer ».

[0094] Les événements déclencheurs de la mise à jour du profile de l'eUICC peuvent être multiples, notamment ceux connus pour le chargement et l'installation de nouveaux profils dès lors qu'ils visent un profil déjà chargé et installé dans l'eUICC. A titre d'exemple, un utilisateur peut scanner un QR code avec le terminal utilisateur 200 déclenchant un accès au serveur 120 (mode Consumer) ou le serveur SM-DP 120 peut lancer une campagne de mise à jour de terminaux (mode M2M). Egalement, en mode Consumer, le LPAd peut sonder un serveur de l'opérateur MNO ou d'une entité opératrice tierce tel qu'un organisme de télécommunication, comme par exemple un organisme investie d'une mission de défense d'intérêts d'opérateurs de téléphonie (exemple : organisme GSMA) et récupérer un événement EventID indicateur d'une mise à jour, ou être simplement configuré (autoconfiguration selon un contexte particulier) pour réaliser une mise à jour de profil à l'aide d'un SM-DP+ par défaut dont l'adresse est mémorisée dans l'eUICC.

[0095] De retour à la [Fig.2], à l'étape 20, le terminal (incluant l'eUICC) reçoit, du serveur SM-DP 120 (ou SM-DP+), un package de profil partiel comportant un ou plusieurs éléments de profil de mise à jour. En mode Consumer, le package de profil lié 30c est reçu par l'assistant LPA (LPAd 220 ou LPAe 330 selon le cas). En mode M2M, il est reçu par l'ISD-P cible de l'eUICC.

[0096] Dans un mode de réalisation, le serveur SM-DP utilise une fonction de mise à jour d'éléments de profil distincte de la fonction LoadProfileElements de SGP.22 (pour le mode Consumer) et de la fonction DownloadAndInstallation de SGP.02 (pour le mode M2M). LoadProfileElements et DownloadAndInstallation sont les fonctions utilisées pour le chargement et l'installation classique d'un nouveau profil. A titre illustratif, les nouvelles fonctions de mise à jour peuvent être nommées UpdateProfileElements pour le mode Consumer et DownloadAndUpdate pour le mode M2M.

[0097] Le SM-DP+ 120 peut ainsi générer le package de profil lié 30c de telle sorte que les segments 31b du package de profil protégé 30b soient identifiés par un type différent de '86' (et de '87' et '88'), par exemple '90' identifiant ainsi la commande UpdateProfileElements ou DownloadAndUpdate. Aussi, en cas de segments typés '86', l'eUICC saura qu'il s'agit d'une installation classique de nouveau profil, alors qu'en cas de segments typés '90', elle saura qu'il y a lieu de lancer une opération de mise à jour du profil.

[0098] A l'étape 22, lorsque le package reçu est détecté comme opérant une mise à jour de profil, l'eUICC traite le package de profil partiel reçu pour mettre à jour le ou les éléments de profil au sein du profil déjà installé.

[0099] Pour ce faire, le package de profil est aiguillé depuis le LPAd 220 (ou LPAe 330) vers l'ISD-P cible en mode Consumer, typiquement par l'usage de commandes LoadBoundProfilePackage définies dans la spécification SGP.22. En mode M2M, l'ISD-P dispose directement du package de profil pour la mise à jour.

[0100] L'ISD-P peut être actif (« enabled ») ou non (« disabled ») lors de la mise à jour du profil.

[0101] De façon similaire à l'installation d'un nouveau profil, la transmission du package de profil partiel comporte l'indication du profil (ou ISD-P) cible. Dans le mode Consumer, l'ICCID du profil cible est par exemple renseigné dans les Profile Metadata accompagnant le package de profil (dans les Store Metadata 33c du package de profil lié 30c dans SGP.22). Dans le mode M2M, l'AID de l'ISD-P cible est indiqué dans le champ X-Admin-Targeted-Application du message HTTP POST transmis à l'eUICC.

[0102] L'ISD-P détermine, grâce à l'identification de la fonction de mise à jour (type '90' des segments 31b, dans l'exemple ci-dessus), s'il s'agit d'une mise à jour de profil ou non. Dans l'affirmative, l'ISD-P bascule dans un mode « mise à jour » dans lequel il exécute une routine de mise à jour du profil P à réception du package de profil partiel, plutôt que la routine d'installation d'un nouveau profil. La [Fig.4] illustre un exemple de routine de mise à jour d'un profil.

[0103] Dans la négative, la procédure classique de chargement et d'installation de profil est mise en œuvre.

[0104] Dans une variante de réalisation à l'usage d'une fonction distincte de LoadProfileElements et DownloadAndInstallation, le package de profil partiel est conforme à ces fonctions (segments 31b typés '86') et est reçu par l'assistant LPAd 220. Ce dernier détermine qu'il s'agit d'un package de profil partiel pour mise à jour de profil par la détection d'un indicateur de mise à jour.

[0105] Dans un mode de réalisation, l'indicateur est présent dans les métadonnées de profil (Profile Metadata 33c) en clair au sein d'un package de profil lié codant ledit package de profil partiel reçu. Dans ce mode de réalisation, les Profile Metadata en clair (segments TLV dont le type vaut '88') comprennent un champ, spécifié par le SM-DP/SM-DP+ 120 à la génération du package, qui indique qu'il s'agit d'une mise à jour de profil. Le LPAd 220 lit ce champ.

[0106] Dans un autre mode de réalisation, l'indicateur est porté dans le QR code acquis par l'utilisateur pour initier l'opération de mise à jour, c'est-à-dire l'opération d'obtention du package de profil reçu.

[0107] Dans un autre mode de réalisation, l'indicateur est porté par l'EventID acquis auprès d'un serveur de l'opérateur MNO ou d'une entité opératrice tierce tel qu'un organisme de télécommunication, comme par exemple un organisme investie d'une mission de défense d'intérêts d'opérateurs de téléphonie (exemple : organisme GSMA) et qui

initie également l'opération de mise à jour, et donc l'opération d'obtention du package de profil reçu.

[0108] Lorsque le LPAd a déterminé qu'il s'agit d'un package de profil partiel (pour mise à jour), alors il le transfère à l'eUICC (l'ISD-P cible via l'ISD-R) à l'aide d'une fonction de chargement distincte de la fonction LoadBoundProfilePackage définie dans la spécification SGP.22 pour le chargement et l'installation de profil. Dans ce cas, l'ISD-P cible reçoit à l'étape 20 le package de profil partiel et, reconnaissant la fonction de chargement distincte, sait désormais qu'il s'agit d'une opération de mise à jour de profil.

[0109] L'ISD-P cible peut alors traiter le package de profil partiel reçu pour mettre à jour (étape 22) le ou les éléments de profil au sein du profil déjà installé. La routine de la [Fig.4] est alors mise en œuvre.

[0110] Lorsque la mise à jour de profil est réalisée alors que l'ISD-P du profil cible est inactif (« disabled »), l'ISD-P peut, suite à la mise à jour de son profil, être passé à l'état actif (« enabled ») de sorte à pouvoir profiter du profil mis à jour.

[0111] La [Fig.4] illustre, à l'aide d'un ordinogramme, un exemple de routine de mise à jour d'un profil mis en œuvre par un ISD-P cible lors du traitement d'un package de profil partiel reçu. Le traitement concerne ici les éléments de profil PEs de mise à jour une fois décodés (SCP03t), c'est-à-dire ceux contenus dans le package à l'exception du Profile Header PH et de l'élément de fin PE End.

[0112] Un élément de profil PE décrit dans le package est considéré comme vide s'il ne comporte que son entête (OID, champ optionnel indiquant s'il est obligatoire, type du PE, longueur du PE), sans contenu utile comme défini dans la spécification TCA. Le package peut donc comprendre un ou plusieurs PEs à traiter.

[0113] A l'étape 50, le PE suivant est sélectionné (dans l'ordre de déclaration au sein du package).

[0114] A l'étape 51, l'ISD-P vérifie si le PE sélectionné est vide ou non. Dans l'affirmative, le PE de même type (PE Type dans l'entête) est supprimé, à l'étape 52, du profil cible déjà installé. Ainsi, une première règle consiste, lorsqu'un élément de profil vide du package reçu est déjà présent dans le profil déjà installé (et donc à mettre à jour), à supprimer cet élément de profil déjà présent dans le profil de l'eUICC.

[0115] Suite à l'étape 52, la routine se poursuit à l'étape 59 qui détermine s'il reste un PE à traiter. Dans l'affirmative, la routine retourne à l'étape 50 pour sélectionner le PE suivant. Sinon, la routine prend fin.

[0116] Dans la négative du test 51 (PE sélectionné non vide), il est déterminé à l'étape 53 si le profil installé dans l'ISD-P comporte un PE du même type que le PE sélectionné.

[0117] Dans l'affirmative, le PE de même type au sein du profil installé est mis à jour, à l'étape 54, en remplaçant son contenu par le contenu du PE sélectionné. Ce rem-

placement peut être réalisé par la suppression du composant de profil correspondant puis par l'installation à nouveau de ce composant à partir du PE sélectionné. En variante, des valeurs du composant de profil déjà installé sont modifiées par des valeurs présentes dans le PE sélectionné (du package reçu) sans suppression intermédiaire du composant de profil.

[0118] Ainsi, une deuxième règle consiste, lorsqu'un élément de profil non vide du package reçu est déjà présent dans le profil installé, à mettre à jour l'élément de profil déjà présent avec le contenu de l'élément de profil du package.

[0119] Suite à l'étape 54, la routine se poursuit à l'étape 59 déjà décrite.

[0120] Dans la négative du test 53, le PE sélectionné définit un nouveau composant de profil à installer. Aussi, ce nouveau composant de profil est installé, à l'étape 55, dans le profil déjà existant, à partir du PE sélectionné.

[0121] Ainsi, une troisième règle consiste, lorsqu'un élément de profil non vide du package reçu est absent du profil déjà installé, à ajouter l'élément de profil du package au profil déjà existant.

[0122] Suite à l'étape 55, la routine se poursuit à l'étape 59 déjà décrite.

[0123] Grâce à cette routine, le ou les différents PEs de mise à jour contenus dans le package reçu sont traités successivement pour mettre à jour, de façon incrémentale, le profil déjà existant dans l'ISD-P, soit par suppression, soit par ajout, soit par modification d'un ou plusieurs composants de profil correspondant au PE ou PEs de mise à jour.

[0124] La [Fig.5] et la [Fig.5a] **illustrent des échanges de message pour la mise à jour d'un profil d'eUICC selon des modes de réalisation de l'invention. Ces échanges s'appuient sur les procédures décrites dans SGP.22 pour le chargement et l'installation d'un nouveau profil en mode Consumer. Certains échanges non utiles à l'invention (notamment entre l'opérateur MNO 130 et le SM-DP/SM-DP+ 120) sont volontairement omis afin de simplifier l'illustration.**

[0125] Les entités impliquées dans cette illustration sont le serveur SM-DP/SM-DP+ 120, l'assistant LPAd 220 du terminal utilisateur 200 et l'eUICC 300. Les détails de communication au sein de l'eUICC sont donc omis, notamment entre l'ISD-R (communiquant avec le LPAd) et l'ISD-P cible réalisant la mise à jour de son profil. Les enseignements décrits ci-après s'appliquent également à un assistant LPAe 330 au sein de l'eUICC, mais également au mode M2M dans lequel le package de profil est directement reçu par l'ISD-P cible (pas d'intervention d'un module LPA). Les échanges de messages correspondant au mode M2M sont décrits en sections 3.1.2 (pour l'authentification) et 3.1.3 (pour le chargement et l'installation d'un profil) de SGP.02.

[0126] Une condition de départ est détectée à l'étape 600. SGP.22 indique différentes conditions de départ possibles. Si un code d'activation est utilisé, celui-ci est fourni à

l'assistant LPAd par l'utilisateur, typiquement par saisie manuelle ou scan d'un QR code. Le code d'activation peut renseigner un profil cible ou en variante renseigner une mise à jour de profil, en plus de l'adresse du serveur SM-DP+ 120. Une autre condition de départ peut consister pour le LPAd à solliciter un serveur SM-DS auprès duquel il récupère une adresse du SM-DP+ 120 ainsi qu'un événement (EventID).

[0127] L'étape 600 déclenche ainsi une procédure d'authentification mutuelle 610 du LPAd avec le serveur SM-DP+ 120. Elle comporte l'établissement 611 d'une nouvelle session HTTPs en mode d'authentification de serveur, entre les deux entités, puis l'appel de la fonction InitiateAuthentification 612 permettant de passer un challenge et des informations d'eUICC (obtenus auprès de l'eUICC) au serveur SM-DP+. Ce dernier génère 613 alors un identifiant de transaction (TransactionID) identifiant la session RSP pour l'ensemble de la procédure de mise à jour. Il génère aussi un ensemble de données cryptographiques (serverChallenge, serverSigned1, server-Signature1), et transmet l'ensemble (incluant le Transaction ID) au LPAd à l'étape 614.

[0128] En réponse, le LPAd génère 615 une structure de données ctxParams1 comportant notamment un champ MatchingID renseignant le code d'activation ou l'EventID mentionné plus haut. Celle-ci et les données cryptographiques reçues sont transmises 616 à l'eUICC pour vérification et génération 617 de données cryptographiques d'eUICC, incluant une structure signée euiccSigned1 comprenant les données suivantes TransactionID, ctxParams1, serverChallenge et des données eUICCInfo2 de l'eUICC, ainsi qu'une génération d'une signature euiccSignature1 basée sur la structure signée euiccSigned1 générée.

[0129] Les données cryptographiques d'eUICC sont retournées 618a au LPAd puis transmises 618b au serveur SM-DP+ 120 comme paramètre d'un appel à la fonction AuthenticateClient.

[0130] Le serveur SM-DP+ 120 vérifie 619 ces données afin de conclure l'authentification mutuelle. A ce stade, le serveur SM-DP+ connaît donc le MatchingID (code d'activation ou l'EventID) correspondant à l'opération souhaitée pour l'eUICC.

[0131] Suite à une authentification 610 réussie, le SM-DP+ 120 détermine 620, à partir du MatchingID, qu'une mise à jour de profil est sollicitée. Le MatchingID peut directement renseigner un événement correspondant à une mise à jour de profil, par exemple un identifiant de package de profil partiel de mise à jour. En variante, le MatchingID peut correspondre à un profil, auquel cas le SM-DP+ 120 détermine si ce profil est déjà installé dans l'eUICC impliquée dans une version antérieure (à l'aide de données historiques), auquel cas un package de profil partiel de mise à jour doit être envoyé à l'eUICC.

[0132] Le SM-DP+ 120 génère 621 et échange 622 à nouveau des données cryptographiques

(smdpSigned2, smdpSignature2) avec l'eUICC, via le LPAd. Si une confirmation de l'utilisateur est nécessaire, des metadata de profil sont également générées à l'étape 621 et transmises 622 au LPAd qui affiche 623 une demande de confirmation, voire de saisie d'un code de confirmation, à l'utilisateur pour la poursuite de la procédure.

[0133] L'eUICC, plus précisément l'ISD-P, vérifie 624 les données cryptographiques reçues pour en déduire (ou générer) des clés de la session RSP et générer des données cryptographiques d'eUICC en retour (euiccSigned2, euiccSignature2). La donnée euiccSigned2 peut inclure la réponse de l'utilisateur (notamment dans le cas d'un code de confirmation saisi par celui-ci). Ces données cryptographiques d'eUICC sont retournées 625a au LPAd puis transmises 625b au serveur SM-DP+ 120 comme paramètre d'un appel à la fonction GetBoundProfilePackage destinée à récupérer le package de profil lié 30c correspondant à la mise à jour du profil.

[0134] Le serveur SM-DP+ 120 vérifie 626 ces données afin de conclure à une confirmation de chargement. Le code de confirmation peut notamment être vérifié par rapport à un code de référence.

[0135] En cas de confirmation, le serveur SM-DP+ 120 génère 627 le package de profil lié 30c comme décrit plus haut, en y intégrant les PEs qui doivent être mis à jour. Dans un mode de réalisation, les segments 31b sont identifiés par une type '90' (ou équivalente) afin d'identifier les commandes TLV comme des commandes de mise à jour.

[0136] Le package de profil lié 30c est transmis 628 au LPAd en réponse à la commande GetBoundProfilePackage.

[0137] La procédure se poursuit par l'installation de la mise à jour. Pour ce faire, le LPAd charge les commandes TLV successives dans l'eUICC (l'ISD-P) à l'aide de la fonction LoadBoundProfilePackage définie dans SGP.22.

[0138] Les commandes expliquées en lien avec la [Fig.3] sont successivement transmises.

[0139] Aussi, la commande TLV en clair 31c, pour l'accord de clé correspondant à la fonction InitialiseSecureChannel, est d'abord transmise 630, permettant à l'ISD-P d'obtenir les clés de session RSP.

[0140] Le LPAd transmet 631 ensuite les commandes TLV 32c relatives aux données de configuration de l'ISD-P (fonction ConfigureISDP) par un ou plusieurs appels à la fonction LoadBoundProfilePackage.

[0141] Puis le LPAd transmet 632 les commandes TLV en clair 33c relatives aux métadonnées de profil (fonction StoreMetadata) par un ou plusieurs appels à la fonction LoadBoundProfilePackage.

[0142] Puis, le LPAd transmet 633 les commandes TLV 34c relatives aux clés de session (fonction ReplaceSessionKeys) si présentes, par un ou plusieurs appels à la fonction LoadBoundProfilePackage.

[0143] Enfin, le LPAd transmet 634 les segments 31b relatifs au package de profil (fonction

LoadProfileElements ou en variante UpdateProfileElements) par un ou plusieurs appels à la fonction LoadBoundProfilePackage.

[0144] L'ISD-P cible identifie, grâce à la fonction de mise à jour transmettant le package de profil partiel (tag '90' des segments 31b), qu'il s'agit d'une mise à jour de profil et exécute alors la routine de mise à jour (par exemple [Fig.5]) comme exposé ci-dessus.

[0145] Si tous les PEs sont traités avec succès, la réponse au dernier appel LoadBoundProfilePackage contient un résultat positif de la mise à jour de profil, lequel est remonté 635 au serveur SM-DP+ 120. Ce dernier peut alors mettre à jour 636 ses bases de données des profils installés (notamment leurs versions) pour l'eUICC. Cela clôt la procédure de mise à jour.

[0146] Cet exemple de la [Fig.5] et de la [Fig.5a] **basé sur SGP.22 prévoit une séquence d'une commande TLV en clair correspondant à la fonction InitialiseSecureChannel, suivie de commandes TLV '87' correspondant à la fonction ConfigureISDP, suivies de commandes TLV en clair '88' correspondant à la fonction StoreMetadata, suivies de commandes TLV '87' optionnelles correspondant à la fonction ReplaceSessionKeys, suivies des commandes TLV de mise à jour (avec par exemple le tag '90') codant le package de profil partiel (ses PEs de mise à jour) sous forme encodée (SCP03t).**

[0147] Les mêmes enseignements sont applicables au protocole de SGP.02, la séquence de commandes pour la procédure de chargement et d'installation d'un profil (adaptée à la mise à jour selon l'invention) comprenant : des commandes TLV '84' correspondant à la fonction Initialize Update de SGP.02, suivies de commandes TLV '85' correspondant à la fonction External Authenticate, suivies de commandes TLV avec par exemple le tag '90' (au lieu de '86', afin d'identifier la mise à jour de profil) encapsulant le package de profil partiel (ses PEs de mise à jour) sous forme encodée (SCP03t).

[0148] Par ailleurs, l'exemple de la [Fig.5] et de la [Fig.5a] **est basé sur une commande TLV différente de LoadProfileElements et DownloadAndInstallation, mais en utilisant la fonction LoadBoundProfilePackage lorsque le LPAd 220 transmet le package de profil partiel à l'eUICC (ISD-P cible). En variante comme décrite plus haut, les fonctions classiques LoadProfileElements et DownloadAndInstallation peuvent être utilisées et le LPAd 220 transmet le package de profil partiel à l'eUICC (ISD-P cible) en utilisant une fonction distincte de la fonction classique LoadBoundProfilePackage.**

[0149] Les exemples qui précèdent ne sont que des modes de réalisation de l'invention qui ne s'y limite pas.

Revendications

[Revendication 1] Procédé de mise à jour d'une carte de circuit intégré universelle, eUICC, (300) intégrée à un terminal hôte (200) et comportant un profil (320), le procédé comprenant les étapes suivantes :
recevoir (20), d'un serveur de préparation de données de gestion d'abonnement SM-DP (120), un package de profil partiel (30a) comportant un ou plusieurs éléments de profil de mise à jour (32a), et
traiter (22), par l'eUICC, le package de profil partiel pour mettre à jour le ou les éléments de profil au sein dudit profil,
caractérisé en ce que le package de profil partiel est reçu via une fonction de mise à jour d'éléments de profil distincte de la fonction LoadProfileElements définie dans la spécification SGP.22 « RSP Technical Specification – Version 2.3 – 30 June 2021 » et de la fonction DownloadAndInstallation définie dans la spécification SGP.02 « Remote Provisioning Architecture for Embedded UICC Technical Specification - Version 4.2 – 07 July 2022 » ou via une fonction de chargement distincte de la fonction LoadBoundProfilePackage définie dans la spécification SGP.22.

[Revendication 2] Procédé selon la revendication 1, dans lequel le package de profil partiel (30a) est codé, au sein d'un package de profil lié (30c) reçu du serveur SM-DP, sous forme de commandes type-longueur-valeur, TLV, (31b) dont le type est différent de '86'.

[Revendication 3] Procédé selon la revendication 1 ou 2, dans lequel le package de profil partiel est reçu du serveur SM-DP par un assistant local de profil du terminal hôte, LPAd, qui transfère le package de profil partiel à l'eUICC à l'aide d'une fonction de chargement distincte de la fonction Load-BoundProfilePackage définie dans la spécification SGP.22 « RSP Technical Specification – Version 2.3 – 30 June 2021 ».

[Revendication 4] Procédé selon la revendication 3, dans lequel l'assistant LPAd détermine qu'un package de profil reçu est un package de profil partiel par la détection d'un indicateur de mise à jour dans au moins l'un parmi :
des métadonnées de profil en clair au sein d'un package de profil lié codant ledit package de profil partiel reçu,
un code entré par un utilisateur du terminal hôte et initiant une opération d'obtention du package de profil reçu,
un événement obtenu d'un serveur distant et initiant une opération

d'obtention du package de profil reçu.

[Revendication 5] Procédé selon l'une des revendications 1 à 4, dans lequel à détection de la fonction de mise à jour ou de chargement distincte, l'eUICC exécute une routine de mise à jour du profil à partir du package de profil partiel reçu, distincte d'une routine d'installation d'un profil dans l'eUICC.

[Revendication 6] Procédé selon la revendication 5, dans lequel la routine de mise à jour du profil met en œuvre une ou plusieurs règles parmi :
lorsqu'un élément de profil non vide dudit package est déjà présent dans ledit profil de l'eUICC, mettre à jour l'élément de profil de l'eUICC déjà présent avec le contenu dudit élément de profil du package de profil partiel,
lorsqu'un élément de profil non vide dudit package est absent dudit profil de l'eUICC, ajouter l'élément de profil du package de profil partiel audit profil de l'eUICC,
lorsqu'un élément de profil vide dudit package de profil partiel est déjà présent dans ledit profil de l'eUICC, supprimer l'élément de profil déjà présent dudit profil de l'eUICC.

[Revendication 7] Carte de circuit intégré universelle, eUICC, (300) intégrable à un terminal hôte (200) et comportant un profil (320), l'eUICC comprenant un processeur configuré pour recevoir, d'un serveur de préparation de données de gestion d'abonnement SM-DP (120), un package de profil partiel (30a) comportant un ou plusieurs éléments de profil de mise à jour (32a), et traiter le package de profil partiel pour mettre à jour le ou les éléments de profil au sein dudit profil, caractérisé en ce que :
le package de profil partiel est reçu via une fonction de mise à jour d'éléments de profil distincte de la fonction LoadProfileElements définie dans la spécification SGP.22 « RSP Technical Specification – Version 2.3 – 30 June 2021 » et de la fonction DownloadAndInstallation définie dans la spécification SGP.02 « Remote Provisioning Architecture for Embedded UICC Technical Specification - Version 4.2 – 07 July 2022 » ou via une fonction de chargement distincte de la fonction LoadBoundProfilePackage définie dans la spécification SGP.22.

[Revendication 8] Système comprenant une carte eUICC (300) selon la revendication 5 et un terminal hôte (200) intégrant ladite carte eUICC.

[Revendication 9] Support d'informations lisible par un microprocesseur, comprenant des instructions d'un programme d'ordinateur pour mettre en œuvre le procédé selon l'une des revendications 1 à 6, lorsqu'elles sont chargées

et exécutées par le microprocesseur.

[Fig. 1]

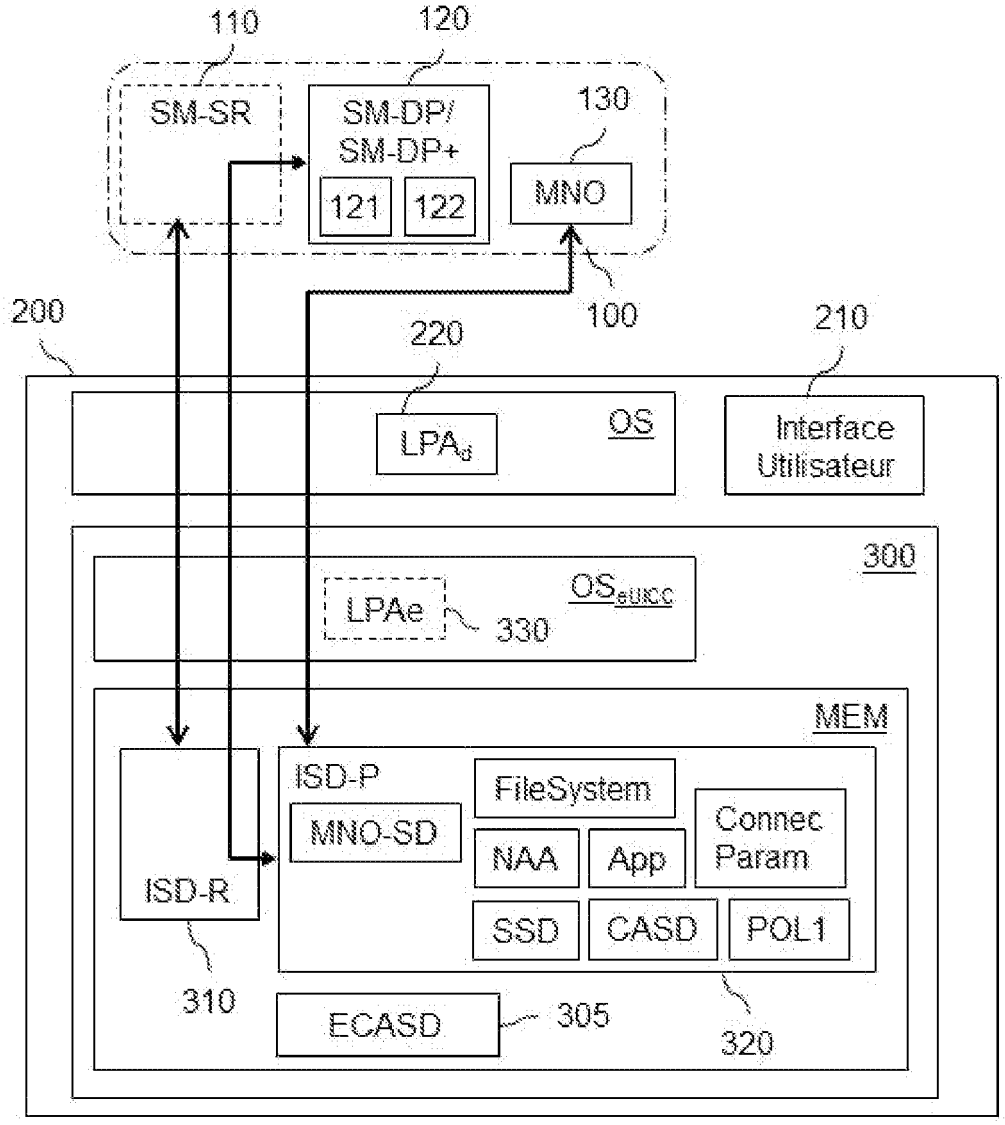

Fig.1

[Fig. 1a]

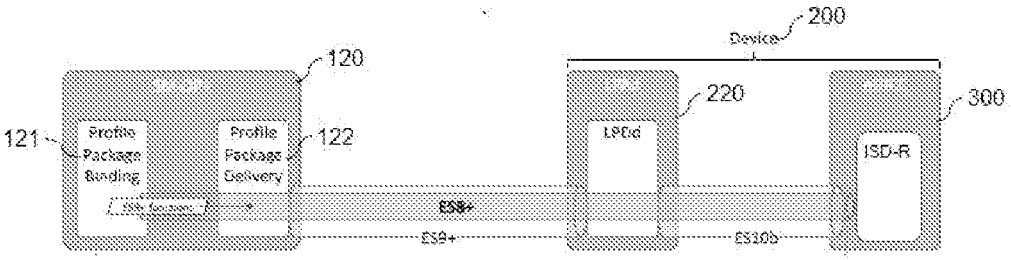

Fig.1a

[Fig. 2]

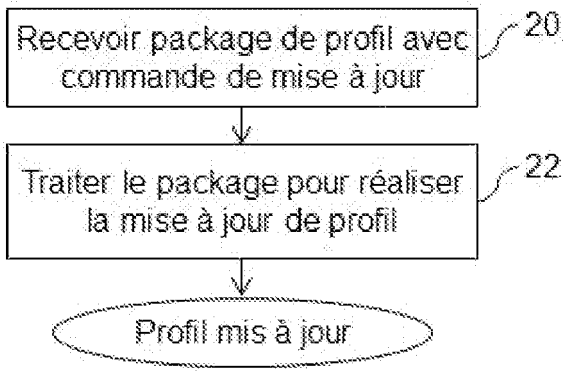

Fig.2

[Fig. 3]

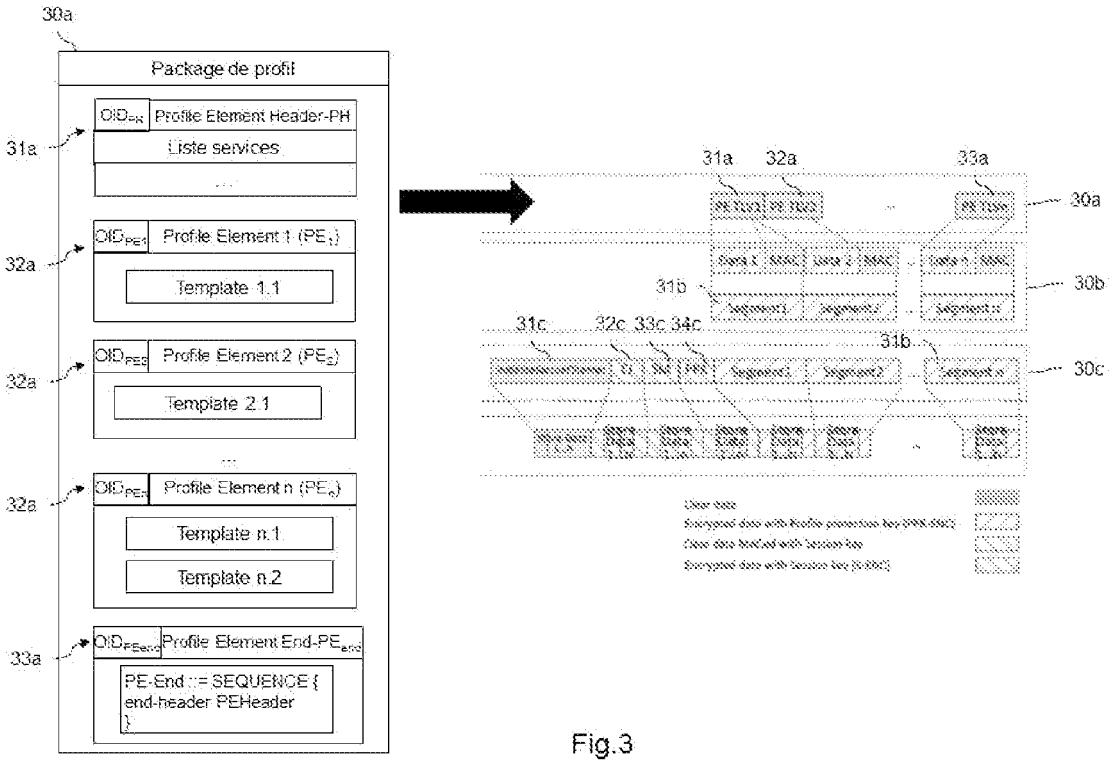

Fig.3

[Fig. 4]

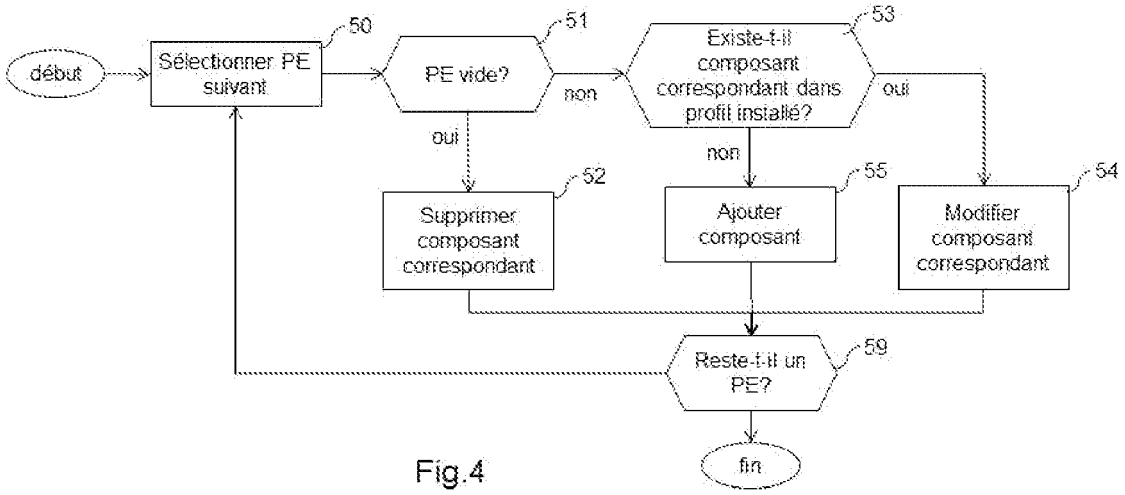

Fig.4

[Fig. 5]

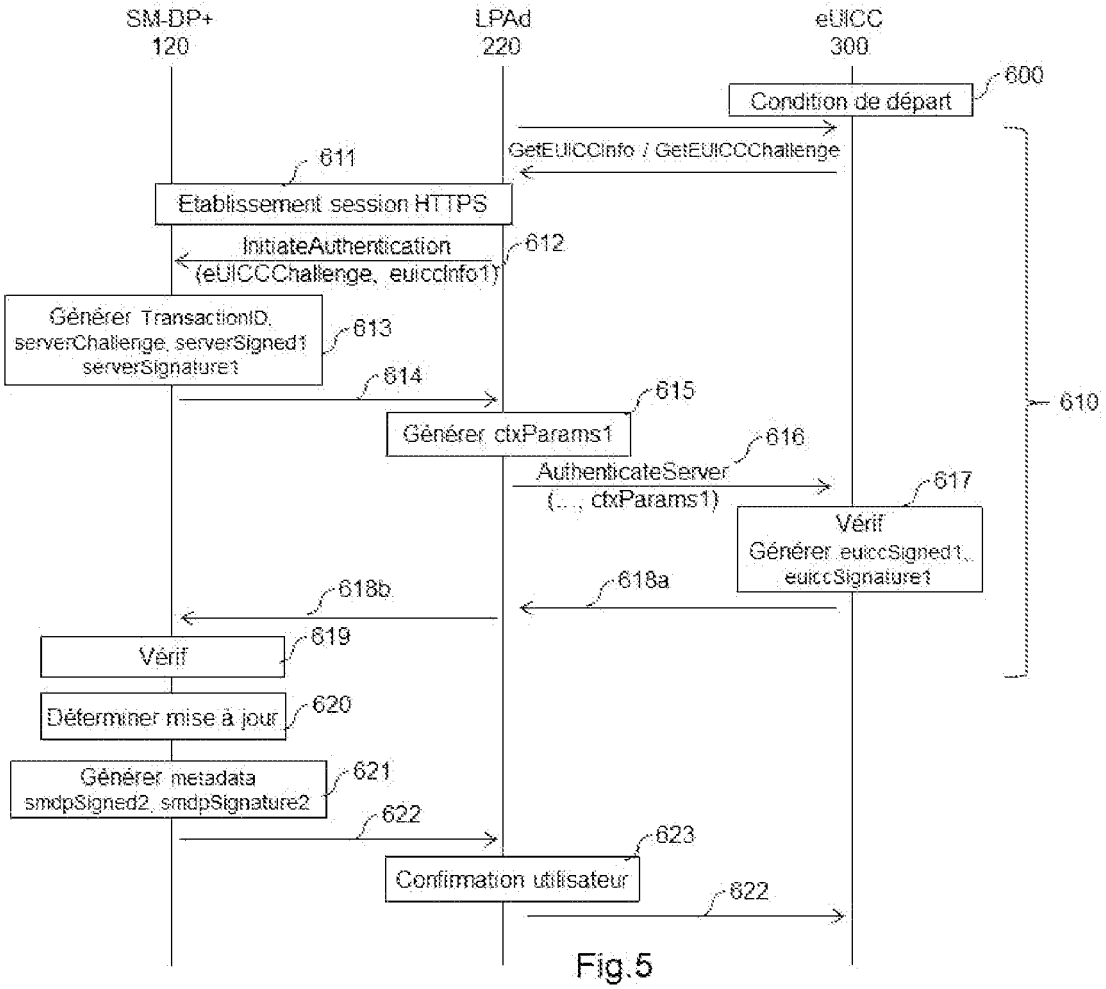
SM-DP+
120
LPAd
220
eUICC
300
600
Condition de départ
GetEUICCInfo / GetEUICCChallenge
611
Etablissement session HTTPS
InitiateAuthentication
(eUICCChallenge, euiccInfo1)
612
Générer TransactionID,
serverChallenge, serverSigned1
serverSignature1
613
614
615
Générer ctxParams1
610
616
AuthenticateServer
(..., ctxParams1)
617
Vérif
Générer euiccSigned1,
euiccSignature1
618b
618a
Vérif
619
Déterminer mise à jour
620
Générer metadata
smdpSigned2, smdpSignature2
621
622
623
Confirmation utilisateur
622

Fig.5

[Fig. 5a]

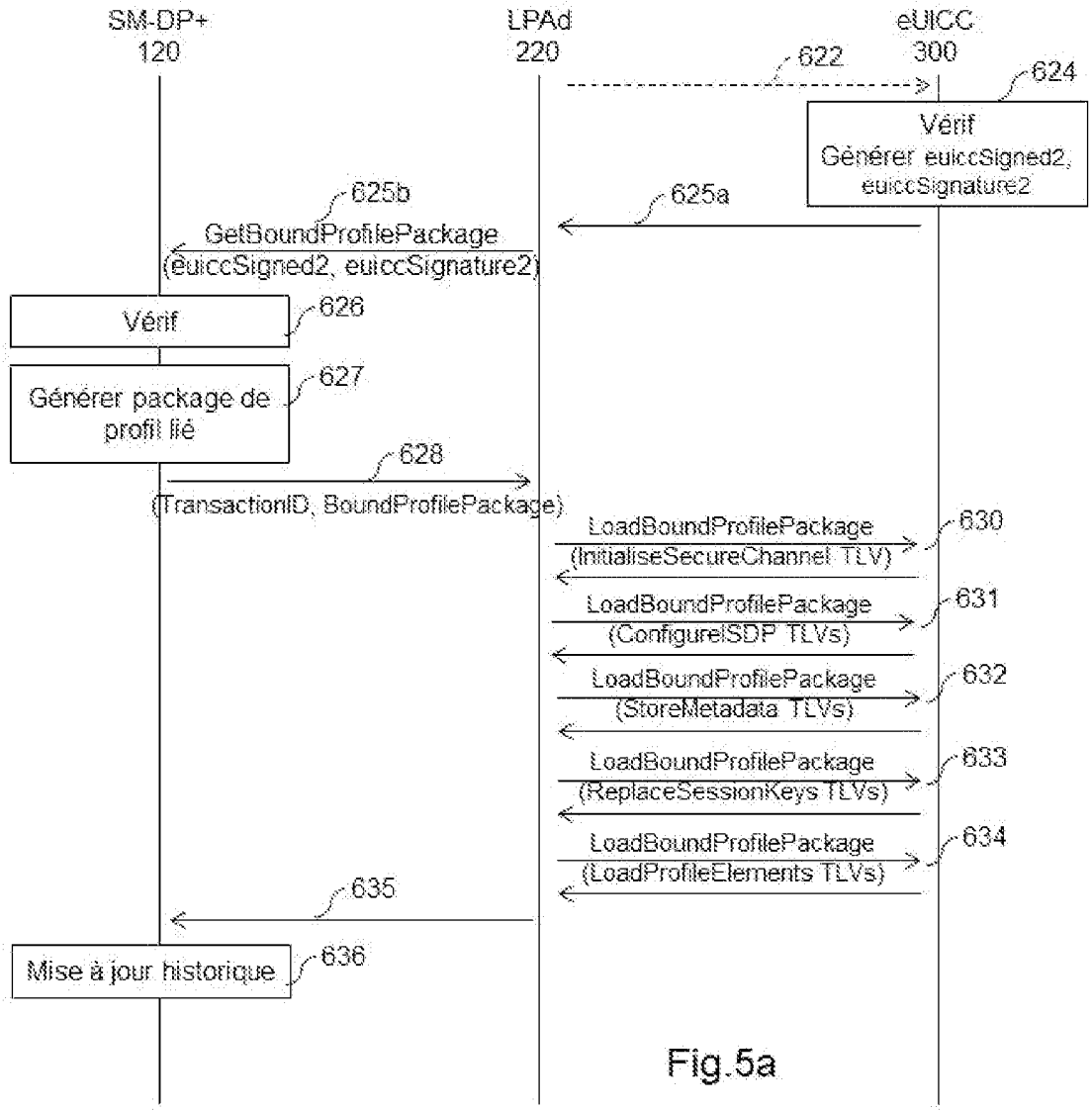
SM-DP+
120
LPAd
220
eUICC
300
622
624
Vérif
Générer euiccSigned2,
euiccSignature2
625b
625a
GetBoundProfilePackage
(euiccSigned2, euiccSignature2)
Vérif
626
Générer package de
profil lié
627
628
(TransactionID, BoundProfilePackage)
LoadBoundProfilePackage
(InitialiseSecureChannel TLV)
630
LoadBoundProfilePackage
(ConfigureISDP TLVs)
631
LoadBoundProfilePackage
(StoreMetadata TLVs)
632
LoadBoundProfilePackage
(ReplaceSessionKeys TLVs)
633
LoadBoundProfilePackage
(LoadProfileElements TLVs)
634
635
Mise à jour historique
636

Fig.5a

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 915851
FR 2213627

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 2022/150686 A1 (NITSCH NILS [DE]) 12 mai 2022 (2022-05-12) * alinéas [0005] - [0017], [0033], [0034], [0097] - alinéa [0102]; figures 1,3 *	1-9	G06K 19/07 H04W 8/18
X,D	US 2018/294949 A1 (YANG XIANGYING [US]) 11 octobre 2018 (2018-10-11) * alinéas [0031] - [0034]; figure 4 *	1,7-9	
X	WO 2016/128141 A1 (GIESECKE & DEVRIENT GMBH [DE]) 18 août 2016 (2016-08-18) * pages 3-7 *	1,7-9	
X	Gsm Association: "SGP.22 -RSP Technical Specification Version 2.0", , 14 octobre 2016 (2016-10-14), XP055325103, Extrait de l'Internet: URL:http://www.gsma.com/rsp/wp-content/uploads/docs_new/SGP.22_v2.0-Technical_Specification.pdf [extrait le 2016-12-01] * pages 16-17 *	2-4	
A	DE 10 2021 003391 B3 (GIESECKE DEVRIENT MOBILE SECURITY GMBH [DE]) 28 juillet 2022 (2022-07-28) * alinéas [0038] - [0041] *	1-9	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

H04W

Date d'achèvement de la recherche	Examinateur
17 juillet 2023	Tozlovanu, Ana-Delia

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 2213627 FA 915851

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 17-07-2023
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 2022150686 A1	12-05-2022	CN 113678484 A	19-11-2021
		DE 102019001840 B3	23-04-2020
		EP 3939344 A1	19-01-2022
		JP 2022535181 A	05-08-2022
		US 2022150686 A1	12-05-2022
		WO 2020187450 A1	24-09-2020
US 2018294949 A1	11-10-2018	US 2018294949 A1	11-10-2018
		US 2022385445 A1	01-12-2022
		US 2022385446 A1	01-12-2022
WO 2016128141 A1	18-08-2016	DE 102015001815 A1	18-08-2016
		WO 2016128141 A1	18-08-2016
DE 102021003391 B3	28-07-2022	DE 102021003391 B3	28-07-2022
		WO 2023274583 A1	05-01-2023

EPO FORM P0465