

(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
3 mars 2011 (03.03.2011)

PCT

(10) Numéro de publication internationale
WO 2011/023554 A1

- (51) Classification internationale des brevets :
H04L 29/06 (2006.01) H04W 12/06 (2009.01)
- (21) Numéro de la demande internationale :
PCT/EP2010/061704
- (22) Date de dépôt international :
11 août 2010 (11.08.2010)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
09305789.1 26 août 2009 (26.08.2009) EP
- (71) Déposant (pour tous les États désignés sauf US) :
GEMALTO SA [FR/FR]; 6 rue de la Verrerie, F-92190 Meudon (FR).
- (72) Inventeur; et
- (75) Inventeur/Déposant (pour US seulement) :
GUICHARD, Olivier [FR/FR]; Les Jardins de St Marcel - n° 8, 46 rue Courenq, F-13001 Marseille (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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— relative à la qualité d'inventeur (règle 4.17.iv))

Publiée :

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

(54) Title : MOBILE ELECTRONIC DEVICE CONFIGURED TO ESTABLISH SECURE WIRELESS COMMUNICATION

(54) Titre : DISPOSITIF ÉLECTRONIQUE NOMADE CONFIGURÉ POUR ÉTABLIR UNE COMMUNICATION SANS FIL SÉCURISÉ

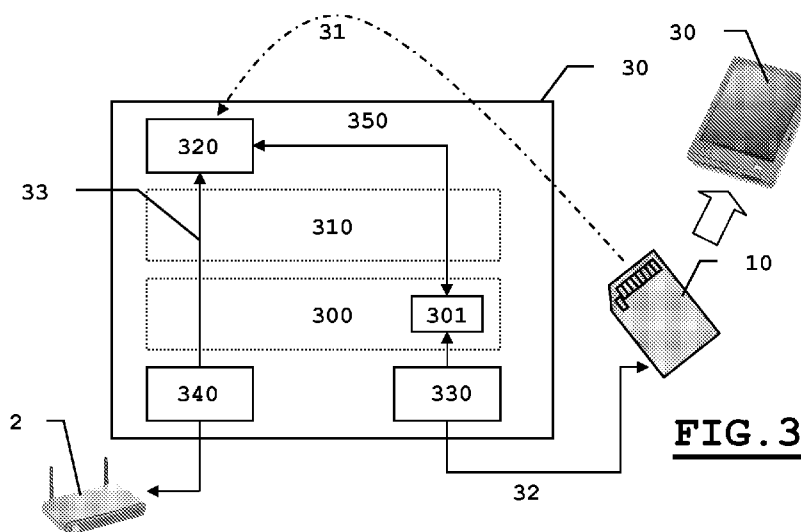


FIG. 3

(57) Abstract : The invention relates to method for configuring a mobile device capable of reproducing, for a user, multimedia content previously provided by a remote content server. The invention relates to using a client installed on said electronic device to relay authentication requests between a card, preferably complying with the provision of the Mobile Commerce Extension standard, and an authentication server that is accessible via an access point.

(57) Abrégé : L'invention concerne un procédé de configuration d'un dispositif nomade apte à restituer à un utilisateur un contenu multimédia préalablement délivré par un serveur de contenus distant. L'invention prévoit l'utilisation

[Suite sur la page suivante]

WO 2011/023554 A1

Dispositif électronique nomade configuré pour établir
une communication sans fil sécurisé

L'invention concerne des dispositifs électroniques communiquant avec le monde extérieur principalement à l'aide de protocoles de communication sans contact. Plus précisément, l'invention concerne des baladeurs vidéo,
5 des tablettes internet multimédia ou plus généralement tous dispositifs électroniques nomades qui accèdent à un contenu multimédia délivré depuis un serveur de contenus distant.

De nouveaux modèles économiques se développent comme
10 par exemple le modèle dit « pay per view ». Selon un tel modèle, un client peut télécharger et/ou visionner un contenu multimédia contre un paiement. Afin de prévenir tout accès non autorisé au dit contenu, le visionnage et/ou le chargement d'un contenu multimédia requiert dès
15 lors une protection de la communication entre un dispositif de visionnage et un serveur de contenus ou une protection directe du contenu. On parle alors de contenu multimédia protégé.

Pour répondre à cette exigence de protection,
20 certains dispositifs nomades disposent de moyens intégrés pour mettre en œuvre un protocole de communication sécurisé sous la forme d'une authentification unilatérale ou mutuelle vis-à-vis de serveurs de contenus.

En variante, des contenus sont préalablement chiffrés
25 et leur chargement et/ou leur visionnage exige(nt) un déchiffrement. On entend par visionnage d'un contenu protégé, le rendu sonore et/ou visuel dudit contenu, ainsi qu'une éventuelle fonction de déchiffrement pouvant être réalisée « à la volée ». Cette fonction de
30 déchiffrement peut être un préalable au dit rendu dans le cadre d'un contenu délivré sous la forme d'un flux vidéo par exemple. Les moyens intégrés de dispositifs nomades

offrant de telles fonctions, assurent ainsi un déchiffrement, lors du stockage d'un contenu délivré chiffré, ou un déchiffrement « à la volée » d'un contenu délivré sous la forme d'un flux vidéo chiffré par exemple. La mise en œuvre de tels traitements s'appuie généralement sur la manipulation de secrets qui peuvent prendre la forme de clés cryptographiques. Ces clés sont préférentiellement obtenues auprès d'un tiers, par exemple un fournisseur de contenus, dans le cadre d'un engagement contractuel établi entre un client et ledit fournisseur. Cet engagement contractuel peut par exemple découler d'un achat ou d'une souscription d'abonnement effectués par un client auprès d'un fournisseur de contenus.

La gestion, le chargement, la révocation desdits secrets sont complexes. Ils nécessitent en outre que les moyens intégrés soient résistants aux principales attaques connues, dans le but d'interdire à des personnes non autorisées, voire malveillantes, d'obtenir des informations relatives aux secrets et d'en faire un usage ou un commerce frauduleux.

Pour répondre à cette condition une première solution consiste à doter un dispositif nomade de moyens intégrés dits TRM pour « *Tamper Resistant Means* » en langue anglaise, signifiant qu'ils sont résistants aux attaques connues. De tels moyens se présentent le plus souvent sous la forme d'une carte à puce insérée dans un dispositif nomade, ou d'un microcontrôleur utilisé dans le monde des cartes à puce, directement intégré dans le dispositif nomade.

On peut trouver ainsi des téléphones mobiles permettant un accès à des contenus multimédia protégés. Les fonctions d'authentification voire de déchiffrement sont assurées par une carte d'identification d'abonné, SIM (*Subscriber Identity Module*) ou USIM (*Universal*

Subscriber Identity Module) présente dans ledit téléphone mobile.

A titre d'exemple, les architectures et protocoles EAP-SIM ou EAP-AKA (*Extensible Application Protocol*)
5 permettent aujourd'hui l'accès à des contenus protégés. Sous l'égide d'un accord entre un opérateur de téléphonie mobile et un fournisseur de contenus protégés, la gestion des secrets propres au dit fournisseur peut être classiquement mise en œuvre au moyen de protocoles
10 sécurisés de type OTA pour *Over The Air*, connus des opérateurs.

On peut trouver en variante des dispositifs nomades qui n'offrent pas la fonction de téléphonie mobile mais qui hébergent des moyens internes résistants, stockant et
15 manipulant les secrets nécessaires. Dans ce cas, la gestion de l'élaboration, de la répartition et de la révocation des secrets incombe aux fournisseurs de contenus. Ces derniers sont souvent contraints à établir des accords avec des fabricants de dispositifs nomades
20 afin que lesdits fabricants puissent initialiser des secrets avant de mettre sur le marché de tels dispositifs nomades. Ainsi, un dispositif nomade doit être par exemple personnalisé par un fabricant pour chaque client ayant souscrit un abonnement auprès d'un fournisseur de
25 contenus. Cette gestion peut devenir rapidement pénalisante, voire contraignante, et nuire au développement du commerce de tels dispositifs nomades ainsi qu'au développement de l'offre de fournisseurs de contenus protégés.

30

Pour pouvoir plus librement exploiter un contenu protégé nécessitant un déchiffrement lors de son téléchargement, une deuxième solution peut consister tout
d'abord à utiliser un premier dispositif tel que
35 précédemment décrit, par exemple un ordinateur personnel couplé à une carte à puce ou encore un téléphone mobile. Ce dernier permet de réaliser les opérations de

téléchargement depuis un serveur de contenus protégés et de déchiffrement. Selon cette deuxième solution, le contenu protégé ainsi déchiffré et chargé peut être transféré depuis le premier dispositif vers un second
5 dispositif nomade offrant des capacités de rendus particulièrement adaptées à son utilisateur ou au dit contenu. Toutefois la majorité de ce type de second dispositif ne disposent pas de moyens internes résistants aux attaques connues, moyens pour permettre un accès, un
10 chargement ou un visionnage de contenus protégés. Cette deuxième solution peut éventuellement présenter un certain avantage pour un utilisateur mais elle se révèle à la fois fastidieuse pour ce dernier et surtout peu sûre pour un fournisseur de contenus. En effet, il devient
15 aisé de distribuer le contenu ainsi déchiffré au plus grand nombre par un client indélicat.

Une troisième solution consiste à télécharger les secrets nécessaires à l'accès, au visionnage d'un contenu protégé depuis un fournisseur de contenus vers un
20 dispositif nomade, tel qu'un ordinateur personnel, ne disposant pas de fonction de téléphonie mobile ni de moyens internes résistants pour exploiter lesdits secrets. Le niveau de sécurité induit par cette troisième
25 solution est très faible et le risque est grand pour un fournisseur de contenus de constater que des secrets ont été divulgués ou transmis par un client indélicat ou même piratés par un tiers malveillant.

30 L'invention vise à résoudre les inconvénients cités de manière à offrir une solution robuste, efficace et économique permettant de configurer, y compris après sa mise sur le marché, un dispositif nomade ne disposant pas
obligatoirement d'une fonction de téléphonie mobile, pour
35 que ce dispositif puisse offrir un accès, un chargement ou un visionnage de contenus multimédia protégés tout en préservant la confidentialité des secrets nécessaires aux

5 dits accès, chargement et/ou visionnage. L'invention permet notamment à un fabricant de produire de tels dispositifs nomades à l'identique et supprime la nécessité d'établir un accord commercial auprès d'un ou plusieurs fournisseurs de contenus pour personnaliser chaque dispositif.

10 A cette fin, il est prévu un dispositif nomade apte à restituer à un utilisateur un contenu multimédia préalablement délivré par un serveur de contenus distant, comportant :

15 - des moyens pour recevoir et gérer une carte de mémoire de masse comportant des moyens internes résistants aux attaques connues pour réaliser des calculs cryptographiques ;

- des moyens pour communiquer avec un point d'accès à un réseau de communication sans fil ;

20 Ledit dispositif comportant en outre un client pour relayer des requêtes d'authentification entre la carte et un serveur d'authentification accessible via le point d'accès.

25 L'invention prévoit en outre un procédé pour configurer un tel dispositif nomade comportant une étape de chargement dans une mémoire dudit dispositif d'un client pour relayer des requêtes d'authentification entre une carte de mémoire de masse comportant des moyens internes résistants aux attaques connues pour réaliser des calculs cryptographiques et un serveur d'authentification accessible via un point d'accès.

30 Selon un premier mode de réalisation, l'étape de chargement peut être réalisée automatiquement à l'insertion de la carte par le dispositif nomade, le client étant déchargé depuis une mémoire de masse de la carte.

35 En variante, l'étape de chargement peut être réalisée par l'utilisateur du dispositif après l'insertion de la carte dans ledit dispositif nomade, au moyen d'une

interface homme-machine offerte par le dispositif. Le client peut ainsi être déchargé depuis une mémoire de masse de la carte.

5 L'invention prévoit que le procédé puisse comporter en outre une étape préalable de chargement dans la mémoire du dispositif de moyens pour communiquer avec lesdits moyens internes résistants aux attaques connues de la dite carte si lesdits moyens pour communiquer sont absents dans le dispositif nomade.

10 Selon cette variante de réalisation de l'invention, l'étape de chargement préalable peut être réalisée automatiquement par le dispositif nomade à l'insertion de la carte ou par un utilisateur du dispositif nomade au moyen d'une interface homme-machine du dispositif, les
15 moyens pour communiquer étant déchargés depuis une mémoire de masse de la carte.

L'invention prévoit également l'utilisation d'une carte de mémoire de masse comportant des moyens internes
20 résistants aux attaques connues pour réaliser des calculs cryptographiques, des moyens de stockage, des moyens pour contrôler l'accès aux dits moyens de stockage et aux moyens internes résistants. Lesdits moyens de stockage comportent un client prévu pour être déchargé depuis les
25 moyens de stockage dans une mémoire d'un dispositif nomade pour relayer des requêtes d'authentification entre la carte et un serveur d'authentification accessible via un point d'accès. Les moyens internes résistants stockent et/ou génèrent des secrets et/ou mettent en œuvre des
30 calculs cryptographiques nécessaires à la complétude des requêtes d'authentification relayées au moyen dudit client après installation de celui-ci au sein du dispositif nomade.

Préférentiellement l'invention prévoit que la carte
35 de mémoire de masse soit conforme aux dispositions de la norme « *Mobile Commerce Extension* » établie par l'organisme « *SD Card Association* ».

D'autres caractéristiques et avantages apparaîtront plus clairement à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent parmi
5 lesquelles :

- la figure 1 présente une architecture permettant l'accès à un contenu protégé depuis un dispositif nomade de type tablette internet multimédia incluant des moyens internes résistants;
- 10 - la figure 2 décrit un objet électronique conforme aux dispositions de la norme « Mobile Commerce Extension » ;
- la figure 3 présente un mode de réalisation conforme à l'invention.

15

En liaison avec la figure 1, un dispositif nomade 1, du type tablette internet multimédia, est apte à établir une communication avec un serveur 6 de contenus multimédia distant. Le dispositif 1 permet le visionnage
20 d'un contenu délivré sous la forme par exemple d'un flux vidéo. Le dispositif 1 intègre des moyens internes la résistants aux attaques connues, symbolisés sur la figure 1 sous la forme d'une carte à puce de type SIM (*Subscriber Identity Module*) ou USIM (*Universal, Subscriber Identity Module*) que l'on retrouve couramment
25 dans un téléphone mobile. Les moyens la pourraient tout aussi bien se présenter sous la forme d'un composant électronique non extractible et directement connecté aux composants électroniques du dispositif 1. Les moyens la réalisent des calculs de chiffrement et/ou de
30 déchiffrement à l'aide de secrets dérivés ou partagés entre un fournisseur de contenus et le dispositif 1. Préalablement à tout échange de secret, il est connu de mettre en œuvre un protocole d'authentification forte par
35 exemple du type EAP-SIM ou EPA-AKA ou encore EAP-TLS. L'acronyme EAP provient de l'expression anglaise *Extensible Application Protocol*. Ce type de protocole

permet d'établir une communication sécurisée utilisant un réseau sans fil tel que défini par exemple par le standard IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 ou plus connu sous le vocable Wi-Fi.

5 Ce type de communication requiert une authentification des utilisateurs et un filtrage des trames qu'ils échangent. Le trafic échangé entre un visiteur dit « Supplicant » et le réseau de communication auquel il désire accéder, est ainsi supervisé. En liaison
10 avec la figure 1, le « Supplicant » est le dispositif nomade 1, comportant une interface réseau sans fil. Un point d'accès 2 dit « Authenticator », filtre les trames et héberge un client dit « Proxy » entre le dispositif 1 et un serveur d'authentification 3. Ce dernier,
15 couramment appelé « RADIUS » dans une architecture EAP, assure un rôle d'interface avec une base de données d'abonnés 4 pour gérer des comptes des utilisateurs et plus précisément des droits conférés à ces derniers. Dans
20 le cadre d'un protocole EAP-SIM ou EAP-AKA, la base de donnée 4 est une base de donnée centrale appelée HLR (*Host Location Register*) qui stocke pour chaque utilisateur identifié par un numéro d'abonné IMSI (*International Mobile Subscriber Identity*), ses droits définis par l'abonnement souscrit et une clé Ki. La base
25 HLR se comporte comme un serveur d'authentification produisant des triplets (RAND, SRES, Kc). RAND est un nombre aléatoire, SRES est un cryptogramme et Kc est une clé de chiffrement. SRES et Kc sont obtenus au moyen d'un algorithme à clé secrète utilisant la clé Ki de l'abonné
30 et RAND. SRES sert à authentifier l'abonné. Kc sert à chiffrer les données et la voix entre un téléphone mobile et le réseau. Un abonné est authentifié par une entité du réseau visité, dite MSC (*Mobile Switching Center*), qui stocke dans une base de donnée locale dite VLR (*Visiting Location Register*) des triplets (RAND, SRES, Kc) délivrés
35 à sa demande par la base HLR.

Le point d'accès 2 permet en outre au dispositif nomade 1 d'accéder au réseau internet 5 ou plus précisément à d'autres dispositifs communicants 5a, 5b, 5c distants.

5

La figure 2 présente une nouvelle génération de cartes de mémoire de masse appelée couramment « McX-enabled SD Card ». Ce type de carte est en quelque sorte une extension d'une carte SD (Secure Digital) traditionnelle. Cette dernière est une carte mémoire amovible de stockage de données numériques pouvant être insérée dans la quasi-totalité des dispositifs électroniques tels qu'un appareil photos, un ordinateur personnel ou portable voire dans un baladeur ou téléphone mobile en utilisant un facteur de forme réduit compatible avec le standard dit Micro-SD. Une carte « McX-enabled SD card » est conforme aux dispositions de la norme « Mobile Commerce Extension » établie par l'organisme « SD Card Association ». Une telle carte 10 comporte des moyens contrôleurs d'accès 11 et une mémoire de stockage 12, comme toute carte SD ou micro-SD. Elle comporte en outre des moyens 13 résistants aux attaques connues similaires à ceux utilisés dans le monde des cartes à puce. Les moyens 13 hébergent des données propres à un abonné et des secrets. Ils réalisent en outre des calculs cryptographiques. Pour solliciter les moyens 13, un protocole de communication comparable à celui mis en œuvre par une carte à puce, est utilisé au travers des moyens contrôleurs 11. Ainsi des commandes généralement de type APDU (*Application Protocol Data Unit*) sont transmises depuis le monde extérieur. A titre d'exemple et selon la figure 2 de telles commandes sont transmises par un ordinateur 20 à une carte 10 insérée dans ledit ordinateur 20. Une telle carte 10 est utilisée principalement dans le cadre d'applications de télévision mobile. Ainsi il est possible d'insérer une carte 10 dans un dispositif nomade 20 tel qu'une tablette internet

multimédia, un baladeur vidéo ou un ordinateur portable. La carte 10 génère alors une ou plusieurs clés de décryptage transmises(s) au dispositif nomade 20 pour lui permettre de déchiffrer un flux vidéo par exemple. La
5 carte 10 est également utilisée pour stocker des contenus multimédia, photos, musiques, documents... Pour exploiter les moyens 13 d'une carte 10, un dispositif nomade 20 doit disposer de moyens logiciels dit « drivers ou pilotes » spécifiques généralement présents dans le
10 système d'exploitation dudit dispositif. Dans le cas contraire, seule la mémoire de masse 12 peut être exploitée par le dispositif 20 au travers des moyens contrôleurs 11.

15 La grande majorité des dispositifs nomades présents actuellement sur le marché ne disposent pas d'une fonction de téléphonie mobile, ni de moyens internes résistants aux attaques connues, pour mettre en œuvre des calculs cryptographiques tels que la génération de
20 secrets, le chiffrement / déchiffrement de données etc. Ils disposent généralement en revanche de moyens de couplage avec d'autres dispositifs électroniques. Ainsi, un tel dispositif nomade peut présenter des moyens de connexion pour recevoir une carte mémoire sous la forme
25 d'une carte SD ou micro-SD.

La figure 3 permet d'illustrer un schéma fonctionnel d'un dispositif nomade 30 tel qu'une tablette internet multimédia conforme à l'invention. Celui-ci comporte des
30 moyens 330 pour transmettre des requêtes de lecture et/ou écriture à des moyens de contrôle 11 d'une carte de mémoire de masse telle que décrite en liaison avec la figure 2. Selon les modèles de dispositifs nomades, certains peuvent comporter en outre des moyens logiciels
35 301 pour transmettre aux travers des moyens 330 des requêtes de lecture et/ou d'écriture et/ou d'exécution de commandes à des cartes telles que décrites en figure 2,

ces dernières disposant de moyens internes résistants tel qu'utilisés dans le monde des cartes à puce. Ainsi des requêtes transmises à la carte par les moyens 301 et 330 sont élaborées selon un format conforme aux commandes
5 dites APDU (Application Protocol Data Unit) propres aux cartes à puce. Le dispositif nomade tel que décrit en figure 3 peut en outre communiquer avec le monde extérieur, notamment Internet, selon un protocole de communication sans fil, tel que le Wi-Fi ou à l'aide
10 d'une connexion physique à un réseau câblé. Des moyens 340 matériels et/ou logiciels sont intégrés au dit dispositif 30 pour mettre en œuvre cette communication.

En outre, un dispositif nomade 30 tel que décrit en liaison avec la figure 3 comporte également un système
15 d'exploitation 300 voire des bibliothèques de fonctions 310 pour mettre en œuvre les moyens 301, 330, 340 et d'autres et ainsi restituer à un utilisateur un contenu multimédia au moyen d'une interface graphique non représentée.

20 Selon une variante de dispositif nomade, le système d'exploitation 300 peut être dit « ouvert » et être enrichi par l'ajout de fonctions nouvelles. Ainsi il peut être envisagé que les moyens 301 nécessaires à la gestion d'une carte conforme à la figure 2, puissent être chargés
25 manuellement ou automatiquement dans le dispositif nomade après sa mise sur le marché. La présence d'un système d'exploitation 300 comportant de tels moyens 301 est nécessaire à la mise en œuvre de l'invention.

Cette dernière propose en effet de configurer un
30 dispositif nomade ne disposant pas de moyens internes résistants, sans pour autant nécessiter une adaptation physique et matérielle du dispositif pour le doter d'un module de sécurité ou composant tel qu'utilisé dans les cartes à puce. En effet, les dispositifs nomades ainsi
35 adaptés existent et soulèvent des inconvénients majeurs car chaque dispositif doit être personnalisé à l'aide notamment d'un identificateur d'abonné, de secrets

propres et dédiés à tel ou tel fournisseur de contenu etc. L'invention prévoit au contraire d'utiliser une carte 10 prévue pour être facilement et couramment accédée depuis un dispositif nomade, ladite carte
5 comprenant des moyens internes résistant 13 tels que décrits en liaison avec la figure 2. Lors de la souscription d'un abonnement auprès d'un fournisseur de contenus, une carte 10 est personnalisée et remise à un utilisateur selon un mode de personnalisation connu et
10 maîtrisé que l'on rencontre fréquemment dans le monde des cartes à puces telles que les cartes de téléphonie mobile SIM ou USIM par exemple. Une carte 10 est en quelque sorte un facteur de forme à double usage : le premier pour lire et écrire des éléments multimédia dans ou
15 depuis une mémoire de masse 12, le second pour échanger avec un équivalent fonctionnel à une carte à puce grâce aux moyens 13.

L'invention prévoit de réaliser un client 320 destiné
20 à être chargé lors de la configuration d'un dispositif nomade 30. Selon un mode de réalisation préféré, ledit client 320 est déployé par un fournisseur de contenus dans la mémoire de masse 12 d'une carte McEX-enabled SD card. Le client 320 est ainsi préalablement chargé dans
25 la mémoire 12 d'une carte 10. Lors de l'insertion d'une carte 10 conforme à l'invention dans un dispositif nomade 30, ce dernier décharge automatiquement ledit client depuis la mémoire 12 vers une mémoire du dispositif afin que le client puisse être reconnu et exploité par le
30 système d'exploitation 300. Cette opération est nécessaire lors de la configuration et peut être ignorée lors des insertions ultérieures de la carte 10. Le chargement peut-être commandé automatiquement par le système d'exploitation 300 du dispositif ou en variante,
35 un utilisateur dudit dispositif peut commander ledit chargement manuellement au moyen d'une interface homme-machine adaptée. Le client 320 chargé remplit le rôle de

« supplicant » tel que présenté en liaison avec la figure 1 selon un protocole d'authentification EAP. Le client 320 a pour rôle de relayer 350 les requêtes d'authentification 33 en provenance ou à destination d'un serveur d'authentification tel que le serveur 3 couplé à la base 4 décrits en figure 1. Ces requêtes sont réceptionnées ou acheminées par les moyens 340 depuis d'un point d'accès 2 remplissant le rôle de « l'authenticator » tels que décrit en figure 1. Lors de la réception d'une requête émanant d'un serveur d'authentificateur, les moyens 340 transmettent la requête au client 320 qui traduit ladite requête en commandes compréhensibles par les moyens 13 de la carte 10. Ces commandes sont transmises à ladite carte par les moyens 301 et 330 du dispositif 30. Le client 320 est en quelque sorte l'équivalent d'un « proxy » d'un serveur sécurisé, ce dernier se présentant sous la forme des moyens 13 d'une carte conforme à l'invention. Lesdits moyens 13 réalisent les traitements nécessaires à la complétude de la requête d'authentification et le résultat est acheminé depuis les moyens 13 au travers des moyens 11, 330, 301, 320 et 340 au point d'accès 2 qui acheminent lesdits résultats au serveur d'authentification 3 et 4. L'invention prévoit notamment que les moyens 13 puissent calculer une clé temporaire et valide durant une session de connexion. Ladite clé est alors acheminée aux moyens 340 aptes à réaliser le cas échéant un déchiffrement performant d'un contenu multimédia délivré au moyen d'un flux vidéo par exemple.

30

Selon une variante, l'invention prévoit que les moyens de stockages 12 d'une carte 10 puissent contenir en outre un composant logiciel 301 correspondant au pilote de commandes nécessaires à un dispositif nomade pour qu'il puisse communiquer avec une carte telle que la carte 10. Ainsi si ce dernier ne dispose pas des moyens 301, il est possible préalablement à l'installation du

35

client 320, de prévoir une étape manuelle ou automatique de chargement depuis la mémoire 12 vers une mémoire du dispositif pour enrichir le système d'exploitation d'un dispositif nomade non prévu pour gérer des cartes SD
5 McEX-enabled telles que décrites en figure 2.

L'invention permet ainsi notamment de configurer tout dispositif nomade ne disposant pas de moyens internes résistants pour que ce dernier puisse mettre en œuvre une
10 authentification forte. Le dispositif nomade ne subit aucune adaptation matérielle. Le protocole de déploiement des secrets et des informations liées à un abonnement se fait au travers d'un protocole de personnalisation connu du monde des cartes à puce, en initialisant des moyens 12
15 et 13 d'une carte ou de tout dispositif électronique en disposant.

L'ensemble constitué par le dispositif nomade 30 configuré et la carte 10 conformes à l'invention est parfaitement apte à mettre en œuvre un protocole
20 d'authentification forte tel qu'EAP. L'invention permet ainsi une grande facilité de développement pour le commerce de contenus multimédia protégés. Ces derniers peuvent être restitués en toute sécurité à un utilisateur d'un dispositif nomade tel qu'un baladeur vidéo couplé à
25 une carte conformement à l'invention.

L'invention a été décrite de manière non limitative en liaison avec le domaine des cartes SD « McEX-enabled ». Elle peut concerner tout type de carte offrant
30 des moyens internes résistants aux attaques connues pour réaliser des calculs cryptographiques et stocker des secrets. Tout type de carte présentant lesdits moyens et étant apte à établir une communication physique ou sans contact avec un dispositif nomade peut être utilisé pour
35 mettre en œuvre l'invention. En outre, l'invention a été décrite préférentiellement en référence à un protocole d'authentification EAP. Tout autre protocole peut être

utilisé à partir du moment où il supporte l'utilisation de requête d'authentification forte telle que décrit EAP. L'invention ne serait être restreinte aux seuls exemples de cartes ou de protocoles ayant permis d'illustrer la
5 mise en œuvre de l'invention.

REVENDICATIONS

1. Dispositif nomade (30) apte à restituer à un utilisateur un contenu multimédia préalablement délivré par un serveur de contenus (6) distant, comportant :
- 5 - des moyens (330, 301) pour recevoir et gérer une carte de mémoire de masse (10) comportant des moyens internes résistants aux attaques connues (13) pour réaliser des calculs cryptographiques ;
- 10 - des moyens (340) pour communiquer avec un point d'accès (2) à un réseau de communication sans fil (5) ;
- caractérisé en ce qu'il comporte en outre un client (320) pour relayer des requêtes d'authentification
- 15 entre la carte (10) et un serveur d'authentification (3, 4) accessible via le point d'accès (2).
2. Procédé pour configurer un dispositif nomade (30) conforme à la revendication 1 caractérisé en ce
- 20 qu'il comporte une étape de chargement dans une mémoire dudit dispositif (30) d'un client (320) pour relayer des requêtes d'authentification entre une
- carte (10) de mémoire de masse comportant des moyens internes résistants aux attaques connues (13) pour
- 25 réaliser des calculs cryptographiques et un serveur d'authentification (3, 4) accessible via un point d'accès (2).
3. Procédé selon la revendication 2 caractérisé en ce
- 30 que l'étape de chargement est réalisée automatiquement à l'insertion de la carte (10) par le dispositif nomade, le client (320) étant déchargé depuis une mémoire de masse (12) de la carte (10).

4. Procédé selon la revendication 2 caractérisé en ce que l'étape de chargement est réalisée par l'utilisateur du dispositif après l'insertion de la carte (10) dans ledit dispositif nomade, au moyen
5 d'une interface homme-machine offerte par le dispositif et en ce le client (320) est ainsi déchargé depuis une mémoire de masse (12) de la carte (10).
- 10 5. Procédé selon l'une quelconques des revendications 2 à 4 caractérisé en qu'il comporte en outre une étape préalable de chargement dans la mémoire du dispositif (30) de moyens pour communiquer (301) avec lesdits moyens internes résistants aux attaques
15 connues (13) de la dite carte (10) si lesdits moyens pour communiquer (301) sont absents dans le dispositif nomade.
- 20 6. Procédé selon la revendication 5 caractérisé en ce que l'étape de chargement préalable est réalisée automatiquement par le dispositif nomade (30) à l'insertion de la carte (10) ou par un utilisateur du dispositif nomade au moyen d'une interface homme-machine du dispositif, les moyens pour communiquer
25 (301) étant déchargés depuis une mémoire de masse (12) de la carte (10).
- 30 7. Carte de mémoire de masse (10) comportant des moyens internes résistants aux attaques connues (13) pour réaliser des calculs cryptographiques, des moyens de stockage (12), des moyens pour contrôler (11) l'accès aux dits moyens de stockage (12) et aux moyens internes résistants (13), caractérisée en ce que :

- 5
- les moyens de stockage (12) comportent un client (320), prévu pour être déchargé depuis les moyens de stockage (12) dans une mémoire d'un dispositif nomade conforme à la revendication 1, pour relayer des requêtes d'authentification entre la carte (10) et un serveur d'authentification (3, 4) accessible via un point d'accès (2) ;
 - 10 - les moyens internes résistants (13) stockent et/ou génèrent des secrets et/ou mettent en œuvre des calculs cryptographiques nécessaires à la complétude des requêtes d'authentification relayées au moyen dudit client après installation de celui-ci au
15 sein du dispositif nomade (30) conforme à la revendication 1.

20 8. Carte de mémoire de masse (10) selon la revendication 7 caractérisée en ce que la dite carte est conforme aux dispositions de la norme « *Mobile Commerce Extension* » établie par l'organisme « *SD Card Association* ».

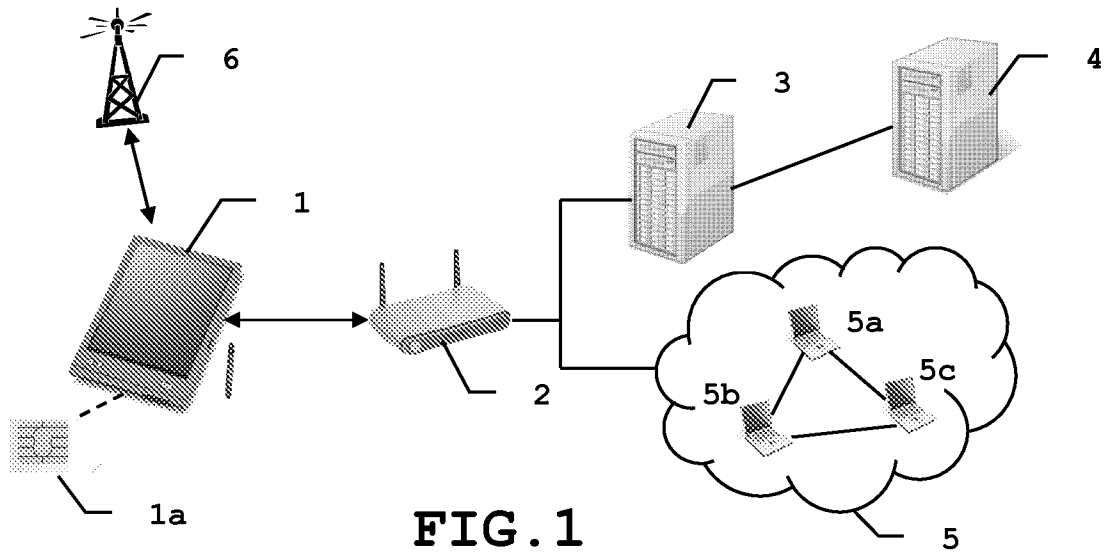


FIG. 1

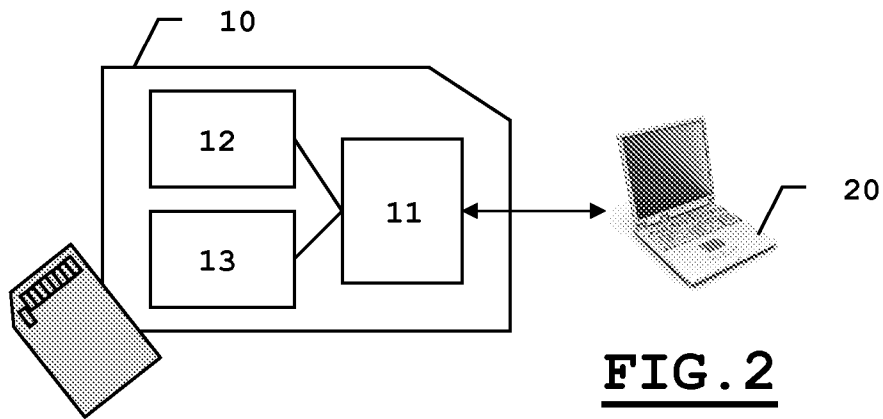


FIG. 2

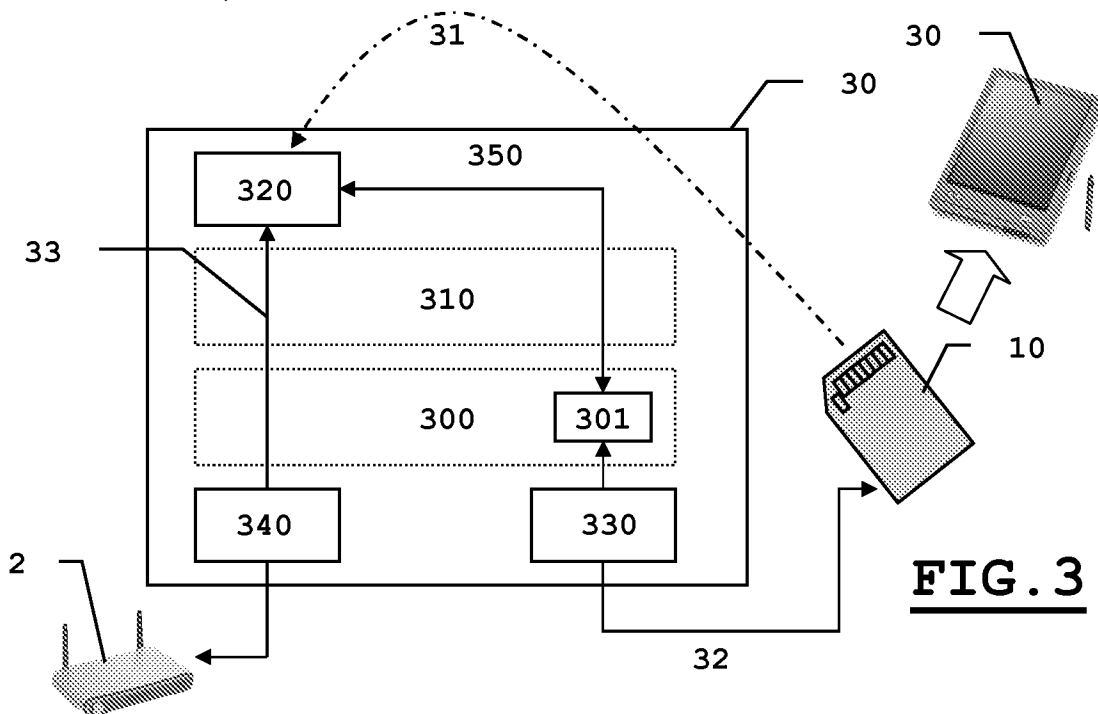


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2010/061704

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L29/06 H04W12/06 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) H04L H04W		
Documentation searched other than <i>minimum documentation</i> 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 practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2007/073937 A1 (FEINBERG EUGENE [US] ET AL) 29 March 2007 (2007-03-29) paragraph [0010] paragraph [0011] paragraph [0015] paragraph [0141] paragraph [0143] System for displaying on a camera, video stored remotely. A memory card able to communicate with an access point and able to store safely crypto information sends an authentication request to an authentication server through an access point. figures 3,5 paragraph [0013] paragraphs [0052], [0053] paragraph [0058] ----- -/--	1-4,7 5,6,8
<input checked="" type="checkbox"/>	Further documents are listed in the continuation of Box C.	<input checked="" type="checkbox"/> 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 document 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 23 November 2010		Date of mailing of the international search report 02/12/2010
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Lázaro, Marisa

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/061704

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US 2009/088133 A1 (ORLASSINO MARK [US]) 2 April 2009 (2009-04-02) paragraph [0005] paragraph [0015] paragraph [0017] paragraphs [0020], [0021] paragraph [0026] paragraphs [0035] - [0038] - paragraph [0038] figure 1</p> <p style="text-align: center;">-----</p>	4-6, 8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2010/061704

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
US 2007073937	A1	29-03-2007	EP 1938573 A2	02-07-2008
			US 2010201845 A1	12-08-2010
			WO 2007035275 A2	29-03-2007
<hr/>				
US 2009088133	A1	02-04-2009	NONE	
<hr/>				

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2010/061704

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
 INV. H04L29/06 H04W12/06
 ADD.

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

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
 H04L H04W

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	US 2007/073937 A1 (FEINBERG EUGENE [US] ET AL) 29 mars 2007 (2007-03-29) alinéa [0010] alinéa [0011] alinéa [0015] alinéa [0141] alinéa [0143] System for displaying on a camera, video stored remotely. A memory card able to communicate with an access point and able to store safely crypto information sends an authentication request to an authentication server through an access point. figures 3,5 alinéa [0013] alinéas [0052], [0053] alinéa [0058]	1-4,7 5,6,8
	----- -/--	

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

Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *Z* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

23 novembre 2010

Date d'expédition du présent rapport de recherche internationale

02/12/2010

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

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

Fonctionnaire autorisé

Lázaro, Marisa

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>US 2009/088133 A1 (ORLASSINO MARK [US]) 2 avril 2009 (2009-04-02) alinéa [0005] alinéa [0015] alinéa [0017] alinéas [0020], [0021] alinéa [0026] alinéas [0035] - [0038] - alinéa [0038] figure 1</p> <p style="text-align: center;">-----</p>	4-6,8

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2010/061704

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication	
US 2007073937	A1	29-03-2007	EP 1938573 A2	02-07-2008
			US 2010201845 A1	12-08-2010
			WO 2007035275 A2	29-03-2007
<hr/>				
US 2009088133	A1	02-04-2009	AUCUN	
<hr/>				