(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
8 octobre 2015 (08.10.2015)

WIPO | PCT

(10) Numéro de publication internationale
WO 2015/150689 A1

(51) Classification internationale des brevets :
G06F 21/74 (2013.01) *G06F 21/57* (2013.01)

(21) Numéro de la demande internationale :
PCT/FR2015/050828

(22) Date de dépôt international :
31 mars 2015 (31.03.2015)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1452812 31 mars 2014 (31.03.2014) FR

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

(72) Inventeurs : **ARFAOUI, Ghada**; Orange/IMT/OLPS/ASE/SEC/NPS, 42 rue des Coutures, BP 6243, F-14000 Caen (FR). **GHAROUT, Saïd**; 167 rue d'Auge, F-14000 Caen (FR). **TRAORE, Jacques**; 23 avenue de la Suisse Normande, F-61100 Saint Georges des Groseillers (FR).

(74) Mandataire : **ORANGE/IPL**; RENARD Béatrice, 38-40 rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (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, 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, ST, SZ,

[Suite sur la page suivante]

(54) Title : METHOD FOR THE SECURE CONFIGURATION OF AN APPLICATION IN A USER TERMINAL

(54) Titre : PROCEDE DE CONFIGURATION SECURISEE D'UNE APPLICATION DANS UN TERMINAL UTILISATEUR

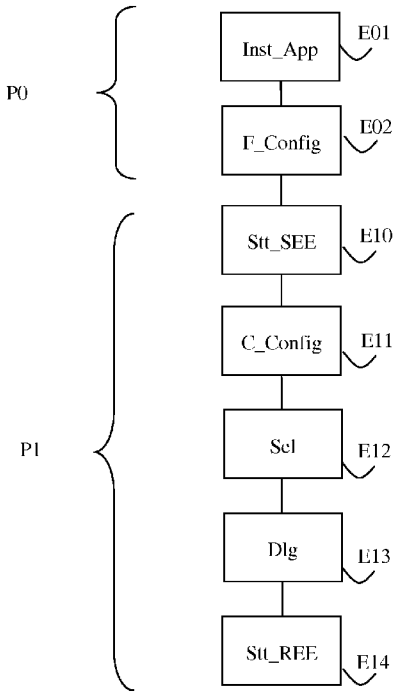

Figure 1

(57) Abstract : The invention concerns a method for the secure configuration of an application, said application being hosted in a mobile terminal (10), said terminal comprising a secure execution environment and a non-secure execution environment, separate from the secure execution environment, the execution of the application being launched in the non-secure execution environment, said method comprising the following steps, implemented by the terminal: executing (E10) a secure operating system establishing the secure execution environment, executing (E14) a non-secure operating system establishing the non-secure execution environment, characterised in that it further comprises: a step (E13) of secure dialogue with an entity, during which at least one item of configuration data of the application is requested from the entity, said dialogue step being executed in the secure execution environment, prior to the step of installing the non-secure operating system.

(57) Abrégé : L'invention concerne un procédé de configuration sécurisée d'une application, ladite application étant hébergée dans un terminal mobile (10), ledit terminal comprenant un environnement d'exécution sécurisée et un environnement d'exécution non sécurisée, distinct de l'environnement d'exécution sécurisée, le lancement de l'exécution de l'application s'effectuant dans l'environnement d'exécution

[Suite sur la page suivante]

WO 2015/150689 A1

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))*

non sécurisée, ledit procédé comprenant les étapes suivantes, mises en œuvre par le terminal: exécution (E10) d'un système d'exploitation sécurisé établissant l'environnement d'exécution sécurisée, exécution (E14) d'un système d'exploitation non sécurisé établissant l'environnement d'exécution non sécurisée, caractérisé en ce qu'il comprend en outre: une étape (E13) de dialogue sécurisé avec une entité, durant laquelle il est requis de l'entité au moins une donnée de configuration de l'application, ladite étape de dialogue s'exécutant dans l'environnement d'exécution sécurisée, préalablement à l'étape d'installation du système d'exploitation non sécurisé.

Procédé de configuration sécurisée d'une application dans un terminal utilisateur

La présente invention concerne un procédé de configuration sécurisée d'une application dans un terminal mobile.

Elle trouve une application particulièrement intéressante dans la sécurisation de services sensibles tels que des services de paiement sur des terminaux mobiles de type smartphone.

Un service sensible, tel qu'un service de paiement, installé sur un terminal d'abonné s'apparente à une dématérialisation de la carte bancaire de l'utilisateur. Un tel service nécessite, lors de l'exécution de celui-ci, des données de configuration propres à cet abonné, par exemple des coordonnées bancaires, un code d'identification personnelle de l'abonné, ou code « PIN » (de l'anglais « Personal Identification Number »). Des données qui définissent un mode d'utilisation du service peuvent également être prévues : montant en-dessous duquel il n'est pas nécessaire de ressaisir son code d'identification personnel pour valider une transaction, durée de fonctionnement de ce mode, etc.

Dans le cas de services sensibles sur terminaux mobiles tels que des services de paiement, on connaît les méthodes de configuration suivantes :

- un utilisateur qui s'abonne auprès de sa banque à une application de paiement, se voit fournir par celle-ci une application préconfigurée. L'application est associée à un compte bancaire de l'utilisateur et à un élément de sécurité du terminal mobile, par exemple une carte d'identité d'abonné ou une carte « microSD » (de l'anglais « micro Secure Digital Card »). L'application est préconfigurée dans le sens où des données de l'utilisateur sont renseignées dans l'application proposée par la banque en téléchargement : données du compte bancaire, code PIN qui pourra être modifié après installation, seuil de transaction au-dessous duquel aucun code PIN ne sera demandé à l'utilisateur, etc. Cependant, la modification ultérieure du code PIN par l'utilisateur, ou la saisie de celui-ci lors de la validation d'une transaction est sensible à des attaques, inhérentes à des vulnérabilités des systèmes d'exploitation de l'utilisateur. Par ailleurs, la configuration de l'application manque de souplesse : l'utilisateur ne peut pas modifier a posteriori des valeurs qui définissent le cadre d'utilisation du service : montant au-dessous duquel le code PIN ne sera pas demandé, etc. ;

- dans un deuxième exemple, l'application de paiement est téléchargée par l'utilisateur sur son terminal mobile puis complètement paramétrée par celui-ci. Lors de ce paramétrage, l'utilisateur fournit ses coordonnées bancaires, le montant maximal des transactions au-dessous duquel aucun code n'est demandé, le code PIN de validation, etc. Cependant une telle solution, bien que très souple en termes de paramétrage du point de vue de l'utilisateur présente des

failles de sécurité inhérentes à des vulnérabilités des systèmes d'exploitation des terminaux mobiles ;

- dans une troisième solution, l'application de paiement installée sur le terminal mobile est adaptée pour communiquer avec une carte bancaire de l'abonné, par exemple au moyen d'une communication en champ proche. L'utilisateur doit donc se munir de cette carte très spécifique et peu répandue actuellement. Dans ce cas, l'application, bien que sûre, est peu conviviale.

Ainsi, aucune des solutions existantes de configuration d'une application sensible sur terminal mobile, telle qu'une application de paiement, n'est réellement satisfaisante et n'allie convivialité et sécurité.

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 configuration sécurisée d'une application, ladite application étant hébergée dans un terminal mobile, ledit terminal comprenant un environnement d'exécution sécurisée et un environnement d'exécution non sécurisée, distinct de l'environnement d'exécution sécurisée, le lancement de l'exécution de l'application s'effectuant dans l'environnement d'exécution non sécurisée, ledit procédé comprenant les étapes suivantes, mises en œuvre par le terminal :

- exécution d'un système d'exploitation sécurisé établissant l'environnement d'exécution sécurisée,

- exécution d'un système d'exploitation non sécurisé établissant l'environnement d'exécution non sécurisée. Le procédé est caractérisé en ce qu'il comprend en outre :

- une étape de dialogue sécurisé avec une entité, durant laquelle il est requis de l'entité au moins une donnée de configuration de l'application, ladite étape de dialogue s'exécutant dans l'environnement d'exécution sécurisée, préalablement à l'étape d'installation du système d'exploitation non sécurisé.

Avec le procédé de l'invention, la configuration de l'application sensible est réalisée de manière sécurisée. Les données sensibles sont en effet fournies dans un environnement d'exécution sécurisée auquel l'environnement d'exécution non sécurisée ne peut accéder. En effet, celui-ci n'est pas encore établi lors de la fourniture des données de configuration. Lors du lancement ultérieur de l'exécution de l'application depuis l'environnement d'exécution non sécurisée, l'entité qui fournit les données de configuration n'a pas besoin de fournir les données sensibles qu'il a préalablement fournies. Les failles de sécurité inhérentes aux systèmes d'exploitation des terminaux mobiles de types smartphone ne peuvent donc être exploitées pour

récupérer ces données sensibles et pour les réutiliser de manière frauduleuse. Par ailleurs, dans le cadre d'une application de paiement, une telle configuration ne nécessite pas de carte bancaire spécifique et un dialogue entre l'application de paiement installée sur le terminal mobile et cette carte. Par ailleurs, la configuration de l'application sensible peut être modifiée lors d'un redémarrage du terminal mobile. Une telle configuration de l'application allie ainsi sécurité, souplesse et convivialité.

Dans un exemple de réalisation, le procédé comprend dans une phase préalable d'installation de l'application sur le terminal mobile, une étape d'enregistrement de l'application dans une liste d'applications configurables de l'environnement d'exécution sécurisée, ledit enregistrement étant destiné à détecter que la donnée de configuration est à demander à l'entité lors du démarrage de l'environnement d'exécution sécurisée.

L'application sensible est prise en compte par l'environnement d'exécution sécurisée au moment de l'installation de celle-ci. Ainsi, lors d'un redémarrage du terminal mobile, la configuration de l'application est mise en œuvre lors de l'exécution du système d'exploitation sécurisé, plus précisément lors de l'établissement de l'environnement d'exécution sécurisée et avant l'exécution du système d'exploitation non sécurisé et l'établissement de l'environnement d'exécution non sécurisée. Cela permet de garantir la sécurité de bout en bout : de l'installation de l'application, jusqu'à la configuration lors d'un redémarrage du terminal mobile.

De façon avantageuse, une temporisation étant armée lors de l'exécution de l'étape de dialogue, l'exécution du système d'exploitation non sécurisé est déclenchée lorsque la temporisation expire et qu'aucune donnée de configuration n'a été fournie par l'entité durant l'étape de dialogue.

L'utilisation d'une temporisation permet de ne pas interrompre le démarrage du terminal mobile dans un cas où aucune donnée de configuration de l'application sensible n'est fournie. Cela correspond par exemple à un cas où un utilisateur ne souhaite pas utiliser l'application sensible ; il n'a donc pas besoin de la configurer. Ainsi, la solution de configuration des applications sensibles est souple et nullement contraignante pour l'utilisateur.

Dans un exemple de réalisation, l'entité est un utilisateur du terminal mobile.

Dans cet exemple, c'est l'utilisateur qui configure l'application sensible dans l'environnement d'exécution sécurisée, avant l'exécution du système d'exploitation non sécurisé.

Dans un autre exemple de réalisation, l'entité est un élément de sécurité du terminal mobile.

Dans cet exemple de réalisation, les paramètres sensibles sont reçus d'un élément de sécurité qui constitue un environnement réputé sûr. Le dialogue entre l'élément de sécurité et

l'environnement sécurisé utilise des interfaces sécurisées. La sécurité est donc garantie. Cet exemple est intéressant dans un cas où l'utilisateur a défini et enregistré un/des profils d'utilisation de l'application et mémorisé ces profils dans l'élément de sécurité. Cette solution permet ainsi une configuration sécurisée et automatique, c'est-à-dire sans intervention de l'utilisateur. Cela limite les risques d'erreur par rapport à une saisie de données de configuration par l'utilisateur.

L'invention concerne également un terminal mobile adapté pour héberger une application nécessitant une configuration sécurisée, ledit terminal comprenant un environnement d'exécution sécurisée et un environnement d'exécution non sécurisée, distinct de l'environnement d'exécution sécurisée, le lancement de l'exécution de l'application s'effectuant depuis l'environnement d'exécution non sécurisée, ledit terminal comprenant :

- des moyens d'exécution d'un système d'exploitation non sécurisé établissant l'environnement d'exécution non sécurisée,
- des moyens d'exécution et de dialogue, agencés pour exécuter un système d'exploitation sécurisé établissant l'environnement d'exécution sécurisée, et pour dialoguer de manière sécurisée avec une entité afin de requérir de ladite entité au moins une donnée de configuration de l'application, le dialogue sécurisé étant établi dans l'environnement d'exécution sécurisée, préalablement à l'exécution du système d'exploitation non sécurisé.

L'invention porte également sur un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal mobile, le programme comprenant des instructions de code pour l'exécution des étapes du procédé de configuration sécurisée selon l'invention, lorsque le programme est exécuté sur ledit terminal mobile.

L'invention concerne aussi un support de données dans lequel est enregistré le programme selon l'invention.

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 du procédé de configuration sécurisée d'une application sensible dans un terminal mobile, selon un exemple de réalisation de l'invention ;
- la figure 2 est une représentation schématique d'un terminal mobile selon un exemple de réalisation de l'invention.

Les étapes d'un procédé de configuration sécurisée d'une application sensible dans un terminal utilisateur, selon un exemple de réalisation, vont maintenant être décrites en relation avec la figure 1.

Un terminal 10 d'utilisateur, par exemple un terminal mobile de type smartphone, est agencé pour héberger et exécuter des applications sensibles, par exemple des applications de paiement. Une application de paiement permet à l'utilisateur d'effectuer des transactions de paiement au moyen de son terminal mobile. L'application constitue en quelques sortes une dématérialisation de la carte bancaire de l'utilisateur dans son terminal mobile.

Selon l'exemple de réalisation décrit ici, l'architecture du terminal mobile 10 est conforme aux spécifications proposées par l'association GlobalPlatform. Ces spécifications définissent une architecture de terminal mobile où coexistent deux environnements d'exécution : un environnement d'exécution sécurisée, ou « TEE » (de l'anglais « Trusted Execution Environment ») et un environnement d'exécution non sécurisée, ou « REE » (de l'anglais « Rich Execution Environment »). L'environnement d'exécution sécurisée TEE est indépendant de l'environnement d'exécution non sécurisée REE. Il est destiné à offrir un environnement logiciel et matériel pour des applications sécurisées. Il est considéré de confiance et s'appuie sur ses propres ressources : un système d'exploitation sûr, des modules logiciels sûrs et des ressources matérielles sûres, comme des fonctions de sécurité telles qu'un stockage sûr, des interfaces de communication avec des composants de sécurité, etc. L'environnement d'exécution non sécurisée REE comprend des composants considérés comme publics, et de ce fait non sûrs. L'environnement d'exécution sécurisée TEE est agencé pour fournir des services de sécurité à l'environnement d'exécution non sécurisée REE au moyen d'interfaces prédéfinies (ou « API », de l'anglais « Application Programming Interface).

Dans une phase préalable P0 d'installation d'une application sensible, dans une étape E01 de téléchargement de l'application, l'utilisateur requiert auprès de sa banque l'installation d'une application de paiement destinée à mettre en œuvre des transactions de paiement au moyen de son terminal mobile 10. Cette installation se fait par exemple par téléchargement via le réseau Internet. Une transaction de paiement peut être mise en œuvre lors d'une communication en champ proche entre le terminal mobile et une borne de paiement d'un commerçant. La communication entre le terminal et la borne est par exemple une communication de type « NFC » (de l'anglais « Near Field Communication »).

L'application de paiement comprend une pluralité de modules logiciels mis à disposition de l'utilisateur par la banque lors du téléchargement et qui sont installés, selon leur niveau de sensibilité et selon une politique définie par la banque, dans une zone sécurisée du terminal mobile, c'est-à-dire une zone comprise dans l'environnement d'exécution sécurisée ou dans une zone non sécurisée, c'est-à-dire une zone comprise dans l'environnement d'exécution non sécurisée. Par exemple, un module relatif à la saisie et au traitement d'un code d'identification personnel (ou code « PIN », de l'anglais « Personal Identification Number ») propre à

l'utilisateur et à l'application de paiement, et destiné à authentifier l'utilisateur lors d'une transaction de paiement est installé dans une zone sécurisée du terminal 10. En particulier, le téléchargement de l'application comprend le téléchargement d'un module de configuration sécurisée, destiné à permettre à l'utilisateur de configurer de manière sécurisée l'application une fois celle-ci installée sur le terminal mobile. Ce module est sensible et installé dans une zone sécurisée du terminal mobile. Un module relatif à l'affichage d'options de l'application est installé dans une zone non sécurisée du terminal. Ainsi, certains modules logiciels de l'application bancaires, lors de ce téléchargement, sont installés dans l'environnement sécurisé du terminal 10 et d'autres, dans l'environnement non sécurisé. En tout état de cause, le déclenchement de l'exécution de l'application de paiement par l'utilisateur est réalisé à partir de l'environnement d'exécution non sécurisée du terminal mobile 10, par exemple en sélectionnant l'application de paiement parmi une liste d'applications disponibles sur le terminal 10. La procédure d'installation de l'application bancaire n'est pas détaillée ici. Elle est supposée connue et la sécurité de cette installation, c'est-à-dire de l'installation de certains modules logiciels sensibles, garantie par la banque.

Au terme de l'étape E01 d'installation, l'application bancaire est installée sur le terminal mobile 10 de l'utilisateur.

On suppose que l'application de paiement nécessite une configuration spécifique de l'utilisateur lors de l'exécution de celle-ci. Par exemple, et de manière classique, l'application, pour s'exécuter, a besoin que l'utilisateur ait fourni ses coordonnées bancaires, si celles-ci n'ont pas été fournies par la banque lors du téléchargement, qu'il fournisse un code PIN afin de valider les transactions, etc. Le code PIN peut être demandé pour valider chacune des transactions, ou n'être demandé que pour valider les transactions dont le montant excède un montant déterminé. Il est en effet habituel que pour de petits montants, inférieurs au montant déterminé, l'application soit configurée de manière à ce que le code PIN ne soit pas requis. Dans un exemple de réalisation, une configuration permet de définir un cadre d'utilisation temporaire de l'application bancaire. Ainsi, une telle configuration permet de définir un montant de transaction au-dessous duquel le code PIN ne sera pas demandé à l'utilisateur, une plage temporelle durant laquelle l'application bancaire fonctionne, d'activer ou de désactiver l'application bancaire, de définir un montant maximal pour toutes les transactions réalisées avec l'application, ou un montant maximal cumulé lors de l'exécution de transactions successives sur une période donnée, etc. On comprend qu'une telle configuration qui définit un cadre personnel d'utilisation de l'application est sensible. Afin que la saisie de paramètres de configuration du service se fasse en toute sécurité, le procédé prévoit une configuration sécurisée de l'application lors d'un (re)démarrage du terminal mobile.

Dans la phase préalable P0 d'installation, il est prévu dans une étape E02 de prise en compte de l'application sensible, de compléter une liste d'applications configurables de l'environnement d'exécution sécurisée TEE afin qu'il soit tenu compte de la présence de l'application sensible sur le terminal mobile 10 et qu'il soit offert à l'utilisateur la possibilité de configurer l'application de manière sécurisée. La liste est par exemple sous forme d'un fichier de données. Cette prise en compte de l'application de paiement dans cette liste d'applications configurables est destinée à requérir, lors d'un (re)démarrage du terminal, des paramètres de configuration auprès de l'utilisateur.

La gestion de la liste des applications configurables est assurée de manière sécurisée dans et par l'environnement d'exécution sécurisée. La sécurité de cette liste est donc garantie. On suppose que le terminal mobile 10 est mis hors tension à la fin de la phase P0 d'installation.

Dans une phase ultérieure P1 de démarrage du terminal, le terminal mobile 10 est mis sous tension par l'utilisateur.

Selon les spécifications GlobalPlatform, une séquence de démarrage d'un terminal mobile comprend deux phases successives : une phase de démarrage de l'environnement d'exécution sécurisée qui comprend l'exécution d'un système d'exploitation sécurisé destiné à établir ou mettre en place l'environnement d'exécution sécurisée sur le terminal mobile, puis une phase de démarrage de l'environnement d'exécution non sécurisée qui comprend l'exécution d'un système d'exploitation non sécurisé destiné à établir l'environnement d'exécution non sécurisée. Il est connu des spécifications GlobalPlatform que le système d'exploitation sécurisé est exécuté à partir d'un microprogramme approuvé (on parle de « firmware » en anglais) qui est authentifié et isolé du système d'exploitation non sécurisé durant le processus de démarrage (on parle de « boot » en anglais). Une fois le microprogramme authentifié, le système d'exploitation sécurisé est exécuté et l'environnement d'exécution sécurisée TEE est établi. Lors de cet établissement, l'environnement d'exécution sécurisée initialise le microprogramme, importe des données cryptographiques telles que des clés, des certificats, des signatures et importe un bout de code, appelé « loader », destiné à charger l'environnement d'exécution non sécurisée. L'environnement d'exécution sécurisée prépare ainsi le démarrage de l'environnement d'exécution non sécurisée. Au terme de l'établissement de l'environnement d'exécution sécurisée, le contrôle est transmis à l'environnement d'exécution non sécurisée. Le démarrage du terminal se poursuit alors avec une exécution du système d'exploitation non sécurisé et un établissement lors de cette exécution de l'environnement d'exécution non sécurisée. A noter que les environnements d'exécution sécurisée et non sécurisée sont établis séquentiellement durant la séquence de démarrage d'un terminal mobile.

Ainsi, pendant la phase de démarrage P1, dans une étape initiale E10 d'exécution du système d'exploitation sécurisé, et conformément aux spécifications GlobalPlatform, il y a exécution du système d'exploitation sécurisé et établissement de l'environnement d'exécution sécurisée. En fin d'établissement de l'environnement d'exécution sécurisée, dans une étape E11 de consultation, l'environnement d'exécution sécurisée consulte la liste des applications configurables stockée de manière sécurisée dans l'environnement d'exécution sécurisée. Les applications configurables sont celles qui ont été installées durant la phase P0 d'installation et qui sont susceptibles d'être configurées par l'utilisateur. Cette étape E11 de consultation fait partie de la phase de démarrage de l'environnement d'exécution sécurisée et est mise en œuvre par l'environnement d'exécution sécurisée. Ainsi, on considère que cette étape est exécutée de manière sécurisée.

La liste des applications configurables comprend au moins l'application de paiement installée précédemment.

Dans une étape E12 de sélection, il est demandé à l'utilisateur, via une interface utilisateur adaptée de sélectionner une application à configurer. L'utilisateur sélectionne par exemple l'application de paiement installée précédemment. Cette sélection déclenche l'exécution du module de configuration sécurisée dans l'environnement d'exécution sécurisée.

Dans une étape E13 de dialogue, il est demandé à l'utilisateur de fournir des paramètres de configuration de l'application de paiement. Différents paramètres de configuration peuvent ainsi être demandés. Par exemple, il est demandé à l'utilisateur de saisir ses coordonnées bancaires si celles-ci n'ont pas été fournies par la banque lors du téléchargement de l'application, le code d'identification PIN de service destiné à valider des transactions si celui-ci n'a pas été renseigné lors du téléchargement de l'application, le code PIN de validation pour des transactions d'un montant inférieur à un montant déterminé par l'utilisateur. Bien sûr, l'invention n'est pas limitée à ces types de paramètre. L'utilisateur peut par exemple définir également des plages temporelles d'utilisation de l'application de paiement, un montant maximal par transaction, un montant cumulé maximal pour un ensemble de transactions effectué pendant un période donnée, etc. Ce dialogue est établi dans l'environnement d'exécution sécurisée et avant la phase de démarrage de l'environnement d'exécution non sécurisée, c'est-à-dire avant que celui-ci ne soit établi. Ainsi, les failles de sécurité inhérentes aux systèmes d'exploitation non sécurisés des terminaux mobiles ne peuvent être exploitées afin notamment de récupérer des données sensibles de l'application bancaires fournies par l'utilisateur. Par ailleurs, l'utilisateur peut éventuellement fournir de nouveaux paramètres de configuration lors d'un redémarrage ultérieur du terminal mobile. La configuration est donc plus

souple qu'avec des solutions connues pour lesquelles la configuration est fournie par la banque et est donc figée jusqu'à la fourniture par la banque d'une nouvelle configuration.

Une fois un ou des paramètres de configuration saisi(s) par l'utilisateur, le processus de démarrage du terminal 10 se poursuit. La phase de démarrage de l'environnement d'exécution sécurisée se termine et le contrôle est transmis à l'environnement d'exécution non sécurisée.

Dans une étape suivante E14 d'exécution du système d'exploitation non sécurisé, il y a exécution du système d'exploitation non sécurisé et établissement de l'environnement d'exécution non sécurisée.

Au terme de cette étape E14, le terminal mobile 10 est démarré. En particulier l'utilisateur peut sélectionner et exécuter l'application bancaire. Lors de la mise en œuvre d'une transaction de paiement, les paramètres saisis lors de l'étape E13 de dialogue sont pris en compte. Par exemple, dans le cas où l'utilisateur a précisé un montant en-dessous duquel il ne souhaitait pas que lui soit demandé son code PIN pour valider les transactions, alors toute transaction d'un montant inférieur sera exécutée sans que l'utilisateur n'ait à saisir le code PIN de validation.

Dans l'exemple de réalisation décrit ici, le démarrage du terminal mobile est interrompu de manière à ce que l'utilisateur saisisse les paramètres de configuration de l'application bancaire. Dans un autre exemple de réalisation, une temporisation est armée durant l'étape E12 de sélection, c'est-à-dire à l'interruption du processus de démarrage de l'environnement sécurisé. Si l'utilisateur ne saisit aucune donnée de configuration durant cette étape alors le démarrage du terminal reprend à l'expiration de la temporisation. Dans ce cas, il y a exécution du système d'exploitation non sécurisé et établissement de l'environnement d'exécution non sécurisée sans paramétrage de l'application de paiement. Ainsi, la configuration sécurisée décrite ci-dessus n'est pas bloquante et n'empêche pas le démarrage du terminal mobile. Lorsque l'utilisateur n'a pas configuré l'application mais lance l'exécution de l'application, celle-ci peut s'exécuter de manière classique, avec une configuration minimale par défaut : par exemple le code PIN de l'utilisateur peut être demandé pour valider chaque transaction. Dans ce cas cependant, la sécurité est moindre et une personne malintentionnée peut exploiter des failles connues des systèmes d'exploitation des terminaux mobiles afin de récupérer cette donnée sensible.

Avec le procédé de configuration décrit ici, le paramétrage de l'application bancaire est fait indépendamment du type de la carte bancaire utilisée. Il ne nécessite donc pas de carte bancaire spécifique.

Dans l'exemple de réalisation décrit précédemment, c'est l'utilisateur qui fournit les valeurs nécessaires à la configuration de l'application sensible. Dans un autre exemple de

réalisation, la configuration de l'application sensible est faite par l'intermédiaire d'un élément de sécurité. Le module de sécurité est par exemple une carte d'identité d'abonné, ou carte « SIM » (pour « Subscriber Identity Module »), agencée pour permettre au terminal mobile d'accéder à un réseau mobile de communications. L'invention n'est pas limitée à un module de sécurité de type carte SIM. Ainsi, le module de sécurité peut également être une carte « (e)-UICC » (pour « (embedded)-Universal Integrated Circuit Card »), ou une zone mémoire sécurisée du dispositif mobile tel un composant TEE embarqué dans le processeur, un élément de sécurité embarqué (ou « embedded secure element »), ou un composant amovible de type microSD.

Dans cet exemple de réalisation, l'étape de sélection E12 est transparente pour l'utilisateur ; il y a par exemple sélection automatique d'une ou de plusieurs applications qui figurent dans la liste des applications configurables.

Dans cet exemple, un profil de configuration est mémorisé dans l'élément de sécurité. Le profil de configuration comprend un ensemble de paramètres de configuration de l'application bancaire. Ce profil est transmis de l'élément de sécurité à l'environnement d'exécution sécurisée au cours de l'étape E13 de dialogue et permet de configurer l'application bancaire. Par exemple, le profil de configuration a été préalablement défini par la banque, en présence et l'utilisateur et avec l'accord de celui-ci. Il a ensuite été transmis à l'élément de sécurité. Dans le cas où l'élément de sécurité est une carte SIM ou une carte (e)-UICC, le profil est transmis à celui-ci par exemple au moyen d'une procédure « OTA » (de l'anglais « Over The Air »). Ce type de procédure est connu et n'est pas détaillé ici. La communication entre l'élément de sécurité et l'environnement d'exécution sécurisé repose sur des interfaces sécurisées définies dans les spécifications GlobalPlatform. Cette communication est donc réputée de confiance.

Un terminal mobile 10, selon un exemple de réalisation, va maintenant être décrit en relation avec la figure 2.

Le terminal mobile 10 est conforme aux spécifications GlobalPlatform. Il comprend ainsi un environnement d'exécution sécurisée 101 et un environnement d'exécution non sécurisée 102. Chacun de ces environnements 101, 102, comprend des ressources qui lui sont propres :

- une unité de traitement, ou « CPU » pour « Central Processing Unit » 101-1, 101-2,

- un ensemble de mémoires, dont une mémoire volatile 101-2, 102-2 et une mémoire de stockage 101-3, 102-3. La mémoire volatile 101-2, 102-2 est agencée pour exécuter des instructions de code, stocker des variables, etc., La mémoire de stockage 101-2, 102-2 est

agencée pour mémoriser des données. Par exemple, la mémoire de stockage 101-2 de l'environnement d'exécution sécurisée, est agencée pour mémoriser des données de sécurité telles que des clés, des certificats, des signatures, etc., ainsi qu'un programme sécurisé (on parle de « trustlet » en anglais) comprenant des instructions de code destinées à mettre en œuvre les étapes du procédé de configuration décrit précédemment.

Le terminal mobile 10 comprend également :

- des moyens d'exécution 102-4, agencés pour exécuter un système d'exploitation non sécurisé adapté pour établir l'environnement d'exécution non sécurisée. Les moyens d'exécution 102-4 sont adaptés pour mettre en œuvre l'étape E14 du procédé de configuration décrit précédemment,

- des moyens 101-4 d'exécution et de dialogue, agencés pour exécuter un système d'exploitation sécurisé établissant l'environnement d'exécution sécurisée, et pour dialoguer de manière sécurisée avec une entité afin de requérir de ladite entité au moins une donnée de configuration de l'application, le dialogue sécurisé est établi dans l'environnement d'exécution sécurisée, préalablement à l'exécution du système d'exploitation non sécurisé. Le dialogue avec l'entité utilise une interface dédiée (non représentée). Dans un cas où l'entité est un utilisateur, l'interface est par exemple un écran. Dans un cas où l'entité est un élément de sécurité, une interface de programmation qui définit les échanges entre l'environnement d'exécution sécurisée 101 et l'élément de sécurité et définie dans le cadre des spécifications GlobalPlatform est utilisée. Les moyens 101-4 d'exécution et de dialogue sont agencés pour mettre en œuvre les étapes E10, E11, E12 et E13 du procédé de configuration sécurisée décrit précédemment.

Les moyens d'exécution 102-4 et les moyens 101-4 d'exécution et de dialogue comprennent des modules logiciels comprenant des instructions de code pour faire exécuter les étapes du procédé de configuration sécurisée tel que décrit précédemment. Les modules logiciels peuvent être stockés dans, ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un CD-ROM, une disquette magnétique ou un disque dur, ou bien un support de transmission, ou un réseau.

REVENDICATIONS

1. Procédé de configuration sécurisée d'une application, ladite application étant hébergée dans un terminal mobile (10), ledit terminal comprenant un environnement d'exécution sécurisée et un environnement d'exécution non sécurisée, distinct de l'environnement d'exécution sécurisée, le lancement de l'exécution de l'application s'effectuant dans l'environnement d'exécution non sécurisée, ledit procédé comprenant les étapes suivantes, mises en œuvre par le terminal :

- exécution (E10) d'un système d'exploitation sécurisé établissant l'environnement d'exécution sécurisée,

- exécution (E14) d'un système d'exploitation non sécurisé établissant l'environnement d'exécution non sécurisée,

caractérisé en ce qu'il comprend en outre :

- une étape (E13) de dialogue sécurisé avec une entité, durant laquelle il est requis de l'entité au moins une donnée de configuration de l'application, ladite étape de dialogue s'exécutant dans l'environnement d'exécution sécurisée, préalablement à l'étape d'installation du système d'exploitation non sécurisé.

2. Procédé de configuration selon la revendication 1, comprenant, dans une phase préalable d'installation (P0) de l'application sur le terminal mobile, une étape (E02) d'enregistrement de l'application dans une liste d'applications configurables de l'environnement d'exécution sécurisée, ledit enregistrement étant destiné à détecter que la donnée de configuration est à demander à l'entité lors du démarrage de l'environnement d'exécution sécurisée.

3. Procédé selon l'une des revendications précédentes, dans lequel, une temporisation étant armée lors de l'exécution de l'étape de dialogue, l'exécution du système d'exploitation non sécurisé est déclenchée lorsque la temporisation expire et qu'aucune donnée de configuration n'a été fournie par l'entité durant l'étape de dialogue.

4. Procédé selon l'une des revendications précédentes, dans lequel l'entité est un utilisateur du terminal mobile.

5. Procédé selon l'une des revendications 1 à 3, dans lequel l'entité est un élément de sécurité du terminal mobile.

6. Terminal mobile (10) adapté pour héberger une application nécessitant une configuration sécurisée, ledit terminal comprenant un environnement d'exécution sécurisée et un environnement d'exécution non sécurisée, distinct de l'environnement d'exécution sécurisée, le lancement de l'exécution de l'application s'effectuant depuis l'environnement d'exécution non sécurisée, ledit terminal comprenant :

- des moyens (102-4) d'exécution d'un système d'exploitation non sécurisé établissant l'environnement d'exécution non sécurisée,

- des moyens (101-4) d'exécution et de dialogue, agencés pour exécuter un système d'exploitation sécurisé établissant l'environnement d'exécution sécurisée, et pour dialoguer de manière sécurisée avec une entité afin de requérir de ladite entité au moins une donnée de configuration de l'application, le dialogue sécurisé étant établi dans l'environnement d'exécution sécurisée, préalablement à l'exécution du système d'exploitation non sécurisé.

7. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal mobile, le programme comprenant des instructions de code pour l'exécution des étapes du procédé de configuration sécurisée 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.

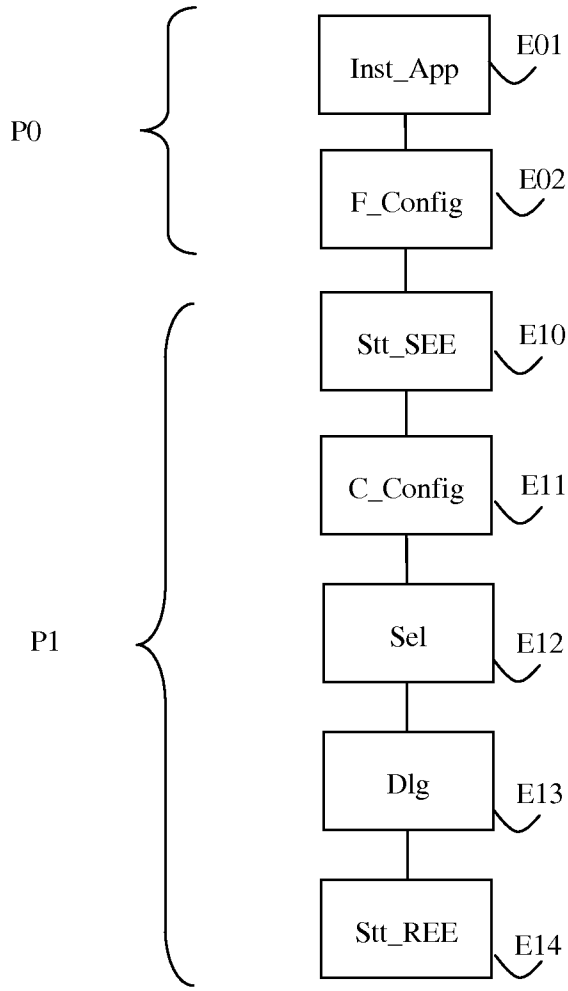

Figure 1

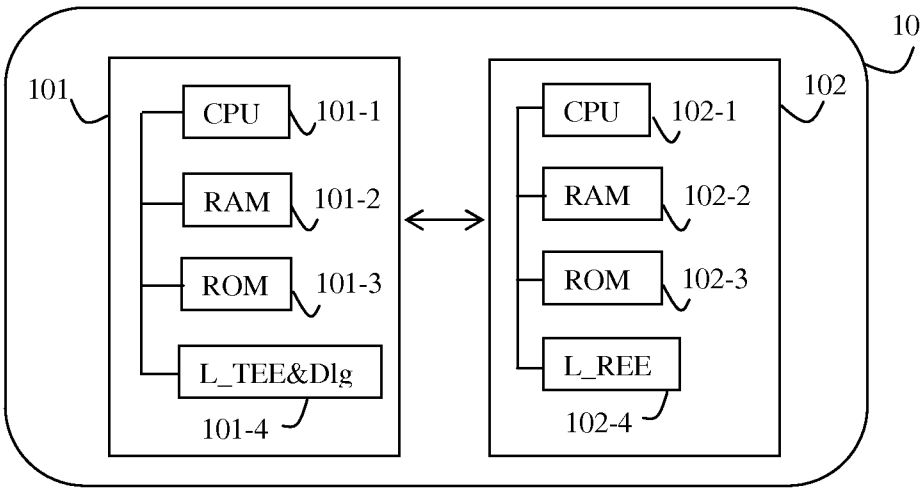

Figure 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/050828

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/74 G06F21/57
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)
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	US 2009/254986 A1 (HARRIS PETER WILLIAM [GB] ET AL) 8 October 2009 (2009-10-08)	1,4,6
Y	paragraph [0006] - paragraphs [0010], [0016], [0024] paragraph [0046] - paragraphs [0050], [0057]; figures 2B, 2C, 5A, 5B	2,3,5,7, 8
X	WO 2013/050154 A1 (GIESECKE & DEVRIENT GMBH [DE]) 11 April 2013 (2013-04-11)	1,6
Y	page 1 - pages 5, 7	2,3,7,8
X	WO 2011/085960 A1 (GIESECKE & DEVRIENT GMBH [DE]; SPITZ STEPHAN [DE]; STERZINGER HERMANN) 21 July 2011 (2011-07-21)	1,6
Y	pages 1, 9 - page 12	2,3

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
5 June 2015	12/06/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ghani, Hamza

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/050828

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/007120 A1 (SPITZ STEPHAN [DE]) 2 January 2014 (2014-01-02) paragraph [0006] - paragraphs [0010], [0029] -----	2,3,5,7, 8
A	NUNO SANTOS ET AL: "Using ARM trustzone to build a trusted language runtime for mobile applications", ARCHITECTURAL SUPPORT FOR PROGRAMMING LANGUAGES AND OPERATING SYSTEMS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 24 February 2014 (2014-02-24), pages 67-80, XP058044535, DOI: 10.1145/2541940.2541949 ISBN: 978-1-4503-2305-5 the whole document -----	1-8

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2015/050828

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009254986 A1	08-10-2009	GB 2459097 A	14-10-2009
		US 2009254986 A1	08-10-2009
WO 2013050154 A1	11-04-2013	CN 103858131 A	11-06-2014
		DE 102011115135 A1	11-04-2013
		EP 2764464 A1	13-08-2014
		JP 2014533395 A	11-12-2014
		KR 20140074296 A	17-06-2014
		US 2014237621 A1	21-08-2014
		WO 2013050154 A1	11-04-2013
WO 2011085960 A1	21-07-2011	DE 102010004446 A1	14-07-2011
		EP 2524333 A1	21-11-2012
		WO 2011085960 A1	21-07-2011
US 2014007120 A1	02-01-2014	CN 103477343 A	25-12-2013
		DE 102011012226 A1	30-08-2012
		EP 2663946 A2	20-11-2013
		KR 20140027110 A	06-03-2014
		US 2014007120 A1	02-01-2014
		WO 2012113547 A2	30-08-2012

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/050828

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/74 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	US 2009/254986 A1 (HARRIS PETER WILLIAM [GB] ET AL) 8 octobre 2009 (2009-10-08)	1,4,6
Y	alinéa [0006] - alinéas [0010], [0016], [0024] alinéa [0046] - alinéas [0050], [0057]; figures 2B, 2C, 5A, 5B	2,3,5,7, 8

X	WO 2013/050154 A1 (GIESECKE & DEVRIENT GMBH [DE]) 11 avril 2013 (2013-04-11)	1,6
Y	page 1 - pages 5, 7	2,3,7,8

X	WO 2011/085960 A1 (GIESECKE & DEVRIENT GMBH [DE]; SPITZ STEPHAN [DE]; STERZINGER HERMANN) 21 juillet 2011 (2011-07-21)	1,6
Y	pages 1, 9 - page 12	2,3

	-/--	

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

[X] 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
5 juin 2015	12/06/2015

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	Ghani, Hamza

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 2014/007120 A1 (SPITZ STEPHAN [DE]) 2 janvier 2014 (2014-01-02) alinéa [0006] - alinéas [0010], [0029] -----	2,3,5,7, 8
A	NUNO SANTOS ET AL: "Using ARM trustzone to build a trusted language runtime for mobile applications", ARCHITECTURAL SUPPORT FOR PROGRAMMING LANGUAGES AND OPERATING SYSTEMS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 24 février 2014 (2014-02-24), pages 67-80, XP058044535, DOI: 10.1145/2541940.2541949 ISBN: 978-1-4503-2305-5 le document en entier -----	1-8

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2015/050828

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009254986 A1	08-10-2009	GB 2459097 A	14-10-2009
		US 2009254986 A1	08-10-2009
WO 2013050154 A1	11-04-2013	CN 103858131 A	11-06-2014
		DE 102011115135 A1	11-04-2013
		EP 2764464 A1	13-08-2014
		JP 2014533395 A	11-12-2014
		KR 20140074296 A	17-06-2014
		US 2014237621 A1	21-08-2014
		WO 2013050154 A1	11-04-2013
WO 2011085960 A1	21-07-2011	DE 102010004446 A1	14-07-2011
		EP 2524333 A1	21-11-2012
		WO 2011085960 A1	21-07-2011
US 2014007120 A1	02-01-2014	CN 103477343 A	25-12-2013
		DE 102011012226 A1	30-08-2012
		EP 2663946 A2	20-11-2013
		KR 20140027110 A	06-03-2014
		US 2014007120 A1	02-01-2014
		WO 2012113547 A2	30-08-2012