



(51) Classification internationale des brevets :
H04L 29/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2014/050306

(22) Date de dépôt international :
14 février 2014 (14.02.2014)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1351354 18 février 2013 (18.02.2013) FR

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

(72) Inventeurs : DUMOULIN, Jérôme; c/o Berthur Technologies, 420 rue d'Estienne d'Orves, F-92700 Colombes (FR). MICHEL, Alexis; c/o Berthur Technologies, 420 rue d'Estienne d'Orves, F-92700 Colombes (FR).

(74) Mandataires : DELUMEAU, François et al.; Cabinet Beau de Loménie, 158 rue de l'Université, F-75340 Paris Cedex 07 (FR).

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée :

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

(54) Title : METHOD FOR CREATING A PROFILE IN A SECURITY DOMAIN OF A SECURED ELEMENT

(54) Titre : PROCEDE DE CREATION D'UN PROFIL DANS UN DOMAINE DE SECURITE D'UN ELEMENT SECURISE

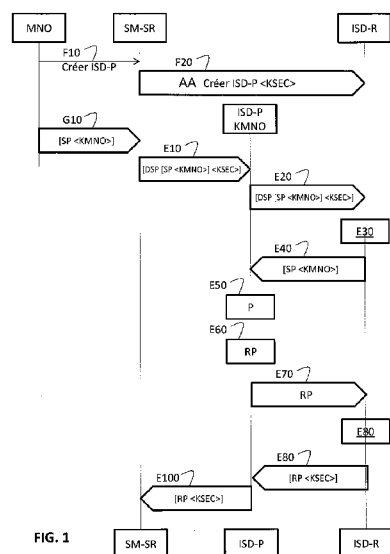


FIG. 1

AA Create

(57) Abstract : The invention relates to a method for creating a profile (P) in a target security domain (ISD-P) of a secured element (10), which comprises: a step (E10) of receiving, by means of said target security domain (ISD-P) and according to a secured protocol that cannot be interpreted by said security domain, data (DSP) comprising a script for installing said profile (P), which is encrypted with a key (KMNO) of the target security domain (ISD-P); a step (E20) of transferring data to a privileged security domain (ISD-R) capable of interpreting the protocol; a step (E30) of decrypting said protocol by means of said privileged security domain in order to obtain said encrypted script; a step (E40) of sending the encrypted script to said target security domain; a step (E50) of decrypting said script encrypted with said key and of executing said script by means of the target security domain (ISD-P), in order to install said profile (P).

(57) Abrégé : Ce procédé de création d'un profil (P) dans un domaine de sécurité cible (ISD-P) d'un élément sécurisé (10) comporte; une étape de réception (E10) par ledit domaine de sécurité cible (ISD-P), selon un protocole sécurisé non interprétable par ce domaine de sécurité, de données (DSP) comportant un script d'installation dudit profil (P) crypté avec une clef (KMNO) du domaine de sécurité cible (ISD-P); une étape (E20) de transfert des données à un domaine de sécurité privilégié (ISD-R) apte à interpréter le protocole; une étape (E30) de décryptage dudit protocole par ledit domaine de sécurité privilégié pour obtenir ledit script crypté;

[Suite sur la page suivante]



PROCEDE DE CREATION D'UN PROFIL DANS UN DOMAINE DE SECURITE D'UN ELEMENT SECURISE

Arrière-plan de l'invention

5

La présente invention se situe dans le domaine des terminaux comportant des éléments sécurisés dans lesquels peuvent être installés des profils.

10 L'invention s'applique en particulier et de façon non limitative aux terminaux dont les éléments sécurisés sont de type eUICC (« embedded UICC (Universal Integrated Circuit Card) ») et en particulier aux téléphones mobiles, aux téléphones intelligents ...

Pour plus de renseignement sur les éléments sécurisés UICC et eUICC, l'homme du métier se rapportera respectivement à la norme ETSI
15 102.221 et aux spécifications ETSI TS 103 383.

Dans ce document, la notion de « profil » doit être interprétée au sens large à savoir comme un ensemble d'au moins un fichier et/ou de données. Un profil au sens de l'invention peut notamment comprendre au moins un élément parmi :

- 20
- un fichier standard tel que défini par les spécifications du 3GPP ou de l'ETSI pour les UICC et leurs applications et notamment par les normes 3GPP 31.102 et ETSI 102.221 ;
 - un fichier propriétaire ;
 - un fichier de configuration d'un système d'exploitation ;

25

 - une application Java Card et des éléments de personnalisation associés ;
 - des données telles que des clefs de protocole de transport, des paramètres d'algorithme d'authentification, ...

Fonctionnellement, dans la plupart des cas notamment, un profil
30 comporte des données en relation avec un service ou avec une application particulière, par exemple une application bancaire de type NFC (Near Field Communication), une application de télécommunication ou une application coopérant avec un serveur distant via un réseau mobile.

Pour des raisons de sécurité, il est usuel et recommandé, afin de
35 cloisonner les différents services offerts par un terminal, d'enregistrer

chacun des profils associés dans un domaine de sécurité propre, tel que défini par le document « Global Platform Card Specification 2.2.1 ».

Une solution permettant de créer un nouveau domaine de sécurité dans un élément sécurisé pour y installer un nouveau profil est donc
5 souhaitable.

Dans l'état actuel de la technique, le GSMA recommande, pour la création et l'activation d'un nouveau domaine de sécurité, d'utiliser un système comportant un serveur de domaine de sécurité et un domaine de sécurité apte à communiquer avec ce serveur selon un protocole de
10 transport sécurisé, la sécurisation des échanges étant réalisée au moyen d'une clef partagée par ces deux entités.

Certains contextes, et notamment le projet eUICC de la GSMA recommandent d'utiliser des mécanismes de la norme Global Platform et en particulier celui selon lequel le nouveau domaine de sécurité et celui à
15 l'origine de sa création et de son activation (domaines père/fils au sens de la norme) soient isolés l'un de l'autre dès l'activation du domaine fils de sorte que le domaine de sécurité père n'est pas en mesure de charger un nouveau profil dans le domaine de sécurité fils.

Dans certains contextes, et notamment dans le projet eUICC de la
20 GSMA, le nouveau domaine de sécurité ne doit pas être en mesure de décrypter le protocole de transport sécurisé offert par ce serveur de domaine de sécurité.

L'invention vise une solution de chargement d'un nouveau profil dans un domaine de sécurité d'un élément sécurisé compatible avec
25 l'ensemble de ces contraintes.

Objet et résumé de l'invention

Ainsi, et d'une façon générale, l'invention concerne un procédé de
30 création d'un profil dans un domaine de sécurité cible d'un élément sécurisé comportant un domaine de sécurité privilégié apte à communiquer avec un serveur de domaine de sécurité selon un protocole de transport sécurisé non décryptable par le domaine de sécurité cible.

Ce procédé comporte :

35 - une étape de réception, par le domaine de sécurité cible, conformément au protocole de transport sécurisé, de données comportant un script

- d'installation du profil, ce script étant crypté avec au moins une clef connue du domaine de sécurité cible ;
- une étape au cours de laquelle le domaine de sécurité cible transfère les données audit domaine de sécurité privilégié selon le protocole de transport sécurisé ;
- 5
- une étape de décryptage du protocole de transport sécurisé par le domaine de sécurité privilégié pour obtenir le script crypté ;
 - une étape au cours de laquelle ledit domaine de sécurité privilégié envoie le script crypté au domaine de sécurité cible ;
- 10
- une étape de décryptage du script crypté par le domaine de sécurité cible en utilisant la ou les clefs précitées ; et
 - une étape d'exécution de ce script par le domaine de sécurité cible pour installer le profil dans ledit domaine de sécurité cible.

Corrélativement, l'invention vise un élément sécurisé comportant :

- 15
- un domaine de sécurité cible ; et un
 - un domaine de sécurité privilégié apte à communiquer avec un serveur de domaine de sécurité selon un protocole de transport sécurisé non décryptable par le domaine de sécurité cible ; et dans lequel
 - le domaine de sécurité cible comporte :
- 20
- des moyens de réception, conformément au protocole de transport sécurisé, de données comportant un script d'installation d'un profil crypté avec au moins une clef connue du domaine de sécurité cible ;
 - des moyens pour transférer ces données au domaine de sécurité privilégié selon le protocole de transport sécurisé ;
- 25
- le domaine de sécurité privilégié comporte :
 - des moyens de décryptage du protocole de transport sécurisé pour obtenir le script crypté ;
 - des moyens pour envoyer le script crypté au domaine de sécurité cible ;
- 30
- le domaine de sécurité cible comportant :
 - des moyens de décryptage du script crypté en utilisant la ou les clefs précitées ; et
 - des moyens d'exécution du script pour installer le profil dans le
- 35
- le domaine de sécurité cible.

Les clefs précitées sont des clefs pouvant notamment être utilisées à des fins de cryptage/décryptage et/ou à des fins d'authentification dans des mécanismes connus en soi de sécurisation cryptographique des échanges.

5 Par conséquent, selon l'invention, le script d'installation du profil est crypté avec au moins une première clef connue du domaine de sécurité cible, le profil crypté étant lui-même crypté selon le protocole de transport sécurisé décryptable par le domaine de sécurité privilégié.

10 Dans un mode de réalisation particulier, le procédé de création de profil selon l'invention comporte une étape de création et d'activation du domaine de sécurité cible par le domaine de sécurité privilégié. Cette pratique est conforme aux recommandations de la GSMA rappelées en préambule de ce document.

15 Préférentiellement, cette étape de création et d'activation du domaine de sécurité comprend l'exécution d'un script par le domaine de sécurité cible pour générer la ou les clefs précitées.

En pratique, cette ou ces clefs sont partagées entre le domaine de sécurité cible et l'entité, par exemple l'opérateur ou le fournisseur de service qui désire installer le profil dans ce domaine de sécurité.

20 Ainsi, le domaine de sécurité cible et cet opérateur/fournisseur de service peuvent communiquer dès l'activation du domaine de sécurité cible par le domaine de sécurité privilégié.

25 Dans un mode de réalisation particulier du procédé de création de profil selon l'invention, le domaine de sécurité cible transfère les données comportant le script d'installation crypté au domaine de sécurité privilégié en utilisant une interface GlobalService de la norme Global Platform.

30 On rappelle que l'interface GlobalService fonctionne selon un mécanisme de type question/réponse dans lequel une première application ayant demandé un service à une deuxième application reprend nécessairement la main après avoir obtenu ce service.

Dans un mode de réalisation particulier du procédé de création de profil selon l'invention, le protocole de transport sécurisé utilisé entre le serveur de domaine de sécurité et le domaine de sécurité privilégié est le protocole SCP80 ou SCP81.

35 Dans un mode de réalisation particulier du procédé de création de profil selon l'invention, le domaine de sécurité cible prépare une réponse

qu'il crypte avec une clef partagée avec l'entité ayant demandé la création du profil (par exemple l'opérateur) puis demande au domaine de sécurité privilégié de chiffrer cette réponse cryptée conformément au protocole de transport sécurisé pour transfert au serveur de domaine de sécurité.

5 Dans un mode particulier de réalisation de l'invention, les domaines de sécurité cible et privilégié sont conformes à la norme GlobalPlatform Card Specification 2.2.1.

Dans un mode particulier de réalisation, l'élément sécurisé selon l'invention est constitué par un composant eUICC tel que défini par la
10 norme ETSI 102 221.

Dans un mode particulier de réalisation, l'élément sécurisé selon l'invention est constitué par un circuit intégré.

L'invention vise aussi un terminal incorporant un élément sécurisé tel que mentionné ci-dessus, par exemple un téléphone mobile.

15 Ce terminal comporte de façon connue des moyens de communication propres pour communiquer avec le serveur de domaine de sécurité. Ces moyens de communication utilisent un protocole connu, par exemple le protocole SMS (Short Message service), le protocole CAT-TP lorsque le protocole de transport sécurisé est le protocole SCP80, ou le
20 protocole HTTP lorsque le protocole de transport sécurisé est le protocole SCP81.

Lorsque le terminal reçoit les données comportant le script crypté d'installation du nouveau profil, il les transmet préférentiellement à l'élément sécurisé selon l'invention au moyen de commandes APDU
25 (Application Protocol Data Unit) et/ou conformément à la norme ISO7816.

Brève description des dessins

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

- la figure 1 représente, sous forme d'organigramme, les principales étapes d'un procédé de création de profil conforme à un mode particulier de réalisation de l'invention ; et

- la figure 2 représente un élément sécurisé conforme à un mode particulier de réalisation de l'invention, incorporé dans un téléphone mobile.

5 Description détaillée de l'invention

En référence à la figure 1, nous allons maintenant décrire un exemple de mise en œuvre de l'invention dans lequel un opérateur MNO souhaite installer un nouveau profil P dans un élément sécurisé 10.

10 Pour que cette opération puisse être réalisée, il est nécessaire, au préalable de créer dans l'élément sécurisé 10 un domaine de sécurité cible réservé à ce nouveau profil P, ce domaine de sécurité cible étant ci-après référencé ISD-P (« Issuer Security Domain – Profile »).

La création du domaine de sécurité cible ISD-P s'effectue, sur
15 demande de l'opérateur MNO (étape F10) de façon connue, au cours d'une étape générale F20, et conformément aux recommandations du GSMA, en utilisant un serveur SM-SR (Subscription Manager Secure Routing) et un domaine de sécurité privilégié de l'élément sécurisé 10 ci-après référencé ISD-R (« Issuer Security Domain – Root »).

20 Le serveur SM-SR et le domaine de sécurité privilégié ISD-R partagent une ou plusieurs clefs sécurisées KSEC et sont chacun aptes à utiliser ces clefs pour mettre en œuvre des fonctions de cryptage/décryptage, et/ou des fonctions d'authentification et à communiquer via le réseau mobile selon un protocole de transport
25 sécurisé, par exemple selon le protocole SCP80 (Secure Channel Protocol) ou selon le protocole SCP81.

Le domaine de sécurité privilégié ISD-R est remarquable en ce qu'il a la capacité de créer un nouveau domaine de sécurité sur l'élément
30 sécurisé 10 et éventuellement la capacité de l'activer, sur réception de commandes (ENABLE, DISABLE ...) définies par la GSMA pour le eUICC ou de commandes (DELETE, INSTALL...) conformes à la norme Global Platform, ces commandes étant reçues du serveur SM-SR.

Comme de façon connue, la création de ce nouveau domaine de sécurité cible ISD-P comprend l'exécution d'un script de création de clefs
35 KMNO permettant une communication sécurisée entre l'opérateur MNO et le domaine de sécurité ISD-P.

On rappelle que conformément à la norme Global Platform, le domaine de sécurité privilégié ISD-R ne peut plus accéder aux services du domaine de sécurité cible ISD-P, une fois celui-ci activé, les domaines de sécurité ISD-R et ISD-P étant isolés. Selon une terminologie de cette
5 norme connue de l'homme du métier, on dit aussi que le domaine de sécurité cible ISD-P est extradé.

Nous allons maintenant expliquer comment l'invention permet à l'opérateur MNO de charger le profil P dans le domaine de sécurité cible ISD-P.

10 Au cours d'une étape G10, l'opérateur MNO envoie au serveur SM-SR un script SP permettant de créer le profil P. Ce script est crypté avec au moins une clef KMNO de l'opérateur MNO.

 Au cours d'une étape E10, le serveur SM-SR envoie des données DSP comportant le script SP au domaine de sécurité cible ISD-P en
15 utilisant le protocole de transport sécurisé, à savoir le protocole SCP80 ou SCP81 dans cet exemple. Ces données sont cryptées avec la clef KSEC.

 En pratique, ces données comportent une information indiquant qu'elles sont destinées au domaine de sécurité ISD-P cible. Cette information peut notamment être contenue dans un champ champ TAR
20 (Toolkit Application Reference) si le protocole SCP80 est utilisé, ou dans un champ AID (Application IDentifier) si le protocole SCP81 est utilisé.

 Le domaine de sécurité cible ISD-P n'offre pas de service permettant de communiquer selon ce protocole de transport sécurisé.

 Par conséquent, et conformément à l'invention, le domaine de
25 sécurité cible ISD-P transmet les données DSP au domaine de sécurité privilégié ISD-R au cours d'une étape E20 pour que celui-ci désencapsule le protocole de transport sécurisé. En pratique, pour effectuer ce transfert, le domaine de de sécurité ISD-P invoque un service du domaine de sécurité ISD-R.

30 Dans le mode de réalisation décrit ici, le domaine de sécurité ISD-P cible transmet les données DSP au domaine de de sécurité privilégié ISD-R en utilisant l'interface GlobalService de la norme Global Platform Card Specification 2.2.

 Le domaine de sécurité privilégié ISD-R désencapsule le protocole
35 de transport sécurisé au cours d'une étape E30, cette désencapsulation

consistant notamment à décrypter les données reçues et à les authentifier par un mécanisme de vérification de signature.

Le domaine de sécurité privilégié ISD-R envoie le script SP crypté avec la clef KMNO de l'opérateur MNO au domaine de sécurité cible ISD-P au cours d'une étape E40.

5 Au cours d'une étape E50, le domaine de sécurité cible ISD-P décrypte et authentifie le script SP reçu du domaine de sécurité ISD-R en utilisant les clefs KMNO partagées avec l'opérateur MNO, ces clefs KMNO ayant été créées au moment de la création du domaine de sécurité ISD-P
10 (étape F20). Si les opérations de décryptage et d'authentification se déroulent correctement, le domaine de sécurité cible ISD-P installe le profil P dans ce domaine de sécurité au cours de cette même étape E50.

 Au cours d'une étape E60, le domaine de sécurité cible ISD-P prépare une réponse RP destinée au serveur SM-SR pour l'informer du succès ou de l'échec de l'installation du profil P.
15

 Le domaine de sécurité cible ISD-P n'est pas en mesure de communiquer selon le protocole de transport sécurisé avec le serveur SM-SR.

 Par conséquent, dans un mode de réalisation particulier, le
20 domaine de sécurité cible IDS-P prépare une réponse RP qu'il crypte avec la clef de l'opérateur KMNO, puis demande au domaine de sécurité privilégié ISD-R de chiffrer cette réponse cryptée pour son transport sécurisé à destination du serveur SM-SR (étape E70).

 Dans le mode de réalisation décrit ici, le domaine de sécurité ISD-
25 P cible envoie la réponse RP cryptée au domaine de de sécurité privilégié ISD-R en utilisant l'interface GlobalService de la norme Global Platform Card Specification 2.2.

 Le domaine de sécurité privilégié ISD-R crypte la réponse RP au cours d'une étape E80 conformément au protocole de transport sécurisé en utilisant la clef KSEC et envoie la réponse cryptée selon ce protocole au
30 domaine de sécurité cible au cours d'une étape E90.

 Le domaine de sécurité cible ISD-P transmet la réponse cryptée au serveur SM-SR au cours d'une étape E100.

 Les étapes F10, F20, G10 et E10 à E100 sont exécutées dans cet
35 exemple dans l'ordre dans lequel elles ont été présentées.

La figure 2 représente un élément sécurisé 10 conforme à l'invention dans un mode particulier de réalisation de l'invention.

Cet élément sécurisé 10 est incorporé dans un téléphone mobile 20 comportant notamment un processeur 21, une mémoire vive 22, une
5 mémoire morte 23 et des moyens 24 de communication sur un réseau mobile. L'élément sécurisé 10 est par exemple constitué par un circuit intégré.

Dans le mode de réalisation décrit ici, les moyens 24 de communication sont adaptés à communiquer avec le serveur de domaine
10 de sécurité SM-SR selon le protocole CAT-TP ou selon le protocole de sécurité HTTP en fonction du protocole de transport sécurisé utilisé SCP 80 ou SCP81.

Dans le mode de réalisation décrit ici, cet élément sécurisé 10 est un composant eUICC tel que défini par la norme ETSI 102 221. Il
15 comporte notamment un processeur 11, une mémoire vive 12, une mémoire morte 13 et des moyens 24 de communication avec le processeur 21 du téléphone mobile.

Le processeur 11 est apte à exécuter les étapes décrites précédemment en référence à la figure 1.

20 Dans le mode de réalisation décrit ici, le téléphone mobile communique avec l'élément de sécurité 10 au moyen de commandes APDU.

L'élément sécurisé 10 comporte un domaine de sécurité cible ISD-P dans lequel le profil P doit être installé et un domaine de sécurité
25 privilégié ISD-R apte à communiquer avec un serveur de domaine de sécurité SM-SR selon un protocole de transport sécurisé non décryptable par le domaine de sécurité cible ISD-P.

En pratique, le domaine de sécurité privilégié ISD-R connaît la ou les clefs de cryptage KSEC et offre des services de communication, de
30 cryptage/décryptage ou/et d'authentification conformes à ce protocole sécurisé, cette clef et ces services n'étant pas connue ou offerts par le domaine de sécurité cible ISD-P.

Le domaine de sécurité cible ISD-P comporte une ou des clefs KMNO partagées avec l'opérateur MNO et des méthodes de
35 cryptage/décryptage et/ou d'authentification utilisant cette ou ces clefs. Ces méthodes sont en particulier adaptées pour décrypter et/ou

authentifier le script d'installation du profil P reçu de domaine de sécurité privilégié ISD-R.

5 Le domaine de sécurité cible ISD-P comporte aussi une méthode apte à exécuter ce pour installer le profil P dans ledit domaine de sécurité cible.

10 Lorsque le domaine de sécurité cible ISD-P reçoit des données conformément au protocole de transport sécurisé, il invoque automatiquement une méthode du domaine de sécurité privilégié ISD-R pour lui transférer ces données. C'est ainsi qu'il transfère au domaine de sécurité privilégié ISD-R les données DSP comportant le script crypté d'installation du profil P.

Le domaine de sécurité privilégié ISD-R comporte des méthodes permettant de décrypter le protocole de transport avec la clef KSEC, cette méthode étant invoquée pour obtenir le script crypté.

15 Le domaine de sécurité privilégié ISD-R est apte à invoquer une méthode du domaine de sécurité cible ISD-P pour lui communiquer des données. Il utilise notamment cette méthode pour envoyer le script crypté au domaine de sécurité cible.

REVENDEICATIONS

1. Procédé de création d'un profil (P) dans un domaine de sécurité cible (ISD-P) d'un élément sécurisé (10) comportant un domaine de sécurité privilégié (ISD-R) apte à communiquer avec un serveur de domaine de sécurité (SM-SR) selon un protocole de transport sécurisé non décriptable par ledit domaine de sécurité cible (ISD-P) ce procédé comportant :
- une étape de réception (E10) par ledit domaine de sécurité cible (ISD-P), conformément audit protocole de transport sécurisé, de données (DSP) comportant un script d'installation dudit profil (P) crypté avec au moins une clef (KMNO) connue dudit domaine de sécurité cible (IDS-P) ;
 - une étape (E20) au cours de laquelle ledit domaine de sécurité cible (IDS-P) transfère lesdites données (DSP) audit domaine de sécurité privilégié (IDS-R) selon ledit protocole de transport sécurisé ;
 - une étape (E30) de décryptage dudit protocole de transport sécurisé par ledit domaine de sécurité privilégié (IDS-R) pour obtenir ledit script crypté ;
 - une étape (E40) au cours de laquelle ledit domaine de sécurité privilégié (IDS-R) envoie ledit script crypté audit domaine de sécurité cible (IDS-P) ;
 - une étape (E50) de décryptage dudit script crypté par ledit domaine de sécurité cible (ISD-P) en utilisant ladite au moins une clef (KMNO) ; et
 - une étape (E50) d'exécution dudit script par ledit domaine de sécurité cible (IDS-P) pour installer ledit profil (P) dans ledit domaine de sécurité cible.

2. Procédé de création de profil (P) selon la revendication 1, caractérisé en ce que ledit domaine de sécurité cible (ISD-P) transfère lesdites données (DSP) audit domaine de sécurité privilégié (IDS-R) en utilisant une interface GlobalService de la norme Global Platform.

3. Procédé de création de profil (P) selon la revendication 1 ou 2, caractérisé en ce que ledit protocole de transport sécurisé est le protocole SCP80 ou SCP81.

5 4. Procédé de création de profil (P) selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit domaine de sécurité cible (ISD-P) envoie (E70) une réponse (RP) audit domaine de sécurité privilégié (ISD-R), cette réponse (RP) étant cryptée (E80) par ledit domaine de sécurité privilégié conformément audit protocole de transport
10 sécurisé, la réponse cryptée étant renvoyée (E90) selon le protocole de transport sécurisé audit domaine de sécurité cible (ISD-P) pour transfert audit serveur (SM-SR).

15 5. Procédé de création de profil (P) selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comporte une étape (F20) de création et d'activation dudit domaine de sécurité cible (ISD-P) par ledit domaine de sécurité privilégié (ISD-R).

20 6. Procédé de création de profil (P) selon la revendication 5, caractérisé en ce que ladite étape (F20) de création et d'activation comprend l'exécution d'un script par ledit domaine de sécurité cible (ISD-P) pour générer ladite au moins une clef (KMNO).

7. Élément sécurisé (10) comportant :

- 25 - un domaine de sécurité cible (ISD-P) ; et un
- un domaine de sécurité privilégié (ISD-R) apte à communiquer avec un serveur de domaine de sécurité (SM-SR) selon un protocole de transport sécurisé non décryptable par ledit domaine de sécurité cible (ISD-P) ;
caractérisé en ce que :
30 - ledit domaine de sécurité cible (ISD-P) comporte :

- des moyens de réception, conformément audit protocole de transport sécurisé, de données (DSP) comportant un script d'installation d'un profil (P) crypté avec au moins une clef (KMNO) connue dudit domaine de sécurité cible (IDS-P) ;
- 5 - des moyens pour transférer lesdites données (DSP) audit domaine de sécurité privilégié (IDS-R) selon ledit protocole de transport sécurisé ;
- ledit domaine de sécurité privilégié (IDS-R) comporte :
 - des moyens de décryptage dudit protocole de transport sécurisé
 - 10 pour obtenir ledit script crypté ;
 - des moyens pour envoyer ledit script crypté audit domaine de sécurité cible (IDS-P) ;
- ledit domaine de sécurité cible (ISD-P) comportant :
 - des moyens de décryptage dudit script crypté en utilisant ladite au
 - 15 moins une clef (KMNO) ; et
 - des moyens d'exécution dudit script pour installer ledit profil (P) dans ledit domaine de sécurité cible.

8. Élément sécurisé (10) selon la revendication 7, caractérisé en

20 ce que lesdits domaines de sécurité (ISD-P, ISD-R) sont conformes à la norme GlobalPlatform Card Specification 2.2.1.

9. Élément sécurisé (10) selon la revendication 7 ou 8 caractérisé en ce qu'il est constitué par un composant eUICC tel que défini

25 par la norme ETSI 102 221.

10. Élément sécurisé (10) selon l'une quelconque des revendications 7 à 9 caractérisé en ce qu'il est constitué par un circuit intégré.

11. Terminal (20) comportant un élément sécurisé (10) selon l'une quelconque des revendications 7 à 10.

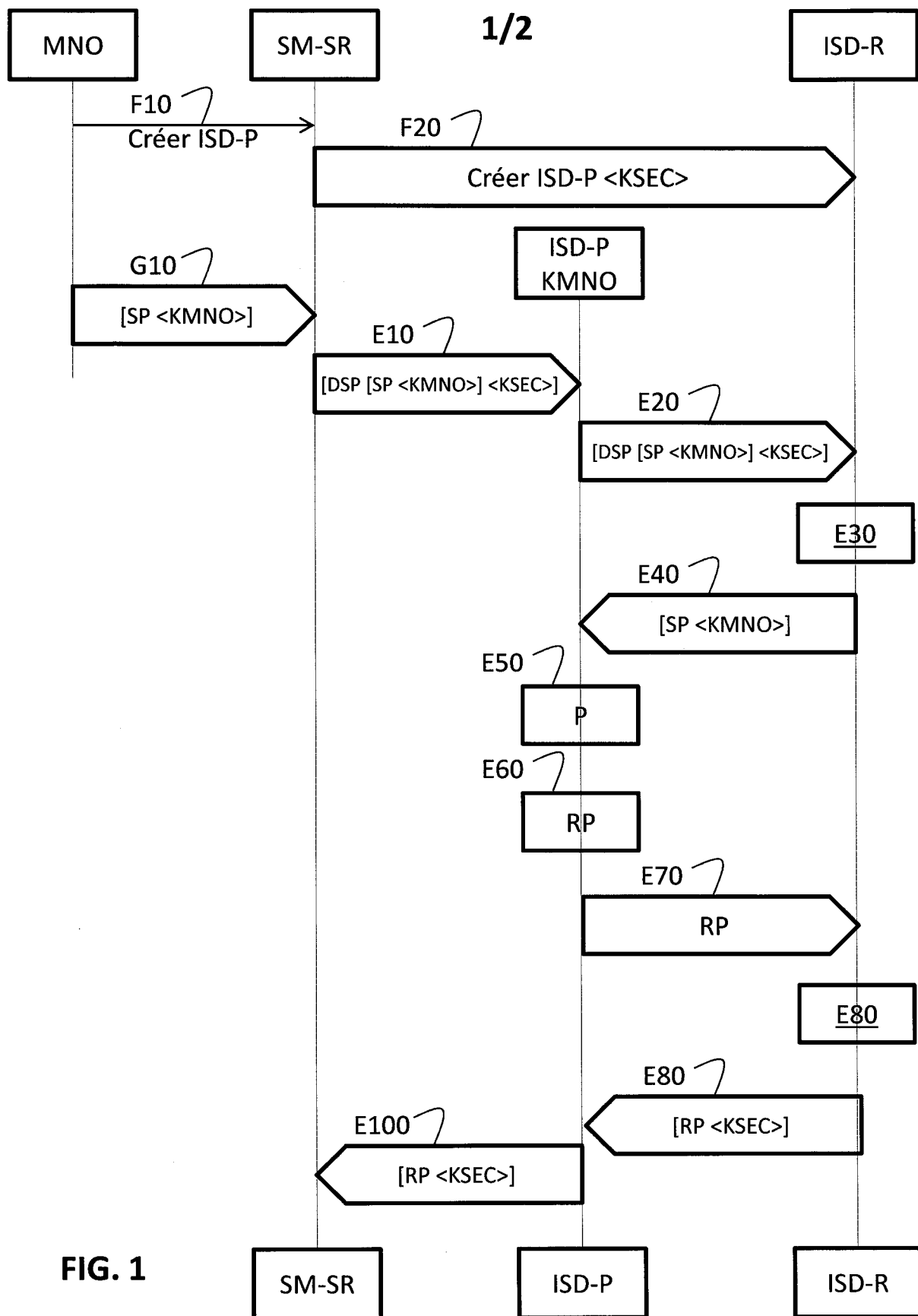


FIG. 1

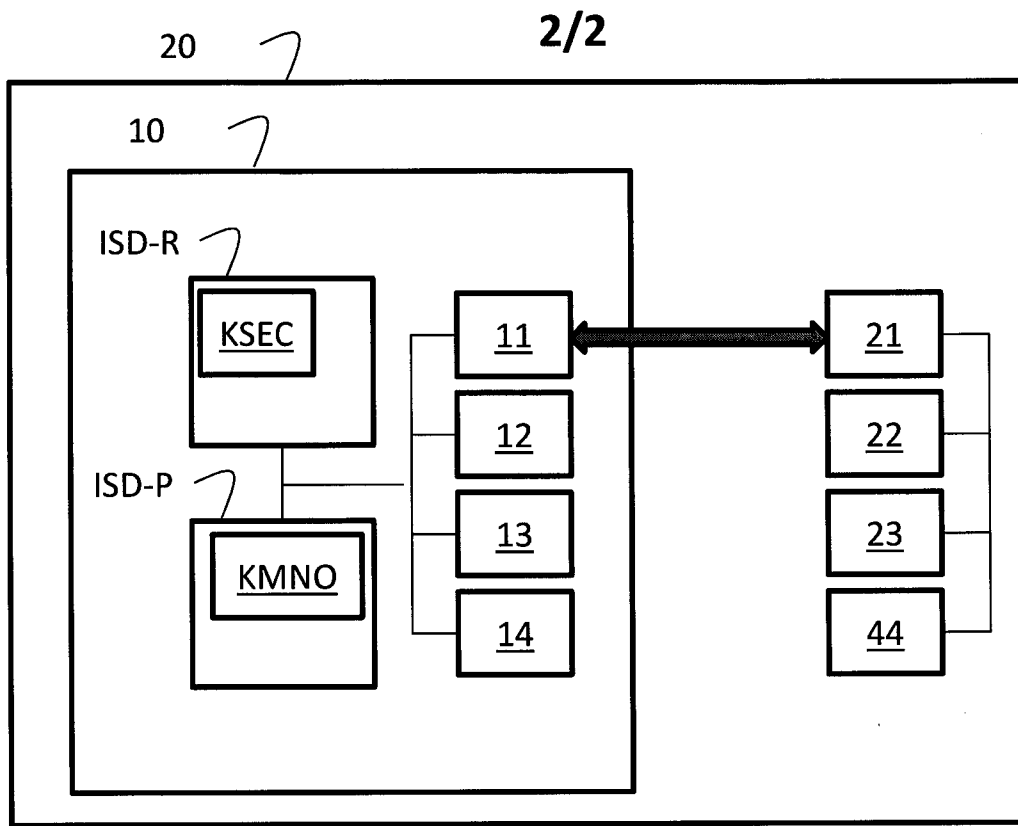


FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2014/050306

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

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

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2005/076204 A1 (HISMARTECH CO LTD [KR]; PARK JIN-SUNG [KR]; YU KI-SOO [KR]; AN SONG-HA) 18 August 2005 (2005-08-18) page 5, line 8 - line 23; figure 1 page 7, line 14 - page 9, line 4; figure 3 page 9, line 15 - page 10, line 21; figure 4 -----	1-11



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

12 May 2014

Date of mailing of the international search report

27/05/2014

Name and mailing address of the ISA/

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

Authorized officer

Raposo Pires, João

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2014/050306

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2005076204	A1	18-08-2005	NONE

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2014/050306

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

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

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

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

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

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 2005/076204 A1 (HISMARTECH CO LTD [KR]; PARK JIN-SUNG [KR]; YU KI-SOO [KR]; AN SONG-HA) 18 août 2005 (2005-08-18) page 5, ligne 8 - ligne 23; figure 1 page 7, ligne 14 - page 9, ligne 4; figure 3 page 9, ligne 15 - page 10, ligne 21; figure 4 -----	1-11



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



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

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

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

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

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

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

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

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

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

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

Date à laquelle la recherche internationale a été effectivement achevée

12 mai 2014

Date d'expédition du présent rapport de recherche internationale

27/05/2014

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

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

Fonctionnaire autorisé

Raposo Pires, João

Renseignements relatifs aux membres de familles de brevets

PCT/FR2014/050306

Document brevet cité
au rapport de recherche

Date de publication

Membre(s) de la
famille de brevet(s)

Date de
publication

W0 2005076204	A1	18-08-2005	AUCUN
---------------	----	------------	-------