(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 067 485**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **17 55844**

(51) Int Cl[8] : ***G 06 F 21/44*** *(2013.01), G 06 F 21/57, 21/62*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26.06.17.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 14.12.18 Bulletin 18/50.

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

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

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

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

(72) **Inventeur(s) :** FILIPIAK ALICIA et GHAROUT SAID.

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

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

(54) PROCEDE DE CONTROLE D'ACCES A UN MODULE DE SECURITE.

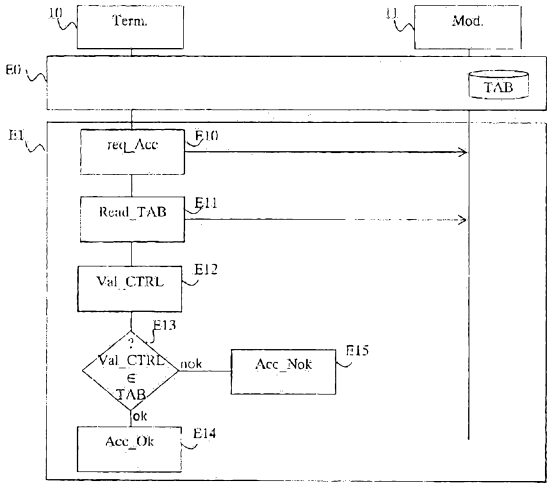
(57) L'invention concerne un procédé de contrôle d'accès à un module de sécurité (11) d'un terminal mobile (10) par une application du terminal mobile, ledit procédé comprenant :

- envoi (E10) par une application courante du terminal mobile d'une requête d'accès (sendAPDU) au module de sécurité, ladite requête d'accès comprenant l'identifiant courant (AIDj) d'une applet comprise dans le module de sécurité,

-lecture (E11) par le système d'exploitation du terminal mobile d'une table de correspondance (TAB) comprenant un ensemble de règles de contrôle d'accès, une règle de contrôle d'accès comprenant l'identifiant d'une applet du module de sécurité associé à une valeur de contrôle pour une application du terminal mobile, ladite règle de contrôle d'accès indiquant que ladite application du terminal mobile est autorisée à communiquer avec l'applet du module de sécurité,

- obtention (E12) d'une valeur de contrôle courante pour l'application courante à partir d'au moins un certificat d'un développeur de l'application courante et d'un identifiant de l'application courante, associés à l'application courante,

- recherche (E13) dans la table de correspondance d'une règle de contrôle d'accès comprenant l'identifiant courant de l'applet associé à la valeur de contrôle courante, l'application courante étant autorisé à communiquer avec l'applet courante lorsque la recherche est positive.



FR 3 067 485 - A1

Procédé de contrôle d'accès à un module de sécurité

La présente invention concerne un procédé de contrôle d'accès d'une application d'un terminal mobile à un module de sécurité compris dans le terminal.

Elle trouve une application particulièrement intéressante dans l'exécution de services sensibles tels que par exemple des services de paiement mobile pour lesquels l'exécution d'opérations sensibles nécessite de contrôler l'accès, depuis le système d'exploitation du terminal mobile qui exécute une application du terminal mobile, à des applications comprises dans le module de sécurité et habituellement appelées « applets ». L'application comprise dans le terminal mobile fait appel à des applets du module de sécurité afin de réaliser certaines opérations de sécurité, telles que par exemple une opération de signature cryptographique, une opération de vérification d'un code PIN (pour « Personal Identification Number »), etc.

La communication entre une application du terminal mobile et le module de sécurité est définie au moyen d'une interface appelée Open Mobile API, définie par un consortium industriel appelé SIMAlliance ; l'interface Open Mobile API est maintenue par l'association GlobalPlatform. Cette interface permet de déterminer si une application du terminal mobile est autorisée à accéder au module sécurité, plus précisément à dialoguer avec une applet du terminal mobile, et de garantir que l'accès à une fonctionnalité du module de sécurité est limité à ce qui est nécessaire au bon fonctionnement de l'application. Le schéma de contrôle d'accès supporté par l'interface OpenMobile API a quant à lui été spécifié par l'association GlobalPlatform. Le contrôle d'accès défini par GlobalPlatform repose sur un standard connu et normalisé, appelé PKCS#15 (« Public Key Crytpography Standards ») qui permet à des utilisateurs de périphériques cryptographiques qui renferment des clés cryptographiques de s'identifier auprès des applications, indépendamment de l'implémentation de l'interface du périphérique cryptographique. GlobalPlatform définit également l'ensemble des règles présentes sur le module de sécurité qui déterminent ce qu'une application a le droit ou non de demander au module de sécurité. Par exemple, une règle peut préciser qu'une application X, présente sur le terminal mobile est autorisée à interagir avec une applet Y, présente sur le module de sécurité, identifiée par un identifiant d'applet normalisé désigné par « AID » (pour « Application IDentifier »), et présente dans le module de sécurité. L'identifiant d'applet AID permet d'identifier de manière unique le fournisseur de l'applet ainsi que cette applet chez ce fournisseur.

L'interface Open Mobile API, ou « OMAPI », décrit une interface permettant la communication entre une application du terminal mobile et une applet du module de sécurité. Cette interface est indépendante du système d'exploitation du terminal mobile. Une application

mobile installée dans le terminal mobile interroge, via l'interface OMAPI, une applet comprise dans le module de sécurité. A cette fin, le module de sécurité mémorise une table de correspondance définie par l'entité qui a émis le module de sécurité, par exemple un opérateur de réseau ou un administrateur du module, et qui comprend un ensemble de règles qui associe un identifiant d'applet du module de sécurité à une valeur de contrôle qui permet de vérifier qu'une application du terminal mobile est autorisée à interagir avec l'applet. Cette table de correspondance est récupérée au niveau du terminal mobile par l'interface OMAPI qui la consulte à chaque requête d'accès au module de sécurité émise par une application. La récupération de la table de correspondance qui contient les règles de contrôle d'accès peut se faire également en interrogeant une applet dans le module de sécurité appelée « ARA-M » (pour « Access Rule Application Master»), spécifiée par GlobalPlatform. C'est donc au niveau de cette interface que se fait le contrôle d'identification et de droit d'accès de l'application.

La valeur de contrôle qui permet de contrôler qu'une application du terminal mobile est autorisée à accéder au module de sécurité comprend le résultat d'une fonction de hachage appliquée à une valeur fournie par le développeur de l'application. Actuellement, le développeur fournit comme valeur soit une empreinte numérique (ou « hash » en anglais) de son propre certificat de développeur, c'est-à-dire de l'ensemble des champs qui composent son certificat, soit une empreinte numérique du certificat de l'application. Le contrôle d'accès consiste alors à vérifier que la valeur de contrôle qui est présente dans la table de correspondance est égale à une valeur de contrôle courante calculée à partir d'informations associées à l'application qui s'exécute et qui souhaite communiquer avec le module de sécurité. A noter que les mécanismes de contrôle d'accès peuvent se contenter de vérifier une empreinte numérique car le certificat à partir duquel l'empreinte a été calculée a déjà été vérifié par le système d'exploitation lors de l'installation de l'application ; son intégrité est donc garantie.

Dans le premier cas où le développeur fournit l'empreinte de son propre certificat de développeur, si plusieurs applications développées par le même développeur sont installées sur le terminal mobile, alors les autorisations d'accès au module de sécurité sont partagées par l'ensemble des applications concernées, quand bien même certaines de ces applications n'auraient aucun besoin d'accéder au module de sécurité. Cela constitue une vulnérabilité pouvant créer une faille de sécurité. En effet, un opérateur ou un fournisseur de services pourrait dans certains cas sous-traiter le développement de ses applications à des tiers. Au final, les différentes applications sont signées ou validées en utilisant le même certificat développeur, en l'espèce celui de l'opérateur ou du fournisseur de service. Il n'est donc pas exclu que certaines des applications développées par des tiers dévient de leurs fonctionnement normal et tentent,

volontairement ou par erreur, de dialoguer avec des applets du module de sécurité, alors que cela n'a pas été spécifié initialement.

Dans le deuxième cas où le champ qui identifie une application correspond à l'empreinte numérique du certificat de l'application, alors chaque modification de l'application nécessite pour l'opérateur de procéder à une mise à jour à distance de la table de correspondance présente dans le module de sécurité. En effet, la mise à jour d'une application, telle qu'un changement de version, entraîne la génération d'un nouveau certificat associé à l'application et donc une modification de l'empreinte numérique du certificat. La mise à jour à distance de modules de sécurité par l'opérateur est cependant une opération coûteuse qu'il convient de limiter, surtout dans le cas où le nombre de modules à mettre à jour est important.

Un des buts de l'invention est de remédier à des insuffisances/inconvénients de l'état de la technique et/ou d'y apporter des améliorations.

A cette fin, l'invention propose un procédé de contrôle d'accès à un module de sécurité d'un terminal mobile par une application du terminal mobile, ledit procédé comprenant :

- envoi par une application courante du terminal mobile d'une requête d'accès au module de sécurité, ladite requête d'accès comprenant l'identifiant courant d'une applet comprise dans le module de sécurité,
- lecture par le système d'exploitation du terminal mobile d'une table de correspondance comprenant un ensemble de règles de contrôle d'accès, une règle de contrôle d'accès comprenant l'identifiant d'une applet du module de sécurité associé à une valeur de contrôle pour une application du terminal mobile, ladite règle de contrôle d'accès indiquant que ladite application du terminal mobile est autorisée à communiquer avec l'applet du module de sécurité,
- obtention d'une valeur de contrôle courante pour l'application courante à partir d'au moins un certificat d'un développeur de l'application courante et d'un identifiant de l'application courante, associés à l'application courante,
- recherche dans la table de correspondance d'une règle de contrôle d'accès comprenant l'identifiant courant de l'applet associé à la valeur de contrôle courante, l'application courante étant autorisé à communiquer avec l'applet courante lorsque la recherche est positive.

En associant à l'identifiant d'une applet du module de sécurité une valeur de contrôle pour une application obtenue à partir du certificat du développeur de l'application et de l'identifiant de l'application, on limite de manière stricte et rigoureuse ce que peut demander l'application du terminal mobile au module de sécurité. En effet, la valeur de contrôle de l'application du terminal mobile, qui dépend du développeur, est également propre à

l'application de par sa dépendance à un identifiant unique de l'application. Ainsi, même si un développeur fournit une pluralité d'applications au terminal mobile, la façon dont la valeur de contrôle associée à l'application est obtenue permet de distinguer les différentes applications développées par ce développeur. Ainsi une application qui n'a pas besoin d'accéder au module de sécurité ne se voit pas accorder un droit d'accès au module de sécurité du fait du développeur qui en est à l'origine. Par ailleurs, même si un développeur mal intentionné parvient à forger l'identifiant d'une application autorisée à communiquer avec le module de sécurité, la dépendance de la valeur de contrôle au certificat du développeur ne permettra pas une communication de l'application développée par ce développeur avec le module de sécurité.

Par ailleurs, l'utilisation d'un identifiant de l'application dans la valeur de contrôle, qui permet de limiter l'accès au module de sécurité à cette seule application, garantit une certaine pérennité de l'entrée de la table de correspondance lors d'un changement de version de l'application sur le terminal mobile. En effet, lorsqu'une nouvelle version de l'application est chargée sur le terminal mobile, il n'est pas nécessaire de mettre à jour l'entrée de la table de correspondance au niveau du module de sécurité puisque même si le code de l'application du terminal mobile a été mis à jour, l'identifiant de l'application est resté le même. Cela évite des procédures coûteuses de mise à jour à distance du module de sécurité lorsque la valeur de contrôle est fonction du certificat de l'application, un nouveau certificat étant réémis pour l'application à chaque changement de version de cette application. Cela est d'autant plus vrai que le nombre de modules de sécurité à mettre à jour est important.

Dans un premier exemple de réalisation, la valeur de contrôle courante est obtenue par concaténation d'une empreinte numérique du certificat du développeur de l'application courante et de l'identifiant de l'application courante.

Dans cet exemple de réalisation, l'espace mémoire est optimisé. En effet, l'espace dans la table de correspondance dédié au stockage de la valeur de contrôle est limité, ce qui peut nécessiter de tronquer la valeur de contrôle. Une telle troncature se fait au détriment de la sécurité. En effet, le risque que deux valeurs de contrôle de deux applications différentes soient égales ne peut être écarté.

Dans un deuxième exemple de réalisation, la valeur de contrôle courante comprend dans un premier champ une empreinte numérique du certificat du développeur de l'application courante et dans un deuxième champ l'identifiant de l'application courante.

Dans cet exemple de réalisation, qui correspond à un autre choix d'implémentation de la table de correspondance, la sécurité est optimisée. En effet, les risques d'obtenir deux entrées de la table de correspondance identiques pour deux applications différentes est réduit au minimum.

Dans un autre exemple de réalisation, la valeur de contrôle courante est obtenue à partir d'une signature numérique du certificat du développeur de l'application courante et de l'identifiant de l'application courante.

Dans cet exemple, la valeur de contrôle, qui est obtenue à partir de la signature du certificat du développeur de l'application courante et de l'identifiant de l'application courante, renforce la sécurité dans le sens où la valeur de contrôle intègre le lien entre l'Autorité de Certification et le développeur. A noter que le système d'exploitation met en œuvre une vérification de l'application, i.e., de la signature du certificat au moyen de la clé publique de l'Autorité de Certification qui a délivré le certificat, au moment de l'installation de celle-ci sur le terminal mobile. Bien sûr, dans le cas de certificats auto-signés, l'Autorité de Certification est la développeur.

Dans un exemple de réalisation, la table de correspondance est une structure de données conforme au format PKCS#15.

La table de correspondance est une entrée du fichier PKCS#15 du terminal mobile. PKCS#15 est un format standard approuvé utilisé pour le transfert de données sensibles entre une application et un périphérique de type module de sécurité. Ainsi, la table de correspondance est adaptée à tout type de terminal mobile.

L'invention concerne aussi un terminal mobile comprenant une application apte à demander à communiquer avec une applet d'un module de sécurité du terminal mobile, ledit terminal mobile comprenant :

- moyens d'envoi, agencés pour qu'une application courante du terminal mobile envoie une requête d'accès au module de sécurité, ladite requête d'accès comprenant l'identifiant courant d'une applet comprise dans le module de sécurité,

- moyens de lecture, agencés pour que le système d'exploitation du terminal mobile lise d'une table de correspondance comprenant un ensemble de règles de contrôle d'accès, une règle de contrôle d'accès comprenant l'identifiant d'une applet du module de sécurité associé à une valeur de contrôle pour une application du terminal mobile, ladite règle de contrôle d'accès indiquant que ladite application du terminal mobile est autorisée à communiquer avec l'applet du module de sécurité,

- moyens d'obtention, agencés pour obtenir une valeur de contrôle courante pour l'application courante à partir d'au moins un certificat d'un développeur de l'application courante et d'un identifiant de l'application courante, associés à l'application courante,

- moyens de recherche, agencés pour rechercher dans la table de correspondance d'une règle de contrôle d'accès comprenant l'identifiant courant de l'applet associé à la valeur de

contrôle courante, l'application courante étant autorisée à communiquer avec à l'applet courante lorsque la recherche est positive.

L'invention concerne également un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal mobile, le programme comprenant des portions de code pour l'exécution des étapes du procédé de contrôle d'accès décrit précédemment, lorsque le programme est exécuté sur ledit terminal mobile.

L'invention concerne aussi un support de données dans lequel est enregistré le programme ci-dessus.

D'autres caractéristiques et avantages de la présente invention seront mieux compris de la description et des dessins annexés parmi lesquels :

- la figure 1 présente les étapes d'un procédé de contrôle d'accès à un module de sécurité par une application du terminal mobile, selon un exemple de réalisation ;
- la figure 2 est une représentation schématique d'un terminal mobile apte à mettre en œuvre le procédé de contrôle d'accès, selon un exemple de réalisation de l'invention.

Les étapes d'un procédé de contrôle d'accès à un module de sécurité par une application du terminal mobile, selon un exemple de réalisation, vont maintenant être décrites en relation avec la figure 1.

Un terminal mobile 10 est équipé d'un module de sécurité 11, embarqué ou pas, ou (e)SIM (pour « (embedded) Subscriber Identity Module »), de type « (e)UICC » (de l'anglais « (embedded) Universal Integrated Circuit Card »). Le module de sécurité 11 est agencé pour gérer des applications opérateur qui se trouvent dans le module ou, dans le cas d'un module de type eUICC, dans un profil dédié à un opérateur. Le terminal mobile 10 est un équipement mobile grand public, par exemple un terminal intelligent de type smartphone, une tablette, etc.

Dans l'exemple de réalisation décrit ici, le module de sécurité est de type UICC, adapté pour gérer des applications d'un opérateur qui se trouvent dans le module de sécurité 11. Dans ce cas le module de sécurité 11 a été émis par l'opérateur.

Le module de sécurité 11 héberge des applications et des données confidentielles manipulées par ces applications. Ces applications comprises dans le module de sécurité s'exécutent dans un environnement dédié appelé « Java Card ». Dans ce contexte, ces applications sont habituellement appelées « applets ». C'est ce terme qui est utilisé par la suite pour désigner les applications qui s'exécutent dans le module de sécurité.

Dans une phase préalable E0 de configuration initiale du module de sécurité 11, un opérateur de réseau mobile (non représenté sur la figure 1), en charge du module de sécurité 11,

configure une table de correspondance TAB pour le module de sécurité 11. La table de correspondance TAB associe une applet, identifiée par un identifiant normalisé d'applet AID (pour « Application Identifier »), à une valeur de contrôle associée à une application du terminal mobile afin d'indiquer que l'application du terminal mobile est autorisée à communiquer avec l'applet comprise dans le module de sécurité 11. En d'autres termes, la table de correspondance TAB comprend des informations qui déterminent ce que des applications du terminal mobile 10 ont le droit de demander au module de sécurité 11.

A noter qu'une application d'un terminal mobile est habituellement certifiée. Une telle certification permet de garantir à l'utilisateur du terminal l'origine de l'application lors de l'installation de celle-ci sur le terminal mobile. La certification repose en général sur des certificats électroniques de confiance, par exemple des certificats électroniques de clés publiques au format X.509. Les certificats X.509 sont supposés connus. Pour mémoire, on rappelle qu'un certificat X.509, attribué par une autorité de confiance appelée habituellement « Autorité de Certification », lie une clé publique d'un couple clé publique/clé privée à un nom, par exemple un adresse électronique, un enregistrement DNS (de l'anglais « Domain Name System »), etc., et que le certificat comprend une signature de l'ensemble des champs du certificat calculée au moyen de la clé privée de l'Autorité de Certification, détenue uniquement par cette Autorité. La vérification du certificat est ensuite effectuée au moyen de la clé publique de l'Autorité de Certification. A noter qu'il existe des certificats auto-signés. Dans ce cas, les champs du certificat sont signés au moyen de la clé privée associée à la clé publique pour laquelle le certificat a été généré. Les certificats auto-signés sont en général à usage interne. Par exemple, un opérateur de réseau peut utiliser des certificats auto-signés pour certifier des applications pour des terminaux mobiles qui comprennent des modules de sécurité qu'il a délivrés. Par exemple, l'opérateur « Orange » peut avoir un certificat développeur auto-signé pour des applications qu'il propose. A contrario, un certificat signé par une Autorité de Certification universellement reconnue, par exemple, la GSMA (pour « GSM Association ») peut être utilisé pour certifier des applications fournies par différents opérateurs et destinées à être exécutées sur un terminal mobile qui embarque un module de sécurité comprenant une pluralité de profils, chaque profil étant propre à un de ces opérateurs de réseau.

Une entité qui a développé une application pour terminal mobile et qui est appelée par la suite « développeur », par exemple « Orange », joint au code de l'application dans ce qui est communément appelée une « enveloppe de l'application », son propre certificat de développeur accompagné d'un élément de vérification de ce certificat, par exemple une empreinte numérique de l'ensemble des champs de ce certificat. L'enveloppe de l'application est comprise dans le code de l'application qui s'exécute et qui est chargé par le système d'exploitation du terminal

mobile. L'empreinte numérique est obtenue par l'application d'une fonction de hachage, par exemple SHA-1 ou SHA-256 (pour « Secure Hash Algorithm »), à l'ensemble des champs du certificat tel que normalisé par exemple pour les certificats X.509 à l'IETF (pour « Internet Engineering Task Force »). La présentation de l'empreinte peut dépendre du système d'exploitation du terminal. En tout état de cause, si un seul champ du certificat est modifié, l'empreinte change. L'empreinte numérique du certificat peut ensuite être vérifiée en appliquant la même fonction de hachage à l'ensemble des champs du certificat et en comparant le résultat à l'empreinte comprise dans l'enveloppe de l'application. Dans une variante de réalisation, plus légère en termes d'implémentation, l'empreinte numérique est obtenue en appliquant une fonction de hachage à la clé publique du certificat.

Dans un autre exemple de réalisation, l'élément de vérification du certificat est la signature de l'ensemble des champs du certificat calculée au moyen de la clé privée associée à la clé publique du certificat. Dans une variante, l'élément de vérification est une signature de la clé publique du certificat calculée au moyen de la clé privée associée à la clé publique certifiée par le certificat.

La table de correspondance TAB comprend une pluralité d'entrées, chaque entrée définit une règle qui est dédiée à la communication d'une application du terminal mobile avec une applet comprise dans le module de sécurité 11. Ainsi, pour une i-ième entrée, la table de correspondance TAB comprend dans un premier champ un identifiant AID_i d'une applet comprise dans le module de sécurité 11, et dans un deuxième champ une valeur de contrôle représentative d'une application AP_i du terminal mobile 10 qui est autorisée à émettre une requête d'accès au module de sécurité 11 qui concerne l'applet AID_i. La valeur de contrôle comprise dans le deuxième champ de la i-ième entrée de la table TAB est obtenue à partir d'au moins deux informations associées à l'application du terminal mobile 10. Le format de l'identifiant d'une application peut varier selon le système d'exploitation du terminal mobile 10. Il peut être propriétaire. Pour un système d'exploitation Androïd, un identifiant d'application est par exemple de la forme « com.orange.pay ». Pour un système d'exploitation iOS, un identifiant d'application est par exemple de la forme « 12345ABCDE.com.orange.pay », où la partie gauche « 12345ABCDE », correspond à un identifiant du développeur, « Orange » par exemple. A noter que ces exemples d'identifiant ne dépendent pas d'une version de l'application ou du code. Un tel format permet d'identifier de façon unique une application parmi l'ensemble des applications d'un fournisseur ou développeur d'applications, ici le développeur, ou opérateur, « Orange ».

Dans une variante de réalisation, l'identifiant de l'application est dans un format normalisé qui comprend un ensemble de champs qui ensemble identifient de manière unique et

universelle l'application. Dans ce format, l'identifiant d'application est également indépendant du code et/ou de la version de l'application. A noter que lorsque l'identifiant de l'application est conforme au format d'identifiant d'application normalisé alors celui-ci comprend un champ qui identifie le développeur. La valeur de contrôle qui comprend l'empreinte du certificat du développeur permet dans ce cas de valider l'origine et l'intégrité de l'application à partir de l'identifiant de l'application en vérifiant que le champ développeur qu'il comprend correspond au développeur dont l'empreinte de certificat est fourni dans la valeur de contrôle. Ainsi, il n'est pas nécessaire de disposer d'un certificat de l'application pour contrôler l'origine et l'intégrité de l'application.

Dans un premier exemple de réalisation, la valeur de contrôle de l'application AP_i du terminal mobile est obtenue en concaténant l'empreinte numérique des champs du certificat du développeur de l'application avec l'identifiant de l'application. Dans ce premier exemple de réalisation, l'espace mémoire est optimisé. En effet, l'espace dans la table de correspondance TAB dédié au stockage de la valeur de contrôle est limité, ce qui peut nécessiter de tronquer la valeur de contrôle. Une telle troncature se fait au détriment de la sécurité. En effet, dans ce cas le risque que deux valeurs de contrôle de deux applications différentes soient égales augmente. Dans un deuxième exemple de réalisation, la valeur de contrôle de l'application AP_i comprend deux sous-champs : un premier sous-champ qui comprend l'empreinte numérique du certificat du développeur de l'application et un deuxième sous-champ qui comprend l'identifiant de l'application. Dans cet exemple de réalisation, la sécurité est optimisée. En effet, les risques d'obtenir deux entrées identiques dans la table de correspondance TAB pour deux applications différentes sont réduits au minimum. Dans une variante de réalisation, au lieu de l'identifiant de l'application, c'est un haché de l'identifiant de l'application, calculé au moyen d'une fonction de hachage qui est utilisé pour obtenir la valeur de contrôle de l'application AP_i. Le haché de l'identifiant de l'application a une taille fixe, ce qui peut faciliter l'implémentation. Bien sûr, l'invention n'est pas limitée à ces exemples pour l'obtention de la valeur de contrôle.

En associant à un identifiant d'applet, ici AID_i, du module de sécurité 11 une combinaison de l'empreinte numérique du certificat du développeur de l'application et de l'identifiant de l'application, on limite de manière stricte et rigoureuse ce que peut demander l'application du terminal mobile au module de sécurité 11. En effet, la valeur de contrôle de l'application AP_i du terminal mobile qui dépend du développeur est également propre à l'application de par sa dépendance à l'identifiant de l'application. Ainsi, même si un développeur fournit une pluralité d'applications au terminal mobile, la façon dont la valeur de contrôle associée à l'application est obtenue permet de distinguer les applications de ce développeur. Par ailleurs, la présence de l'identifiant de l'application qui permet de limiter

l'accès au module de sécurité à cette seule application, garantit une certaine pérennité de l'entrée de la table lors d'un changement de version de l'application sur le terminal mobile. Lorsqu'une nouvelle version de l'application est chargée sur le terminal mobile, il n'est pas nécessaire de mettre à jour l'entrée de la table de correspondance TAB. En effet, même si le code de l'application du terminal mobile a été mis à jour, l'identifiant de l'application reste le même. Cela évite ainsi des procédures complexes et coûteuses de mise à jour à distance de la table de correspondance TAB par l'opérateur.

La table de correspondance TAB ainsi créée est configurée par l'opérateur sur le module de sécurité 11 du terminal 10 en fin de phase de configuration E0. Cette configuration est mise en œuvre au moyen de procédures sécurisées connues, par exemple au moyen de procédures OTA (de l'anglais « Over The Air »), une fois le module de sécurité 11 et le terminal mobile 10 mis en circulation. Dans un autre exemple de réalisation, la configuration de la table de correspondance TAB dans le module de sécurité 11 est effectuée en usine, avant la mise en circulation du module de sécurité. Une telle configuration est adéquate pour des applications qui se trouvent par défaut sur le terminal mobile lors de sa mise en circulation ; elle évite une mise à jour a posteriori au moyen de procédures OTA, qui sont coûteuses pour l'opérateur.

Dans une phase ultérieure E1 d'utilisation, on suppose qu'une application courante AP_j installée sur le terminal mobile 10 est exécutée, par exemple à l'initiative de l'utilisateur qui l'a sélectionnée à partir d'un menu du terminal. On suppose que l'application courante AP_j est une application sensible qui a besoin d'exécuter une ou plusieurs applets comprises dans le module de sécurité 11.

Dans une étape E10 d'envoi d'une requête d'accès, le terminal mobile 10, plus précisément, le système d'exploitation du terminal mobile 10 qui exécute les instructions de code de l'application courante AP_j du terminal mobile 10 qui ont été chargées en mémoire, envoie une requête d'accès sendAPDU au module de sécurité 11. La requête d'accès sendAPDU est une commande de type « send APDU » (pour « Application Protocol Data Unit »). Les messages APDU, normalisés, sont des messages habituellement échangés entre un module de sécurité et un lecteur de module. La requête d'accès comprend l'identifiant AID_j d'une applet courante du module de sécurité 11 avec laquelle l'application courante AP_j souhaite communiquer. Une telle requête d'accès envoyée au module de sécurité 11 est soumise à un contrôle d'accès. En effet, il convient de vérifier que l'application courante AP_j du terminal mobile 10 est autorisée à demander l'exécution par le module de sécurité 11 de l'applet courante AID_j qui correspond à une fonctionnalité sensible.

A cette fin, dans une étape E11 de lecture, le système d'exploitation, plus précisément une interface de contrôle d'accès, comprise dans le terminal mobile 10 et agencée pour vérifier

les autorisations d'accès d'une application mobile aux applets comprises dans le module de sécurité 11 lit la table de correspondance TAB qui comprend les règles de contrôle d'accès au module de sécurité 11 et qui est mémorisée dans le module de sécurité 11. Pour mémoire, une règle de contrôle d'accès comprend l'identifiant d'une applet du module de sécurité associé à une valeur de contrôle pour une application du terminal mobile. La présence de la règle de contrôle d'accès dans la table TAB indique que l'application du terminal mobile est autorisée à dialoguer avec l'applet du module de sécurité.

Dans une étape suivante E12 d'obtention d'une valeur de contrôle courante de l'application, le système d'exploitation du terminal mobile 10, plus précisément l'interface de contrôle d'accès au module de sécurité 11 qui est exécutée par le système d'exploitation, lit à partir de données associées à l'application courante AP_j du terminal mobile qui a envoyé la requête d'accès, une valeur de contrôle courante. La valeur de contrôle courante est comprise dans l'enveloppe de l'application courante comprise dans le code exécutable de l'application courante. C'est un élément d'information qui a été associé au code de l'application, par exemple par le développeur de l'application. Dans un exemple de réalisation, la valeur de contrôle courante est la concaténation de l'empreinte numérique des champs du certificat du développeur de l'application courante et d'un identifiant de l'application, par exemple « com.orange.pay ». Dans une variante de réalisation, l'empreinte numérique du certificat du développeur et l'identifiant de l'application sont associées à l'application en tant que deux valeurs distinctes. Dans ce cas, le système d'exploitation, plus précisément l'interface de contrôle d'accès au module de sécurité 11 concatène ces deux informations afin d'obtenir la valeur de contrôle courante pour l'application courante AP_j.

Dans une étape suivante E13 de recherche, le système d'exploitation du terminal mobile, plus précisément l'interface de contrôle d'accès au module de sécurité 11, recherche dans la table de correspondance TAB une règle qui comprend l'identifiant de l'applet courante AID_j et la valeur de contrôle courante de l'application AP_j.

Dans un premier cas (branche « ok » sur la figure 1) où une règle qui comprend l'identifiant de l'applet AID_j associée à la valeur de contrôle courante de l'application AP_j, indiquant que l'application du terminal mobile AP_j est autorisée à dialoguer avec l'applet AID_j du module de sécurité 11, est trouvée dans la table TAB, alors dans une étape E14 d'accès, l'application AP_j accède à l'applet AID_j. Cet accès comprend l'exécution de l'applet AID_j dans le module de sécurité 11 et l'envoi d'un résultat d'exécution à l'application courante AP_j du terminal mobile 10.

Dans un deuxième cas (branche « nok » sur la figure 1) où aucune règle comprenant l'applet AID_j et la valeur de contrôle courante de l'application AP_j n'est trouvée dans la table,

l'accès est refusé dans une étape E15 de fin. Un code d'erreur peut être envoyé à l'application courante du terminal mobile 10 et un message peut être affiché à l'attention de l'utilisateur sur une interface du terminal mobile 10.

La table de correspondance TAB est une structure de données qui respect le format d'un fichier PKCS#15. PKCS#15 est un format standard, approuvé, utilisé pour le transfert de données sensibles entre une application et un périphérique de type module de sécurité. Ainsi, la table de correspondance est adaptée à tout type de terminal mobile.

Dans l'exemple de réalisation décrit précédemment, la valeur de contrôle d'une application est obtenue à partir de l'empreinte des champs du certificat du développeur et de l'identifiant de l'application. L'invention n'est pas limitée à cet exemple. Ainsi, dans un autre exemple de réalisation, la valeur de contrôle est obtenue à partir d'une empreinte numérique de la clé publique du certificat et de l'identifiant de l'application. Cet exemple est plus léger en termes d'implémentation. Dans un autre exemple de réalisation, la valeur de contrôle est obtenue à partir d'une signature des champs du certificat du développeur et de l'identifiant de l'application. Enfin, dans un autre exemple de réalisation, la valeur de contrôle est obtenue à partir d'une signature de la clé publique du certificat du développeur et de l'identifiant de l'application. La prise en compte de la signature du certificat ou de la signature de la clé publique du certificat utilisation dans la valeur de contrôle implique l'Autorité de Certification.

Un terminal mobile 10, agencé pour mettre en œuvre le procédé de contrôle d'accès d'une application au module de sécurité, selon un exemple de réalisation, va maintenant être décrit en relation avec la figure 2.

Le terminal mobile 10 est un équipement mobile grand public, par exemple un terminal intelligent de type smartphone, une tablette, etc., équipé d'un module de sécurité 11 (e)SIM, de type (e)UICC. Le module de sécurité 11 est agencé pour gérer des applications opérateur qui se trouvent dans le module ou, dans le cas d'un module de type eUICC, dans un profil dédié à un opérateur.

Le terminal mobile 10 est un équipement informatique qui comprend de manière classique :

- une unité de traitement ou processeur 101, ou "CPU" (de l'anglais "Central Processing Unit"), destinée à charger des instructions en mémoire, à les exécuter, à effectuer des opérations ;

- un ensemble de mémoires, dont une mémoire volatile 102, ou "RAM" (pour "Random Access Memory") utilisée pour exécuter des instructions de code, stocker des variables, etc., et une mémoire de stockage 103 de type « EEPROM » (de l'anglais « Electrically Erasable

Programmable Read Only Memory »). En particulier, la mémoire de stockage 103 est agencée pour mémoriser un module logiciel de contrôle d'accès qui comprend des instructions de code pour mettre en œuvre les étapes du procédé de contrôle d'accès tel que décrit précédemment. Le module logiciel constitue une interface d'accès au module de sécurité 11 pour les applications du terminal mobile 10. Plus précisément, lorsqu'une application du terminal mobile 10 chargée dans la mémoire du terminal mobile s'exécute et requiert l'accès à une applet du module de sécurité 11, le système d'exploitation qui exécute les instructions interagit avec le module de contrôle d'accès en tant qu'interface d'accès au module de sécurité 11.

Le terminal mobile 10 comprend également :

- un module d'envoi 104, agencé pour qu'une application courante du terminal mobile envoie une requête d'accès sendAPDU au module de sécurité 11. La requête d'accès comprend l'identifiant courant AID_j d'une applet comprise dans le module de sécurité à laquelle l'application souhaite accéder. Le module d'envoi 104 est agencé pour mettre en œuvre l'étape E10 du procédé de contrôle d'accès tel que décrit précédemment ;
- un module de lecture 105, agencé pour que le système d'exploitation du terminal mobile, plus précisément l'interface d'accès au module de sécurité, lise une table de correspondance TAB comprenant un ensemble de règles de contrôle d'accès, une règle de contrôle d'accès comprenant l'identifiant d'une applet du module de sécurité associé à une valeur de contrôle pour une application du terminal mobile. La règle de contrôle d'accès qui figure dans la table de correspondance TAB indique que l'application du terminal mobile est autorisée à accéder à l'applet du module de sécurité. Le module de lecture 105 est agencé pour mettre en œuvre l'étape E11 du procédé de contrôle d'accès tel que décrit précédemment ;
- un module d'obtention 106, agencé pour obtenir une valeur de contrôle courante pour l'application courante à partir d'au moins un certificat d'un développeur de l'application courante et d'un identifiant de l'application courante, associés à l'application. Le module d'obtention 106 est agencé pour mettre en œuvre l'étape E12 du procédé de contrôle d'accès tel que décrit précédemment ;
- un module de recherche 107, agencé pour rechercher dans la table de correspondance TAB une règle de contrôle d'accès comprenant l'identifiant courant de l'applet associé à la valeur de contrôle courante, l'accès par l'application courante à l'applet courante étant autorisé lorsque la recherche est positive. Le module de recherche 107 est agencé pour mettre en œuvre l'étape E13 du procédé de contrôle d'accès tel que décrit précédemment.

Les modules d'envoi 104, de lecture 105, d'obtention 106 et de recherche sont de préférence des modules logiciels comprenant des instructions logicielles pour mettre en œuvre les étapes du procédé de contrôle d'accès tel que précédemment décrit.

L'invention concerne donc aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé de contrôle d'accès tel que décrit précédemment lorsque ce programme est exécuté par un processeur du terminal 10,

- un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur décrit ci-dessus.

REVENDICATIONS

1. Procédé de contrôle d'accès à un module de sécurité (11) d'un terminal mobile (10) par une application du terminal mobile, ledit procédé comprenant :

- envoi (E10) par une application courante du terminal mobile d'une requête d'accès (sendAPDU) au module de sécurité, ladite requête d'accès comprenant l'identifiant courant (AID_j) d'une applet comprise dans le module de sécurité,

- lecture (E11) par le système d'exploitation du terminal mobile d'une table de correspondance (TAB) comprenant un ensemble de règles de contrôle d'accès, une règle de contrôle d'accès comprenant l'identifiant d'une applet du module de sécurité associé à une valeur de contrôle pour une application du terminal mobile, ladite règle de contrôle d'accès indiquant que ladite application du terminal mobile est autorisée à communiquer avec l'applet du module de sécurité,

- obtention (E12) d'une valeur de contrôle courante pour l'application courante à partir d'au moins un certificat d'un développeur de l'application courante et d'un identifiant de l'application courante, associés à l'application courante,

- recherche (E13) dans la table de correspondance d'une règle de contrôle d'accès comprenant l'identifiant courant de l'applet associé à la valeur de contrôle courante, l'application courante étant autorisé à communiquer avec l'applet courante lorsque la recherche est positive.

2. Procédé selon la revendication 1, dans lequel la valeur de contrôle courante est obtenue par concaténation d'une empreinte numérique du certificat du développeur de l'application courante et de l'identifiant de l'application courante.

3. Procédé selon la revendication 1, dans lequel la valeur de contrôle courante comprend dans un premier champ une empreinte numérique du certificat du développeur de l'application courante et dans un deuxième champ l'identifiant de l'application courante.

4. Procédé selon la revendication 1, dans lequel la valeur de contrôle courante est obtenue à partir d'une signature numérique du certificat du développeur de l'application courante et de l'identifiant de l'application courante.

5. Procédé selon l'une des revendications précédentes dans lequel la table de correspondance (TAB) est une structure de données conforme au format PKCS#15.

6. Terminal mobile (10) comprenant une application apte à demander à communiquer avec une applet d'un module de sécurité du terminal mobile, ledit terminal mobile comprenant :

- moyens d'envoi (104), agencés pour qu'une application courante du terminal mobile envoie une requête d'accès au module de sécurité, ladite requête d'accès comprenant l'identifiant courant d'une applet comprise dans le module de sécurité,

- moyens de lecture (105), agencés pour que le système d'exploitation du terminal mobile lise d'une table de correspondance (TAB) comprenant un ensemble de règles de contrôle d'accès, une règle de contrôle d'accès comprenant l'identifiant d'une applet du module de sécurité associé à une valeur de contrôle pour une application du terminal mobile, ladite règle de contrôle d'accès indiquant que ladite application du terminal mobile est autorisée à communiquer avec l'applet du module de sécurité,

- moyens d'obtention (106), agencés pour obtenir une valeur de contrôle courante pour l'application courante à partir d'au moins un certificat d'un développeur de l'application courante et d'un identifiant de l'application courante, associés à l'application courante,

- moyens de recherche (107), agencés pour rechercher dans la table de correspondance d'une règle de contrôle d'accès comprenant l'identifiant courant de l'applet associé à la valeur de contrôle courante, l'application courante étant autorisée à communiquer avec à l'applet courante lorsque la recherche est positive.

7. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal mobile, le programme comprenant des portions de code pour l'exécution des étapes du procédé de contrôle d'accès selon l'une des revendications 1 à 5, lorsque le programme est exécuté sur ledit terminal mobile.

8. Support de données dans lequel est enregistré le programme selon la revendication 7.

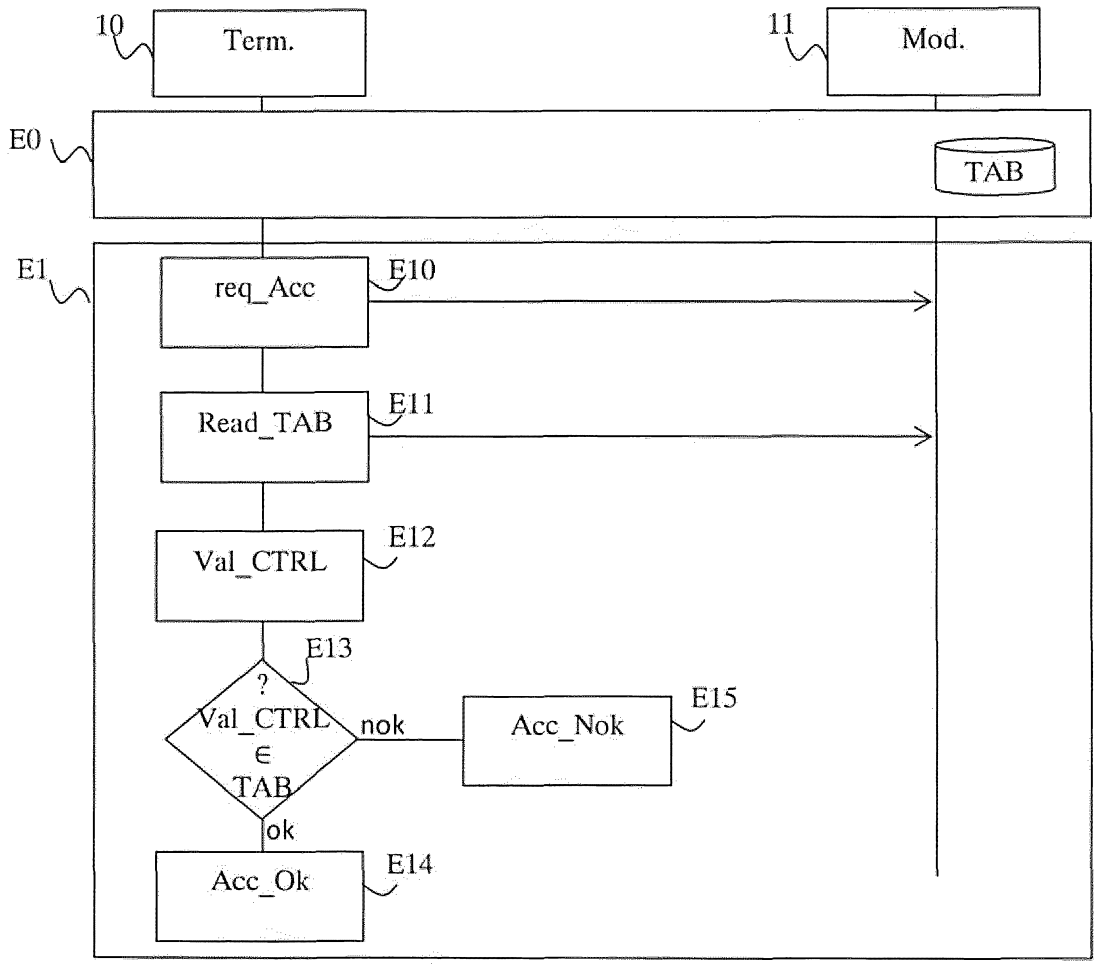


Figure 1

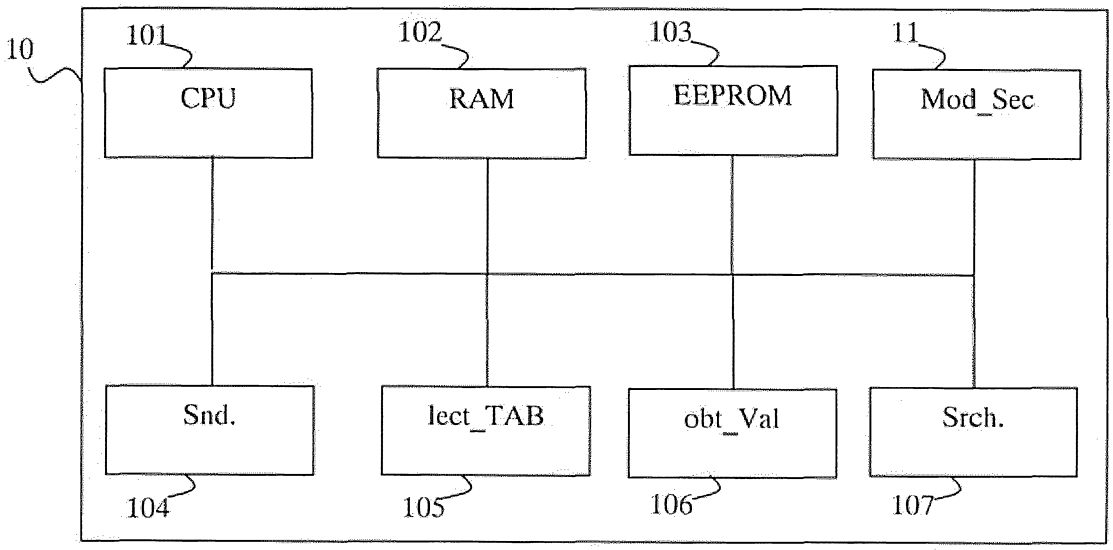


Figure 2

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 841319
FR 1755844

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		
Y	Olga Gadyatskaya ET AL: "Security-by-Contract for Open Multi-Application Smart Cards", e-Smart'2011, 23 septembre 2011 (2011-09-23), XP055419079, Extrait de l'Internet: URL:http://disi.unitn.it/~gadyatskaya/docs/eSmartGadyatskaya.pdf [extrait le 2017-10-25] * Slides 2-31 *	1-8	G06F21/44 G06F21/62 G06F21/57
Y	US 2013/067533 A1 (KADAM SUNIL SHANKAR [US] ET AL) 14 mars 2013 (2013-03-14) * alinéa [0003] - alinéa [0007] * * alinéa [0018] - alinéa [0071]; revendications 1-5; figures 1,2 *	1-8	
A	US 2009/202078 A1 (BAR-EL HAGAI [IL] ET AL) 13 août 2009 (2009-08-13) * alinéa [0011] - alinéa [0033]; figures 1,2 * * alinéa [0090] - alinéa [0095] *	1-8	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06F
A	BESSON FRÉDÉRIC ET AL: "SawjaCard: A Static Analysis Tool for Certifying Java Card Applications", 11 septembre 2014 (2014-09-11), NETWORK AND PARALLEL COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 51 - 67, XP047298912, ISSN: 0302-9743 ISBN: 978-3-642-27168-7 * page 51 - page 65 *	1-8	

Date d'achèvement de la recherche	Examinateur
25 octobre 2017	Ghani, Hamza

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 1755844 FA 841319

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 25-10-2017
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 2013067533 A1	14-03-2013	AUCUN	
US 2009202078 A1	13-08-2009	AUCUN	

EPO FORM P0465