(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
23 juillet 2020 (23.07.2020)

WIPO | PCT

(10) Numéro de publication internationale
WO 2020/148492 A1

(51) Classification internationale des brevets :
G06F 21/51 (2013.01) *G06F 21/57* (2013.01)

(21) Numéro de la demande internationale :
PCT/FR2020/050017

(22) Date de dépôt international :
07 janvier 2020 (07.01.2020)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1900300 14 janvier 2019 (14.01.2019) FR

(71) Déposant : **ORANGE** [FR/FR] ; 78 rue Olivier de Serres, 75015 PARIS (FR).

(72) Inventeur : **BANDIN, Stéphane** ; ORANGE GARDENS - TGI/OLR/IPL/PATENTS -, 44 avenue de la République -, CS 50010, 92326 CHÂTILLON CEDEX (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM,

(54) Title: AUTHORIZATION FOR THE LOADING OF AN APPLICATION ONTO A SECURITY ELEMENT

(54) Titre : AUTORISATION DU CHARGEMENT D'UNE APPLICATION DANS UN ÉLÉMENT DE SÉCURITÉ

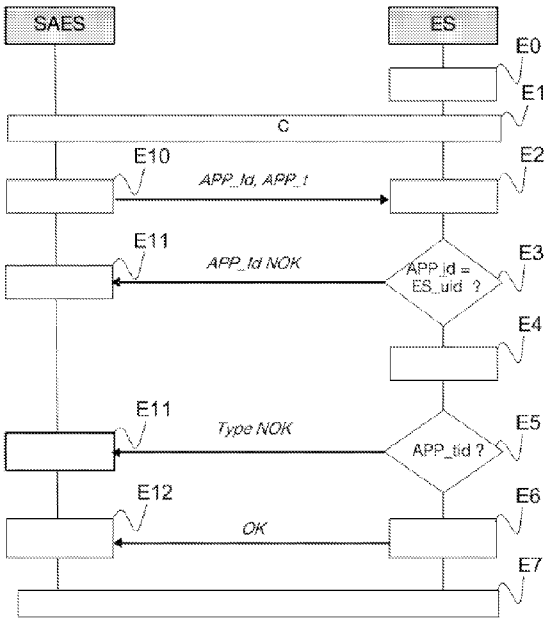


Figure 2

(57) Abstract: The invention relates to a method and device for authorizing the loading of an application (APP) onto a security element (ES) that can communicate with a loading server (SAES) of an application provider. The method is implemented by the security element and comprises the following steps: - obtaining (E0) at least one type of authorized application (APP_tid); - obtaining (E2) the type of application to be loaded (APP_t); - comparing the type of application to be loaded (APP_t) and the type of authorized application (APP_tid); - depending on the results of the comparision, authorizing the loading (E6) of the application.

(57) Abrégé : L'invention concerne un procédé et un dispositif d'autorisation du chargement d'une application (APP) dans un élément de sécurité (ES) apte à communiquer avec un serveur (SAES) de chargement d'un fournisseur d'applications. Le procédé est mis en œuvre

WO 2020/148492 A1

[Suite sur la page suivante]

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

Publiée:

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

par l'élément de sécurité et comprend les étapes suivantes: - obtention (E0) d'au moins un type d'application autorisée (APP_tid); - obtention (E2) du type de l'application à charger (APP_t); - comparaison du type de l'application à charger (APP_t) et du type d'application autorisée (APP_tid); - en fonction des résultats de la comparaison, autorisation du chargement (E6) de l'application.

DESCRIPTION

Titre : Autorisation du chargement d'une application dans un élément de sécurité.

1. Domaine de l'invention

L'invention concerne un élément de sécurité. Elle s'applique en particulier à un élément de sécurité apte à télécharger des applications sur un réseau de communications.

2. Art Antérieur

Le transfert de données entre une machine distante et un élément de sécurité, comme par exemple une carte à puce, est le plus souvent sécurisé par des mécanismes cryptographiques. Ces mécanismes, qu'ils soient symétriques ou asymétriques, permettent de garantir la confidentialité et l'intégrité des données échangées, créant ainsi un canal de communication sécurisé entre la machine distante et l'élément de sécurité.

L'établissement d'un canal de communication sécurisé, qui permet en outre d'identifier l'émetteur des données, est une preuve de confiance jugée suffisante entre les deux parties ; par conséquent, le destinataire ne contrôle pas la nature des données avant d'en accepter la réception.

Il en résulte que l'émetteur est en mesure d'utiliser le canal de communication sécurisé pour envoyer des données, notamment des applications, qui peuvent être indues.

3. Exposé de l'invention

L'invention vient améliorer l'état de la technique.

Elle propose à cet effet un procédé d'autorisation du chargement d'une application dans un élément de sécurité apte à communiquer avec un serveur de chargement d'un fournisseur d'applications, le procédé étant mis en œuvre par l'élément de sécurité et comprenant les étapes suivantes:

- obtention d'au moins un type d'application autorisée ;
- obtention du type de l'application à charger ;
- comparaison du type de l'application à charger et du type d'application autorisée ;
- en fonction des résultats de la comparaison, autorisation du chargement de l'application.

Avantageusement, selon l'invention, une application est chargée dans l'élément de sécurité seulement si une information de vérification a permis de la valider. L'information de vérification étant fonction du type de l'application à charger, un fournisseur, même fiable, ne peut pas charger une application non souhaitée dans l'élément de sécurité.

Par « application » on entend ici un ensemble de données (actives, comme des codes informatiques ou passives, comme des données de toute nature, y compris des clés cryptographiques) destinées à être utilisées ensuite sur l'élément de sécurité. L'application est associée à un « type », qui correspond par exemple à une catégorie d'applications (télécommunications, identité, droits numériques, objets connectés, paiement, etc.). L'application peut prendre en particulier la forme d'un programme informatique et de données associées ; le programme informatique peut comprendre des éléments de système d'exploitation.

Par « élément de sécurité » on entend tout élément matériel et/ou logiciel assurant la sécurité des données en conformité avec les règles et les exigences de sécurité fixées par une autorité de confiance, par exemple une carte à puce, une carte SIM (pour *Subscriber Identity Module*) ou l'une quelconque de leurs évolutions : eSIM (embedded SIM), UICC (pour *Universal Integrated Circuit Card*), eUICC (pour *embedded UICC*) ou une architecture de type SSP (pour *Smart Secure Platform*) en cours de définition à l'ETSI. On pourra se référer par exemple au document « SIM evolution » de M. Klaus Vedder (20TH SIGOS CONFERENCE FOR TELCO & DIGITAL EXPERIENCE - 9 - 11 July 2018 | Nuremberg) pour une présentation de cette architecture. Selon un autre exemple, l'architecture de l'élément de sécurité peut être de type TEE (pour *Trusted Execution Environnement*), c'est-à-dire une zone (mémoire) sécurisée et isolée d'autres environnements d'exécutions, située dans un dispositif (de type téléphone portable), garantissant que des données sensibles sont stockées, traitées et protégées dans un environnement de confiance.

Par « fournisseur d'applications » on entend une entité qui met à disposition une ou plusieurs applications pour l'élément de sécurité, comme par exemple un opérateur de réseau mobile (aussi appelé MNO), un représentant d'un état fournissant des applications d'identité, une banque fournissant des applications de paiement, etc. Le fournisseur d'application est identifié de manière unique par un

identifiant comme par exemple une URI (pour *Universal Resource Identifier*), une chaîne de caractères, une suite de chiffres, etc.

Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est en outre caractérisé en ce que l'élément de sécurité est accessible à au moins un utilisateur identifié par un identifiant d'utilisateur, le type d'application autorisée est relatif audit utilisateur et le procédé comporte une étape d'obtention dudit identifiant d'utilisateur.

Ce mode de mise en œuvre de l'invention permet de contrôler le chargement des applications pour un utilisateur donné, lorsque l'élément de sécurité est associé à un ou plusieurs utilisateurs qui disposent de droits sur cet élément, notamment le droit d'utiliser les ressources de cet élément de sécurité pour une application ou un service donné. Ils sont dotés d'un identifiant d'utilisateur, comme par exemple un nom, un numéro, une chaîne de caractères, une URI, etc. Le type d'application autorisé étant relatif à un utilisateur particulier, on s'assure ainsi que chaque utilisateur peut bénéficier de manière sécurisée du chargement de ses propres applications.

Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est en outre caractérisé en ce qu'il comporte une étape d'obtention d'un identifiant du fournisseur de l'application à charger et en ce que l'information de vérification est calculée en fonction dudit identifiant du fournisseur.

Ce mode de mise en œuvre de l'invention permet notamment de renforcer la validation du chargement par l'introduction d'un identifiant du fournisseur dans le calcul de la donnée de validation, qui permet d'écarter des fournisseurs non autorisés. Avantageusement, si l'information de validation est établie en combinant identifiant du fournisseur et type d'application autorisée, on pourra refuser de charger une application dont le type n'est pas autorisé pour un fournisseur donné, et éventuellement pour un utilisateur donné.

Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est caractérisé en ce qu'il comporte en outre :

- une étape de comparaison de l'identifiant du fournisseur de l'application à charger et de l'identifiant de l'utilisateur ;
- en fonction des résultats de la comparaison, une étape de refus du chargement de l'application.

Ce mode de mise en œuvre de l'invention permet de renforcer la sécurité de la vérification en comparant l'identifiant du fournisseur avec celui de l'utilisateur de l'élément de sécurité. Ainsi, par exemple, si les deux entités sont de type « banque », le chargement pourra-t-il être accepté, mais si l'une des entités n'est pas une banque, on aboutira au refus de chargement de l'application.

Selon un autre mode particulier de réalisation de l'invention, le procédé d'autorisation est en outre caractérisé en ce qu'un identifiant dudit utilisateur et au moins un type d'application autorisée pour ledit utilisateur sont enregistrés sous forme d'un certificat dans une mémoire de l'élément de sécurité.

Avantageusement selon ce mode, un certificat électronique peut être utilisé pour transmettre les données à l'élément de sécurité. Un tel certificat, utilisé pour identifier et authentifier une personne, mais aussi pour chiffrer des échanges, peut correspondre à une norme bien connue de l'homme du métier (comme par exemple la norme X509).

L'invention concerne également un dispositif d'autorisation du chargement d'une application dans un élément de sécurité apte à communiquer avec un serveur de chargement d'un fournisseur d'applications, le dispositif comportant:

- un module d'obtention d'au moins un type d'application autorisée ;
- un module d'obtention du type de l'application à charger ;
- un module de comparaison du type de l'application à charger et du type d'application autorisée ;
- un module d'autorisation du chargement de l'application de l'application, en fonction des résultats de la comparaison.

Le terme module peut correspondre aussi bien à un composant logiciel qu'à un composant matériel ou un ensemble de composants matériels et logiciels, un composant logiciel correspondant lui-même à un ou plusieurs programmes ou sous-programmes d'ordinateur ou de manière plus générale à tout élément d'un programme apte à mettre en œuvre une fonction ou un ensemble de fonctions telles que décrites pour les modules concernés. De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions pour le module concerné (circuit intégré, carte à puce, carte à mémoire, etc.).

L'invention concerne également une carte électronique comportant un tel dispositif d'autorisation.

L'invention concerne également une zone mémoire sécurisée comportant un tel dispositif d'autorisation.

L'invention concerne également un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé ci-dessus selon l'un quelconque des modes particuliers de réalisation décrits précédemment, lorsque ledit programme est exécuté par un processeur. Le procédé peut être mis en œuvre de diverses manières, notamment sous forme câblée ou sous forme logicielle. 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.

L'invention vise aussi un support d'enregistrement ou support d'informations lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus. Les supports d'enregistrement mentionnés ci-avant peuvent être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple un disque dur. D'autre part, les supports d'enregistrement peuvent correspondre à 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. Les programmes selon l'invention peuvent être en particulier téléchargés sur un réseau de type Internet.

Alternativement, les supports d'enregistrement peuvent correspondre à un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

Ce dispositif d'autorisation et ce programme d'ordinateur présentent des caractéristiques et avantages analogues à ceux décrits précédemment en relation avec le procédé d'autorisation. Les caractéristiques optionnelles évoquées pour le procédé peuvent s'appliquer au dispositif et au programme.

4. Liste des figures

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante de modes de réalisation particuliers, donnés à titre de simples exemples illustratifs et non limitatifs, et des dessins annexés, parmi lesquels :

[Fig 1] La figure 1 illustre un exemple d'environnement de mise en œuvre de l'invention selon un mode particulier de réalisation de l'invention,

[Fig 2] La figure 2 illustre des étapes du procédé d'autorisation de chargement d'une application selon un mode particulier de réalisation de l'invention,

[Fig 3] La figure 3 illustre un dispositif configuré pour mettre en œuvre le procédé d'autorisation de chargement selon un mode particulier de réalisation de l'invention.

[Fig 4] La figure 4 illustre un dispositif configuré pour mettre en œuvre le procédé d'autorisation de chargement selon un autre mode particulier de réalisation de l'invention.

5. Description d'un mode de réalisation de l'invention

5.1 Principe général de l'invention

Le procédé décrit ici propose une méthode de vérification de la nature des données constitutives d'une application au sein d'un élément de sécurité (ES) avant d'en accepter la réception. Chaque utilisateur de l'élément de sécurité doit préalablement être enregistré via un identifiant, ainsi que la liste des types d'applications pour lesquelles cet utilisateur autorise le téléchargement, dans une mémoire de l'ES. Avant le téléchargement, le type de l'application est vérifié par l'élément de sécurité. Avantageusement, un émetteur/fournisseur n'est donc plus en mesure d'utiliser le canal de communication, même sécurisé, pour envoyer des données indues.

5.2 Modes particuliers de réalisation de l'invention.

La **figure 1** illustre un exemple d'environnement de mise en œuvre de l'invention selon un mode particulier de réalisation, dans le contexte d'un téléchargement d'une application (APP) depuis une machine distante, ou serveur d'applications pour élément de sécurité (SAES), vers un élément de sécurité (ES).

Selon ce mode de réalisation, l'élément de sécurité ES possède au moins un utilisateur doté d'un identifiant noté ES_uid. Cet utilisateur définit le(s) type(s) d'applications qu'il autorise à être téléchargé(s) sur l'ES. Il peut y avoir plusieurs

utilisateurs d'un même ES, comme représenté à la figure 1, où l'ES possède deux utilisateurs A et B (ES_uid_A et ES_uid_B). L'élément de sécurité peut être intégré par exemple dans un dispositif comme un smartphone. Il peut être matériel, ou logiciel, ou une combinaison des deux.

Le serveur d'applications communique avec l'Élément de sécurité (ES) pour télécharger une application (APP) à travers le canal de communication C.

Selon un mode particulier de réalisation de l'invention, le canal de communication C est sécurisé, par exemple par l'utilisation de clés cryptographiques.

L'application à télécharger (APP) est associée à un fournisseur et dispose d'un type ; on note APP_id l'identifiant du fournisseur d'applications et APP_t le type de l'application. APP_t peut être utilisé par un ou plusieurs fournisseurs.

On note APP_tid l'identifiant représentant le type d'applications APP_t proposé par le fournisseur APP_id ; par exemple, si APP est l'application de fidélité du marchand xyz, APP_id *(id=xyz)* est l'identifiant de ce marchand, APP_t correspond au type « applications de fidélité » et APP_tid_A est le type « applications de fidélité » du marchand xyz pour le client A

Selon un mode particulier de réalisation de l'invention, la valeur APP_tid est composée en combinant la valeur d'APP_id et d'APP_t.

Selon un mode particulier de réalisation de l'invention : l'application APP est une application d'identité électronique ; un type d'application APP_t est un type d'application d'identité (passeport, permis de conduire…) ; un fournisseur est un état ou un représentant d'un état (ANSSI en France ou le BSI en Allemagne) représenté dans l'ES par un ES_uid ; plusieurs états peuvent s'entendre pour utiliser les mêmes valeurs d'APP_t, ne dépendant pas d'APP_id du fournisseur (un citoyen franco-allemand peut avoir un passeport de chacun des deux pays). La mise en œuvre de l'invention dans ce contexte permet de garantir que seul l'état français est en mesure de télécharger les applications d'identité françaises et n'est pas en mesure de télécharger les applications d'identité d'un autre état.

La **figure 2** illustre des étapes du procédé de chargement d'une application selon un mode particulier de réalisation de l'invention

L'étape E0 correspond à une étape d'initialisation. Elle peut être réalisée à n'importe quel moment (initialisation de la carte, ou personnalisation ultérieure par

l'utilisateur, etc.). Pour chaque utilisateur de l'ES, les informations qui suivent sont enregistrées dans la mémoire de l'ES :

- Un identifiant unique ES_uid de l'utilisateur. Selon un mode particulier de réalisation, la valeur d'ES_uid est égale à la valeur d'APP_id ;
- La liste des APP_tid, c'est -à-dire, la liste des types d'applications pour lesquelles le téléchargement est autorisé par l'utilisateur.

Selon un mode de réalisation particulier, ces informations sont mémorisées dans un certificat électronique (Cert), comportant par exemple les informations suivantes :

- L'identifiant de l'émetteur du certificat (par exemple : urn:xyz.com). Cet identifiant joue alors le rôle de ES_uid.
- La liste des APP_tid, c'est-à-dire la liste des types d'applications pour lesquelles le téléchargement est autorisé par l'utilisateur de l'ES pour un fournisseur donné.

Lors d'une étape **E1**, le serveur et l'élément de sécurité, SAES et ES établissement un canal de communication C.

Selon un mode particulier de réalisation de l'invention, ce canal de communication est sécurisé par l'utilisation de certificats électroniques à clé publique, comme présenté auparavant.

Lors d'une étape **E10**, le serveur SAES envoie sur le canal de communication C l'identifiant du fournisseur (APP_id) et le type d'application (APP_t) d'une application APP à télécharger, reçues lors d'une étape E2.

Lors d'une étape **E3** facultative, l'élément de sécurité ES vérifie que le fournisseur de cette application est bien autorisé. Selon un mode de réalisation, il compare la valeur d'APP_id reçue aux valeurs d'ES_uid enregistrées :

- Si la valeur d'APP_id ne correspond à aucune valeur d'ES_uid enregistrée, ES répond à SAES que APP_id n'est lié à aucun utilisateur enregistré pour cet ES ; ES n'accepte pas le téléchargement d'APP. Ceci permet d'éviter qu'un fournisseur d'application utilise indûment l'élément de sécurité. Par exemple, si l'ES_uid vaut lambda (e.g. telco pour un opérateur de télécommunications) mais l'App_id est associé à une banque, cette étape échoue car l'utilisateur lambda (le telco) n'est pas en mesure de charger une application bancaire.

- Si la valeur d'APP_id correspond à une valeur d'ES_uid enregistrée, le traitement se poursuit.

Selon un mode particulier de réalisation de l'invention présenté auparavant, selon lequel le canal de communication est sécurisé par l'utilisation de certificats électroniques à clé publique, l'identifiant de l'émetteur du certificat (ES_uid) est extrait du certificat.

Puis lors d'une étape **E4**, l'élément de sécurité ES obtient une information de validation, notée APP'_tid à partir du type d'application APP_t, ou selon un mode de réalisation préféré, en combinant les informations envoyées par le serveur SAES, APP_id et APP_t.

Selon un mode particulier de réalisation de l'invention, APP_tid est calculé selon le procédé décrit dans la spécification IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace" ; un tel identifiant est aussi connu sous la dénomination « UUID version 5 », où NID (Namespace Identifier) est égal à APP_id et NSS (Namespace Specific String) est égal à APP_t.

Selon un autre mode de réalisation particulier de l'invention, ce traitement peut être confié à une entité externe par l'élément de sécurité.

Lors d'une étape **E5**, l'élément de sécurité ES compare la valeur d'APP'_tid calculée ou obtenue à l'étape précédente aux valeurs d'APP_tid enregistrées pour l'utilisateur ES_uid ; si la valeur d'APP'_tid ne correspond à aucune valeur d'APP_tid enregistrées pour l'utilisateur ES_uid, ES répond au serveur SAES que le type d'application n'est pas autorisé par l'utilisateur ; ES n'accepte pas le téléchargement de l'application APP.

Lors d'une étape **E6,** si la valeur d'APP'_tid correspond à une valeur d'APP_tid enregistrée pour l'utilisateur ES_uid, ES indique à SAES que le téléchargement d'APP est autorisé.

Selon un mode particulier de réalisation de l'invention présenté auparavant, selon lequel le canal de communication est sécurisé par l'utilisation de certificats électroniques à clé publique, cette étape consiste à comparer la valeur d'APP'_tid calculée à l'étape E4 aux valeurs d'APP_tid extraites du certificat utilisé pour l'établissement du canal de communication, c'est-à-dire la liste des types d'applications pour lesquelles le téléchargement est autorisé par l'utilisateur de l'ES.

Lors d'une étape **E11**, le serveur SAES télécharge l'application APP sur l'élément de sécurité ES qui la reçoit au cours d'une étape E7.

La **figure 3** illustre un dispositif DISP configuré pour mettre en œuvre le procédé de chargement selon un mode particulier de réalisation de l'invention.

Le dispositif DISP a l'architecture classique d'un élément de sécurité, et comprend notamment une mémoire MEM, une unité de traitement UT, équipée par exemple d'un processeur PROC, et pilotée par le programme d'ordinateur PG stocké en mémoire MEM. Le programme d'ordinateur PG comprend des instructions pour mettre en œuvre les étapes du procédé de chargement tel que décrit précédemment, lorsque le programme est exécuté par le processeur PROC.

À l'initialisation, les instructions de code du programme d'ordinateur PG sont par exemple chargées dans la mémoire avant d'être exécutées par le processeur PROC. Le processeur PROC de l'unité de traitement UT met notamment en œuvre les étapes du procédé d'autorisation du chargement selon l'un quelconque des modes particuliers de réalisation décrits en relation avec la figure 2, selon les instructions du programme d'ordinateur PG.

Le dispositif DISP comprend un module de communication COM configuré pour établir des communications avec un réseau, par exemple IP, pour le téléchargement de l'application APP. L'application APP est chargée dans une partie de la mémoire M.

Selon un mode particulier de réalisation, un tel dispositif est une carte SIM.

Selon un mode particulier de réalisation, un tel dispositif est un TEE (pour Trusted Execution Environnement) tel qu'évoqué plus haut.

Selon un autre mode particuliers de réalisation, représenté à la **figure 4**, un tel dispositif est une plateforme sécurisée de type iSSP (*pour integrated Smart Secure Platform)* telle que définie notamment dans la norme en cours d'élaboration de l'organisme ETSI, de référence TS 103 666-2, intitulée : *« Smart Secure Platform (SSP); Integrated SSP (iSSP) characteristics »*. Cette évolution des éléments sécurisés répond à de nouvelles exigences fonctionnelles et sécuritaires de l'élément de sécurité (SE) permettant, entre autre, la gestion multi-applicative, l'optimisation des architectures logicielles et hardwares, la réduction des coûts d'intégration et des capacités de stockage sécurisé accrues, etc.

L'architecture hardware et logicielle d'une iSSP, tel que représenté à la figure 4, est découpée en trois parties : une plateforme primaire (*Primary Platform* - PP) composée du hardware lui-même (processeurs, mémoires, etc.) ainsi que d'un système d'exploitation bas niveau (LLOS) et de services de base (SB) , par exemple de communication ; des plateformes secondaires (*Secondary Platform Bundles* - SPB) composés d'un système d'exploitation de haut niveau (HLOS) et d'une famille d'applications notées A1, A2, etc. (par exemple : relatives à l'USIM, l'identité, etc. de l'utilisateur) ; d'un module de chargement (*Secondary Platform Bundle Loader* – SPBL), SPB particulier permettant de gérer les autres SPB (chargement, activation…). Dans ce contexte, l'invention s'applique au mécanisme de téléchargement d'applications de type « Secondary Platform Bundle » (SPB) : le procédé d'autorisation du chargement d'une application, tel que décrit plus haut, est mis en œuvre par les éléments matériels et logiciels de l'iSSP de telle manière qu'une famille ou un ensemble d'applications (SPB) peut être chargé dans la mémoire de l'iSSP par le chargeur (SPBL) après vérification de son type, et éventuellement de son fournisseur, pour un utilisateur donné.

Selon un mode de réalisation, l'iSSP contient un certificat d'une autorité de certification (par exemple la GSMA, une association internationale d'opérateurs de téléphonie mobile) qui contient les types de famille d'applications (SPB) autorisées à être téléchargées ; par exemple les SPB Telecom, SPB Paiement, SPB Identité, etc. On notera que plusieurs autorités (GSMA, banque, état-nation, etc.), plusieurs utilisateurs, et plusieurs familles d'applications peuvent coexister dans l'iSSP.

Il va de soi que le mode de réalisation qui a été décrit ci-dessus a été donné à titre purement indicatif et nullement limitatif, et que de nombreuses modifications peuvent être facilement apportées par l'homme de l'art sans pour autant sortir du cadre de l'invention.

REVENDICATIONS

1. Procédé d'autorisation du chargement d'une application (APP) dans un élément de sécurité (ES) apte à communiquer avec un serveur (SAES) de chargement d'un fournisseur d'applications, le procédé étant mis en œuvre par l'élément de sécurité et comprenant les étapes suivantes:
   - obtention (E0) d'au moins un type d'application autorisée (APP_tid) ;
   - obtention (E2) du type de l'application à charger (APP_t) ;
   - comparaison du type de l'application à charger (APP_t) et du type d'application autorisée (APP_tid) ;
   - en fonction des résultats de la comparaison, autorisation du chargement (E6) de l'application.
2. Procédé d'autorisation selon la revendication 1, pour lequel l'élément de sécurité est accessible à au moins un utilisateur identifié par un identifiant d'utilisateur (ES_uid), le type d'application autorisée (APP_tid) est relatif audit utilisateur, et le procédé comporte une étape obtention (E0) dudit identifiant d'utilisateur.
3. Procédé d'autorisation selon la revendication 1 ou 2, caractérisé en ce qu'il comporte une étape d'obtention (E2) d'un identifiant du fournisseur (APP_id) de l'application à charger et en ce que l'information de vérification est obtenue en fonction dudit identifiant du fournisseur (APP_id).
4. Procédé d'autorisation selon la revendication 3, caractérisé en ce qu'il comporte en outre :
   - une étape de comparaison (E3) de l'identifiant du fournisseur (APP_id) de l'application à charger et de l'identifiant de l'utilisateur (ES_uid) ;
   - en fonction des résultats de la comparaison, une étape de refus (E3) du chargement de l'application.
5. Procédé d'autorisation selon l'une des revendications 2 à 4, caractérisé en ce qu'un identifiant dudit utilisateur (ES_uid) et au moins un type d'application autorisée pour ledit utilisateur (APP_tid) sont enregistrées sous forme d'un certificat (Cert) dans une mémoire de l'élément de sécurité.
6. Dispositif d'autorisation du chargement d'une application (APP, SPB) dans un élément de sécurité (ES, iSSP) apte à communiquer avec un serveur (SAES) de chargement d'un fournisseur d'applications, le dispositif comportant :

- un module (PG, MEM) d'obtention d'au moins un type d'application autorisée (APP_tid);
- un module d'obtention du type de l'application à charger (APP_t) ;
- un module de comparaison du type de l'application à charger (APP_t) et du type d'application autorisée (APP_tid) ;
- un module d'autorisation du chargement (E6) de l'application (COM, SPBL), en fonction des résultats de la comparaison.

7. Carte électronique (SIM, iSSP) comportant un dispositif d'autorisation selon la revendication 6.

8. Zone mémoire sécurisée (TEE) comportant un dispositif d'autorisation selon la revendication 6.

9. Programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 5, lorsque le programme est exécuté par un processeur.

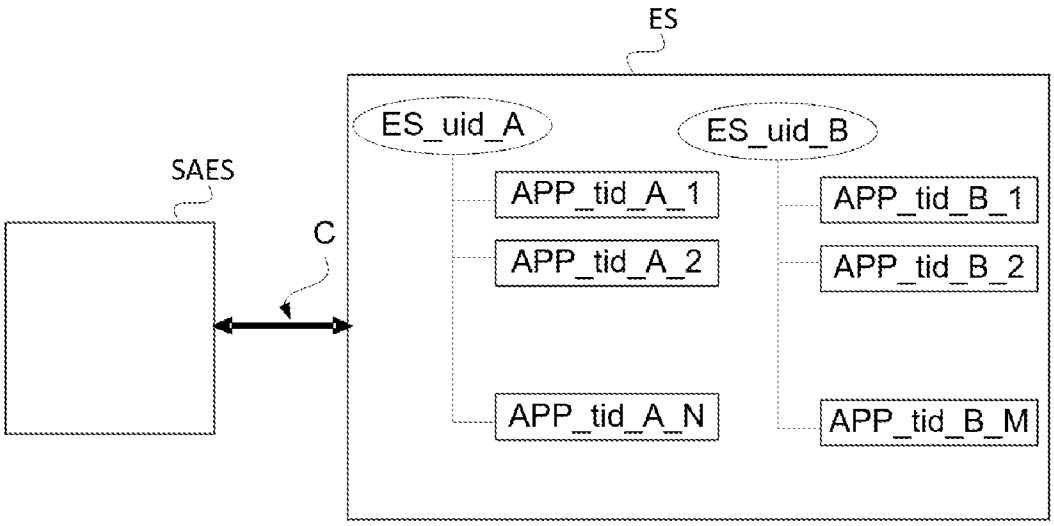


Figure 1

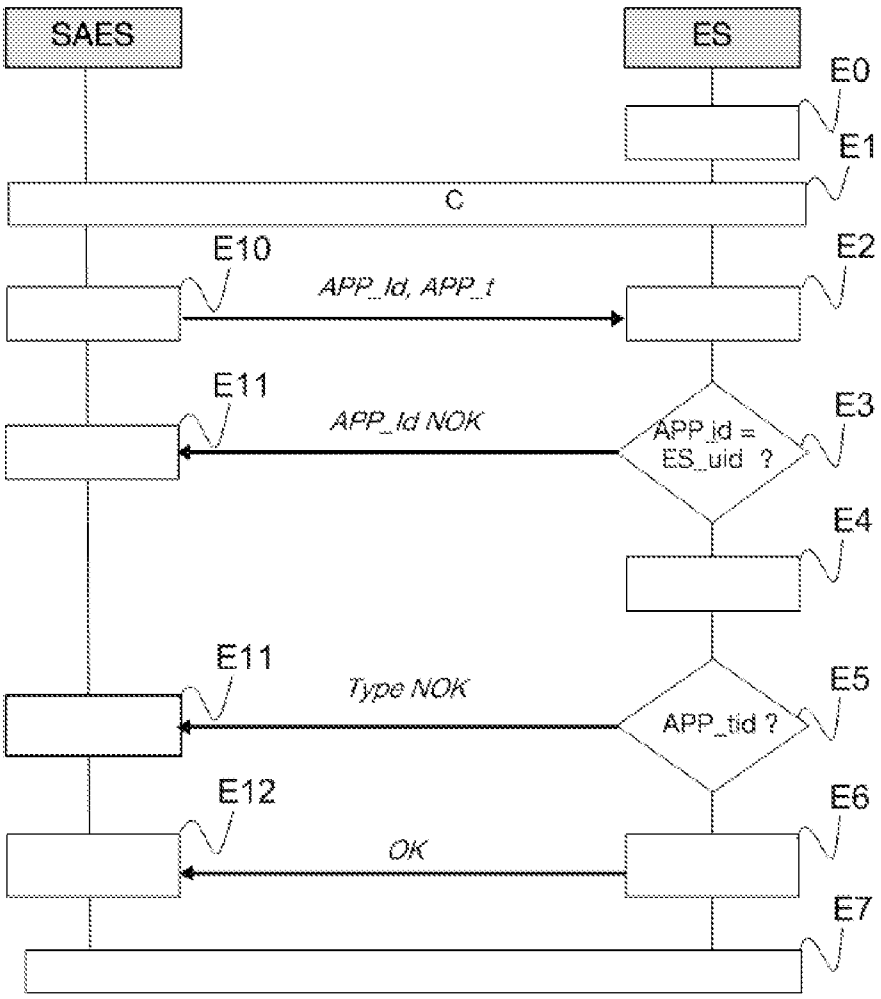


Figure 2

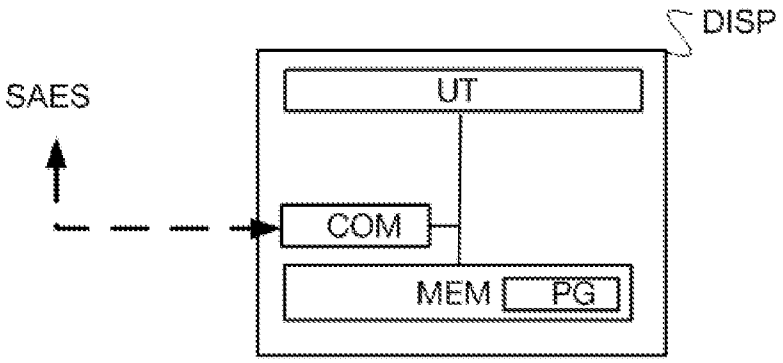


Figure 3

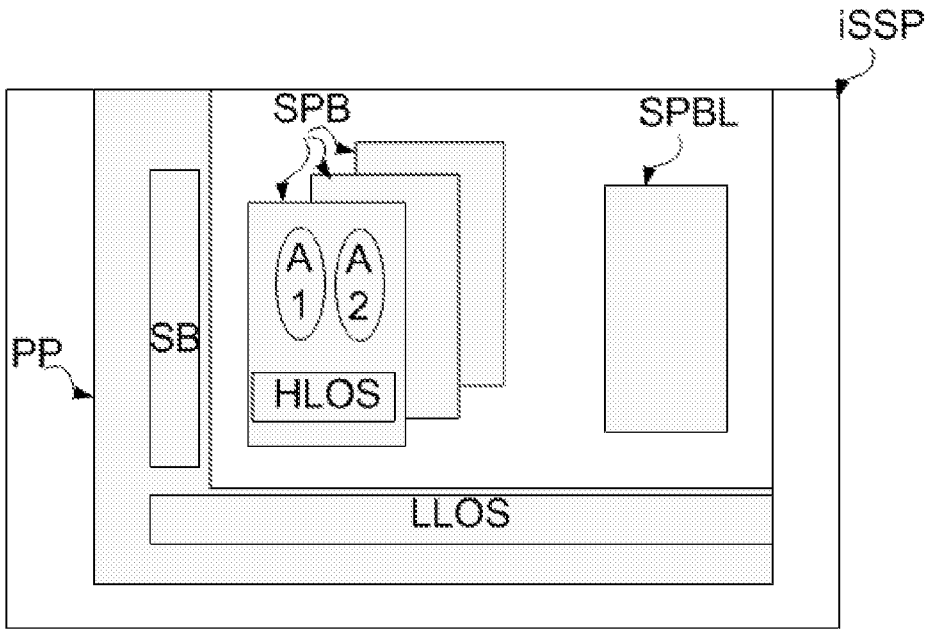


Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR2020/050017

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/51(2013.01)i; ***G06F 21/57***(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 107944261 A (GUANGDONG XIAOTIANCAI TECHNOLOGY CO LTD) 20 April 2018 (2018-04-20) paragraph [0006] paragraph [0026] paragraph [0079] paragraph [0085] - paragraph [0088]	1-9
A	CN 107944262 A (GUANGDONG XIAOTIANCAI TECHNOLOGY CO LTD) 20 April 2018 (2018-04-20) paragraph [0067] - paragraph [0078]; figure 1 paragraph [0080] - paragraph [0107]	1-9

☐ 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	Date of mailing of the international search report
04 March 2020	**13 March 2020**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Vinck, Bart** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FR2020/050017

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 107944261 A	20 April 2018	NONE	
CN 107944262 A	20 April 2018	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2020/050017

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/51 G06F21/57
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)
G06F

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

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CN 107 944 261 A (GUANGDONG XIAOTIANCAI TECHNOLOGY CO LTD) 20 avril 2018 (2018-04-20) alinéa [0006] alinéa [0026] alinéa [0079] alinéa [0085] - alinéa [0088] -----	1-9
A	CN 107 944 262 A (GUANGDONG XIAOTIANCAI TECHNOLOGY CO LTD) 20 avril 2018 (2018-04-20) alinéa [0067] - alinéa [0078]; figure 1 alinéa [0080] - alinéa [0107] -----	1-9

☐ 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	Date d'expédition du présent rapport de recherche internationale
4 mars 2020	13/03/2020

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

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2020/050017

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
CN 107944261 A	20-04-2018	AUCUN	
CN 107944262 A	20-04-2018	AUCUN	