(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
16 janvier 2014 (16.01.2014)

WIPO IPCT

(10) Numéro de publication internationale
WO 2014/009646 A1

(51) Classification internationale des brevets :
G06Q 20/32 (2012.01)

(21) Numéro de la demande internationale :
PCT/FR2013/051630

(22) Date de dépôt international :
9 juillet 2013 (09.07.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1256779 13 juillet 2012 (13.07.2012) FR

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

(72) Inventeurs : **AUBIN, Yann-Loïc;** C/o Oberthur Technologies, 420 rue d'Estienne d'Orves, F-92700 Colombes (FR). **DUCROS, Christophe;** C/o Oberthur Technologies, 420 rue d'Estienne d'Orves, F-92700 Colombes (FR). **DESPIERRE, Thierry;** C/o Oberthur Technologies, 420 rue d'Estienne d'Orves, F-92700 Colombes (FR). **GAUVIN, David;** C/o Oberthur Technologies, 420 rue d'Estienne d'Orves, F-92700 Colombes (FR). **RICO, Ruben;** C/o Oberthur Technologies, 420 rue d'Estienne d'Orves, F-92700 Colombes (FR).

(74) Mandataires : **LEFEVRE, David** et al; Cabinet Beau De Lomenie, 158 rue de l'Université, F-75340 Paris Cedex 07 (FR).

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

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

Publiée :

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

(54) Title : SECURE ELECTRONIC ENTITY FOR AUTHORIZING A TRANSACTION

(54) Titre : ENTITE ELECTRONIQUE SECURISEE POUR L'AUTORISATION D'UNE TRANSACTION

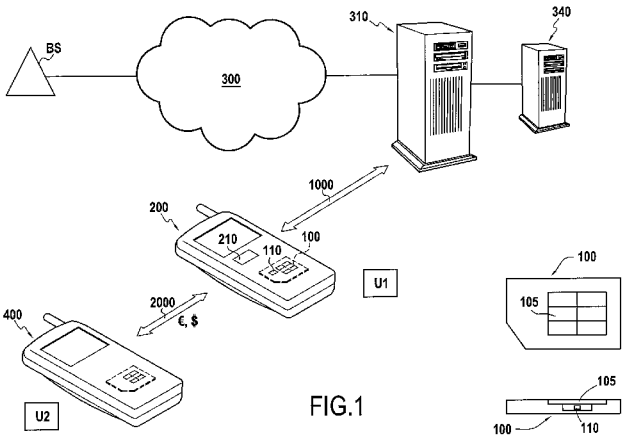

FIG.1

(57) Abstract : The invention pertains to a secure electronic entity (100) comprising a communication interface (105), characterized in that it comprises means, for, when it is connected by said communication interface (105) to a portable electronic device (200) having means of connection to a télécommunications network (300), - authenticating a remote transaction vérification server (310) in the télécommunications network (300) and authenticating itself with said remote server (310), - then establishing a secure connection (1000), via the télécommunications network, with said remote server (310), - and receiving, via said communication interface (105), data relating to a transaction envisaged (2000) with a third-party device (400) and transmitting said data, via the secure connection (1000), to the remote server (310) so that it analyses said data with a view to taking a décision as to a possible authorization of the transaction.

(57) Abrégé :

[Suite sur la page suivante]

WO 2014/009646 A1

L'invention porte sur une entité électronique sécurisée (100) comportant une interface de commumcation (105), caractérisée en ce qu'elle comporte des moyens, pour, quand elle est connectée par ladite interface de communication (105) à un dispositif électronique portable (200) disposant de moyens de connexion à un réseau de télécommunications (300), - authentifier un serveur de vérification de transaction (310) distant dans le réseau de télécommunications (300) et s'authentifier auprès dudit serveur distant (310), - puis établir une connexion sécurisée (1000), via le réseau de télécommunications, avec ledit serveur distant (310), - et recevoir, via ladite interface de communication (105), des données relatives à une transaction envisagée (2000) avec un dispositif tiers (400) et les transmettre, via la connexion sécurisée (1000), au serveur distant (310) pour qu'il les analyse en vue de prendre une décision quant à une éventuelle autorisation de la transaction.

Entité électronique sécurisée pour l'autorisation d'une transaction

Domaine technique et art antérieur

L'invention s'inscrit dans le domaine du paiement à distance, et plus précisément le paiement à un terminal de paiement à l'aide d'une entité électronique portable.

Il est connu de payer à l'aide d'une carte à microcircuit (carte bancaire à puce) et d'un terminal de paiement de commerçant, relié à un réseau de communication sécurisé par lequel il communique avec les organismes du système de paiement EMV *(Europay Mastercard Visa).*

La communication entre la carte à microcircuit et le terminal de paiement peut se faire avec ou sans contacts, notamment en utilisant la technologie NFC *(Near-Field Communication) .*

Le terminal de paiement contient quant à lui l'application permettant de vérifier les transactions envisagées, compte tenu de règles établies pour le commerçant et la carte de paiement. Il demande, si besoin est, une autorisation à un serveur distant.

Le terminal de paiement effectuant ces opérations est sécurisé, et son détenteur ne peut pas y ajouter de nouvelles applications.

Ainsi, un téléphone portable, ou une tablette graphique ne peuvent pas, sans développements particuliers, être utilisés comme terminal de paiement.

Le document WO 2008/063990 décrit un système pour paiement à un point de vente non nécessairement relié à un réseau. L'acheteur utilise son téléphone portable pour se connecter à un centre de paiement par le réseau de téléphonie mobile. Il transmet au centre de paiement un identifiant du point de vente. La communication entre le point de vente et le téléphone portable se fait par un moyen de communication à courte portée, ou une communication audio. Le niveau de sécurité est faible.

Le document WO 2010/128442 décrit un terminal de paiement incorporé dans une zone sécurisée d'une carte mémoire, telle une carte à mémoire flash, à insérer

dans un téléphone portable. La carte comporte une deuxième zone sécurisée qui incorpore une ou plusieurs cartes de paiement émises par une ou plusieurs banques pour le porteur du téléphone. Le terminal de paiement est identifié comme appartenant à une banque ou une institution qui le loue au commerçant. Il ne fonctionne qu'avec un dispositif initiateur dont doit être équipé le commerçant. La solution est peu sécurisée, car elle implique un terminal de paiement présent dans le téléphone de l'acheteur.

Pour offrir une solution surmontant les inconvénients ainsi évoqués, on souhaite mettre en place une solution de paiement sécurisée fonctionnant avec les téléphones portables compatibles existants, et ne nécessitant pas que le commerçant s'équipe de nouveaux équipements.

Objet de l'invention et avantages apportés par celle-ci

Pour cela, il est proposé une entité électronique sécurisée comportant une interface de communication, **caractérisée en ce qu**'elle comporte des moyens, pour, quand elle est connectée par ladite interface de communication à un dispositif électronique portable disposant de moyens de connexion à un réseau de télécommunications,

- authentifier un serveur de vérification de transaction distant dans le réseau de télécommunications et s'authentifier auprès dudit serveur distant,
- puis établir une connexion sécurisée, via le réseau de télécommunications, avec ledit serveur distant,
- et recevoir, du dispositif électronique portable, des données relatives à une transaction envisagée avec un dispositif tiers et les transmettre, via la connexion sécurisée, au serveur distant pour qu'il les analyse en vue de prendre une décision quant à une éventuelle autorisation de la transaction.

L'invention porte aussi sur un serveur de vérification de transaction comportant une connexion à un réseau de télécommunications, **caractérisé en ce qu'**il comporte des moyens pour,

- s'authentifier auprès d'une entité électronique sécurisée d'un dispositif électronique distant dans le réseau de télécommunications et authentifier ladite entité électronique sécurisée,

- puis établir une connexion sécurisée, via ledit réseau, avec ladite entité électronique sécurisée,
- et recevoir, via la connexion sécurisée, des données d'une transaction envisagée, et traiter ces données pour prendre une décision quant à une éventuelle autorisation de la transaction.

Grâce à cette entité électronique sécurisée et ce serveur de vérification de transaction, une transaction avec paiement à distance peut être effectuée dans des conditions sécurisées. Notamment, les clients de l'utilisateur de l'entité électronique sécurisée peuvent engager une transaction avec celui-ci avec un haut niveau de confiance, car ils savent que leurs données de paiement ne seront pas interceptées par un tiers non autorisé. De plus, le gestionnaire du serveur de vérification peut autoriser la vérification et la validation des transactions envisagées au sujet desquelles il reçoit des informations par la connexion sécurisée, car il sait que seul la personne disposant de l'entité électronique sécurisée a pu émettre les informations.

Dans un mode de réalisation particulier, l'entité électronique sécurisée, pour authentifier le serveur de vérification dans le réseau de télécommunications, envoie audit dispositif électronique portable un premier élément d'authentification d'échange encrypté avec une clé privée de l'entité électronique sécurisée, reçoit dudit serveur de vérification un deuxième élément d'authentification d'échange associé au serveur de vérification, et effectue une comparaison entre les premier et deuxième éléments d'authentification d'échange.

Dans un mode de réalisation particulier, l'entité électronique sécurisée, pour s'authentifier auprès dudit serveur distant, fournit, audit dispositif électronique portable, un paramètre d'identification auprès du service de paiement, par exemple un numéro d'abonné à un service de paiement, encrypté avec une clé privée de l'entité électronique sécurisée.

De même, dans un mode de réalisation, pour authentifier l'entité électronique sécurisée, le serveur reçoit du dispositif électronique distant et par ledit réseau, une signature cryptée, et effectue une vérification de la signature.

Pour s'authentifier auprès de l'entité électronique sécurisée, le serveur peut aussi recevoir du dispositif électronique distant un élément d'authentification d'échange accompagné d'une signature, effectue une vérification de la signature, et, en cas de vérification positive, réémet à destination de l'entité électronique sécurisée, ledit élément d'authentification d'échange.

De manière avantageuse, l'entité électronique comprend des moyens pour communiquer via ladite interface de communication avec une application d'un dispositif électronique portable à l'aide d'un mécanisme d'accès sécurisé (de type *« Access Control»),* ce qui permet à l'entité électronique sécurisée d'envoyer le premier élément d'authentification d'échange, de fournir le numéro d'abonné ou de recevoir des données relatives à la transaction envisagée de manière sécurisée.

Egalement de manière avantageuse, l'interface de communication peut être adaptée pour la communication entre l'entité électronique sécurisée et une interface de communication à courte portée du dispositif électronique portable. Par exemple, cette interface de communication peut être de type SWP *{Single Wire Protocol).*

La connexion sécurisée peut être une connexion de type SMS *{Short Message Service),* CAT-TP *(Card Application Toolkit - Transport Protocol)* ou http *{Hypertext Transfer Protocol).*

Avantageusement, l'entité électronique sécurisée comprend des moyens pour prendre en compte une information reçue du dispositif électronique portable indiquant que l'entité électronique sécurisée n'a pas pu être authentifiée par un serveur distant.

Selon un aspect de réalisation, l'entité électronique sécurisée peut comporter de plus des moyens pour fournir, audit dispositif électronique portable, un élément mémorisé lors d'une précédente utilisation, pour permettre à l'utilisateur du dispositif électronique portable de vérifier qu'il utilise une application du dispositif électronique portable qu'il a déjà utilisé auparavant.

Selon un autre aspect, l'entité électronique sécurisée comporte de plus des moyens pour vérifier l'identité d'un utilisateur du dispositif électronique portable.

L'invention porte aussi sur un procédé de paiement d'une somme d'argent d'un acquéreur à un commerçant, comprenant des étapes

- d'authentification du commerçant et d'un dispositif électronique portable associé au commerçant auprès d'un serveur de vérification de transaction distant
- de saisie par le commerçant d'un montant à payer sur le dispositif électronique portable associé au commerçant
- d'établissement d'une communication à courte portée entre le dispositif électronique portable associé au commerçant et un dispositif électronique portable associé à un acquéreur et sélection, sur le dispositif électronique portable associé à l'acquéreur, d'un environnement de paiement
- de transfert, par une connexion sécurisée, de données de transaction au serveur distant
- de vérification sur le serveur distant, des données de transaction pour savoir si la transaction doit être autorisée, incluant notamment les étapes de gestion du risque terminal de la norme EMV.

Ce procédé présente l'avantage de permettre l'utilisation du dispositif électronique portable comme une librairie EMV de niveau 2 avec les agréments correspondants, et de permettre également de déporter dans le serveur distant les opérations de vérification.

L'authentification du dispositif électronique portable associé au commerçant auprès du serveur et l'établissement de la connexion sécurisée peuvent avantageusement, mais pas exclusivement, être effectués à l'aide d'une entité électronique portable sécurisée telle que présentée plus haut.

Brève description des figures

La figure 1 présente un mode de réalisation d'un dispositif selon l'invention.

Les figures 2 et 3 présentent un mode de réalisation d'un procédé selon l'invention.

Description d'un mode de réalisation

En **figure 1,** on a présenté les dispositifs intervenant dans l'invention. Un commerçant (créditeur) UI dispose d'un téléphone portable 200 comprenant une carte SIM *(Subscriber Identity Module* aussi appelée UICC, *Universal Integrated*

Circuit Card) 100 qui a été remise au commerçant par exemple par l'opérateur de téléphonie mobile. La carte SIM 100 est représentée en agrandissement dans la partie inférieure droite de la figure 1, en vue de dessus et en vue de coupe, de côté. La carte SIM 100 a une interface de communication 105 à contacts lui permettant de communiquer avec le téléphone portable 200, par exemple de type SWP ou IS07816, et elle embarque une application 110, communément appelée applet, qui est configurée par l'organisme d'acquisition de paiement et dans laquelle est notamment enregistré un numéro d'abonné à l'organisme d'acquisition de paiement. Cette application 110 permet la réalisation de la transaction. A la place d'une carte SIM, une carte microSD (micro *Secure Digital)* ou un module sécurisé embarqué communément appelé eSE peut être utilisé.

Le téléphone portable 200 est aussi équipé d'une application de paiement vendeur 210, communément appelée MIDLET (ce qui signifie conforme à la norme MIDP, ou « *Mobile Information Device Profile* »), lui permettant de communiquer avec un utilisateur (ici le commerçant Ul) pour exécuter, en lien avec l'application 110 de la carte SIM 100 et un serveur distant (référencé 310, et qui sera présenté plus loin), différentes fonctions d'un terminal de point de vente.

Le commerçant entre en relation avec un acheteur (débiteur) U2 qui dispose d'un téléphone portable 400 ou plus généralement d'un moyen de paiement sans contact. Dans le cas où ce moyen de paiement est un téléphone portable 400, il est équipé d'une application de paiement acheteur (non représentée), qui a été fournie à l'acheteur préalablement par sa banque, ou, plus généralement, par un émetteur de moyens de paiement.

Le téléphone 200 est capable de se connecter à un réseau de téléphonie mobile 300, par l'intermédiaire d'une station de base BS. Les téléphones 200 et 400 sont capables de communiquer l'un avec l'autre directement par des moyens de communication sans fils à courte portée, par exemple de type NFC et répondant à la norme ISO 14443. L'interface de communication 105, qui est par exemple de type SWP, permet à l'entité électronique sécurisée de communiquer avec les moyens de communication sans fils à courte portée de type NFC du terminal.

Un serveur 310 est relié au réseau de téléphonie mobile 300. La carte SIM 100 et le serveur 310 sont configurés pour établir une connexion sécurisée entre eux, via une station de base du réseau de téléphonie mobile. Le serveur 310 est un serveur de vérification de transactions, géré par un organisme auprès duquel le commerçant dispose d'un numéro d'abonné.

Le serveur de vérification de transactions 310 peut entrer en communication avec un deuxième serveur 340, qui est relié au serveur de l'émetteur de moyen de paiement de l'acheteur U2.

Le serveur de vérification de transactions 310 communique de manière sécurisée avec la SIM 100.

En **figure 2,** on a présenté la première partie d'un procédé de paiement selon l'invention.

Le commerçant Ul effectue une étape El d'activation de l'application de paiement 210 de son téléphone 200.

L'application de paiement 210 se déclenche et affiche la date de la dernière transaction acceptée, qu'elle lit dans la carte SIM 100. Cet affichage permet au commerçant Ul de vérifier que l'application qu'il utilise est une application authentique, qui n'a pas été remplacée par une application pirate (malware ou autre) depuis la dernière transaction. Une autre information dynamique pourrait être utilisée.

L'application 210 de paiement 210 du téléphone 200 demande alors au commerçant Ul d'entrer son code PIN *{Personal Identification Numbei),* via une interface homme-machine, au cours d'une étape E2 de requête de code PIN. Le commerçant Ul compose alors son code PIN au cours d'une étape E3. D'autres méthodes d'identification du commerçant pourraient être utilisées, telle qu'une reconnaissance de données biométriques, par exemple. L'activation de l'application 210 peut aussi, dans une variante, utiliser la lecture d'une étiquette (tag) externe contenant des informations d'accréditation du commerçant Ul.

L'application 210 de paiement du téléphone 200 demande ensuite, au cours d'une étape E4 et via son interface homme-machine, au commerçant Ul d'introduire le

montant à débiter. Celui-ci donne cette information à l'application de paiement du téléphone 200 au cours d'une étape E5.

Au cours d'une étape E6, l'application de paiement 210 du téléphone 200 affiche un message d'invitation à destination de l'acheteur U2, lui demandant de positionner son moyen de paiement à proximité des moyens de communication à courte portée du téléphone 200. Au cours d'une étape E7, le commerçant Ul indique oralement à l'acheteur U2 de placer son moyen de paiement en face de son téléphone 200.

Parallèlement aux étapes E4 à E7, le code PIN du commerçant est transmis de l'application 210 du téléphone 200 à l'application 110 de la carte SIM 100, au cours d'une étape E8. L'application 110 est une application sécurisée qui a été introduite dans la carte SIM 100 en respectant les critères de sécurité relatifs à celle-ci. Elle dispose donc d'une forte intégrité. La communication entre l'application de paiement 210 du téléphone et l'application 110 de la carte SIM peut par exemple se faire avec le mécanisme d'Access Control pour authentifier l'application de paiement du téléphone vis-à-vis de la carte SIM (l'étape E8 est indiquée avec le symbole AC sur la figure 2 pour rappeler cette sécurisation).

L'application 110 vérifie à son tour le code PIN (Code confidentiel du commerçant), puis, à la demande de l'application 210, génère un élément d'authentification d'échange, spécifiquement choisi pour l'échange qu'elle va mener avec le serveur 310. Cet élément d'authentification d'échange est ici un nombre aléatoire ou tout autre type de donnée variable, choisi après vérification du code PIN par l'application applet ou au moment du démarrage de l'application applet.

L'application 110 de la carte SIM 100 crée alors un message comprenant à la fois le nombre aléatoire et le numéro spécifique au commerçant (numéro d'abonné), qui a été introduit dans la carte SIM 100, lors de la personnalisation de celle-ci. L'application 110 signe et crypte le message, en utilisant une clé de cryptographie asymétrique qui a également été introduite dans la carte SIM.

Le message crypté est transmis par l'applet 110 de la carte SIM 100 à l'application de paiement 210 du téléphone 200, au cours d'une étape E9 (sécurisé par le

mécanisme *à'Access Control).* L'application de paiement 210 du téléphone est configurée pour envoyer ce message au serveur 310 au cours d'une étape E10, qui constitue une étape de requête d'authentification par le serveur 310 de la carte SIM 100. Cet envoi se fait par une technique de communication disponible dans le réseau 300, comme par exemple l'envoi d'un SMS, d'un message USSD *(Unstructured Supplementary Service Data)* ou d'une commande HTTP. L'envoi est adressé au serveur 310 à l'aide d'une adresse de ce serveur, par exemple un numéro de téléphone ou une adresse Internet, qui est enregistrée dans l'application de paiement du téléphone 200 ou dans la carte SIM 100.

Le serveur 310 analyse le contenu du message reçu, en le décryptant à l'aide de la clé correspondant à la clé précédemment utilisée par l'application 110. On précise que d'autres moyens de cryptographie pourraient être utilisés, à la place d'un couple de clés asymétriques.

Le serveur 310 vérifie la signature et le numéro de commerçant. Puis, si le numéro de commerçant correspond à la signature, il conclut que l'émetteur du message est bien l'application 110 de la carte SIM qui a été remise au commerçant U2. Le terminal 310 émet un message en retour à destination de l'application 110 de la carte SIM 100, par exemple sous la forme d'un SMS. Le terminal envoie, au cours d'une étape Eli, un message PUSH normalisé, constituant une commande pour demander à l'application 110 de la carte SIM 100 d'ouvrir une connexion sécurisée pour communiquer avec lui. Ce message comprend le nombre aléatoire qui avait été généré par la carte SIM 100

L'application 110 de la carte SIM 100 reçoit le message PUSH, déchiffre et compare le nombre contenu dans celui-ci et le nombre aléatoire qu'elle a généré précédemment. S'ils sont identiques, l'application en conclut que l'émetteur du message PUSH est un serveur de confiance, authentique, géré par l'organisme de paiement.

L'application 110 de la carte SIM génère alors, à destination du serveur 310 une commande *Openchannel* par exemple, comme défini dans la norme ETSI TS 102223, demandant l'ouverture d'une connexion sécurisée, de type SMS, CAT-TP ou HTTP (cette dernière variante est définie dans le document Amendement B de

la norme *Global Platform).* Le transfert de cette commande est effectué au cours de l'étape E12.

Par exemple un canal de communication sécurisé 1000 est alors créé entre l'application 110 de la carte 100 et le serveur 310 avec des commande UDP *{User Datagram Protocol,* pour un canal CAT-TP) ou TCP/IP *{ Transmission Control Protocol / Internet Protocol'* pour un canal HTTP) transmises par le téléphone 200 (indépendamment de l'application de paiement) qui interagit avec la carte SIM par des commandes et des acquittements APDU *{application protocol data unit),* pour activer le système *Bearer Independent Protocol* (BIP).

Ou alors, dans une variante, des SMS sont échangés entre le serveur 310 et l'application 110, de manière transparente pour le téléphone 200.

Au cours d'une étape E13, les paramètres commerçants sont transmis par le serveur 310 à l'application 110 par la connexion sécurisée 1000. Les paramètres commerçants comprennent la liste AID (identifiants d'applications bancaires pour terminal de paiement), les devises, les plafonds et autres données permettant à l'application 110 de réaliser de manière autonome la transaction de paiement entre le commerçant Ul et l'acquéreur U2 au travers des téléphones 200 et 400 (ce qui inclut, dans le cadre d'une transaction EMV, les fonctions suivantes : sélection de l'application, *Get Processing Option, Read record* et *Generate AC).* L'avantage de l'étape E13 est de pouvoir utiliser le téléphone 200 comme une librairie EMV de niveau 2 avec les agréments correspondants. L'échange des paramètres commerçants entre le téléphone 200 et la carte SIM 100 se fait avec la sécurisation du mécanisme *d'Accès Control.*

Parallèlement aux étapes El à E13, l'acheteur U2 effectue une étape Fl d'activation de l'application de paiement acheteur du téléphone 400. Cette activation peut comprendre la composition d'un code personnel et le choix d'un environnement de paiement.

En **figure 3,** on a représenté la suite du procédé selon l'invention. L'étape E13 de transmission des paramètres commerçant à la carte SIM et/ou à l'application de paiement du téléphone 200 est représentée à nouveau.

Elle est suivie d'une étape E14 de communication du téléphone 100 et du téléphone 200, par leurs interfaces NFC, pour permettre au téléphone 200 de sélectionner le même environnement de paiement que celui sélectionné sur le téléphone 100, pour traiter les options de traitement, et pour effectuer l'authentification des données d'application de paiement du téléphone 400 et vérifier le numéro de moyen de paiement (numéro PAN, *Primary Account Number)* et la date d'expiration associée, ces informations étant présentes dans la carte SIM du téléphone 400, et ayant été attribuées à l'acheteur Ul lors de son abonnement auprès de sa banque.

Une étape E15 d'identification de l'acheteur U2 par entrée de son code personnel est ensuite effectuée. D'autres méthodes d'identification pourraient être utilisées, notamment une reconnaissance biométrique. Mais pour une transaction d'un petit montant, l'identification de l'acheteur peut aussi être omise. Le code personnel est composé sur le clavier du téléphone 400, et vérifié à l'aide d'une communication entre les téléphones 400 et 200.

Il est ensuite procédé à une étape E16 de gestion du risque terminal (commerçant). Cette étape est effectuée entièrement sur le serveur 310. Elle peut comprendre l'examen de l'historique des transactions sur la journée, pour le commerçant UL L'avantage de l'étape E16 est de déporter dans le serveur 310 les opérations de vérifications, par exemple *Card Holder vérification* et *Terminal Risk Management,* habituellement réalisées dans un terminal de paiement sans contact.

On procède ensuite à une étape E17 de génération d'un cryptogramme de transaction sur la base des données de transaction (montant date lieu) et des données bancaires (identifiant bancaire de l'utilisateur du téléphone 400). Ce cryptogramme est généré par la coopération de la carte SIM du téléphone 400 et de l'application de paiement du téléphone 200.

Pendant les étapes E14 à E17, l'application 110 de la carte SIM 100 reste inactive.

Une étape E18 de transfert des données de transaction depuis l'application de paiement 210 du téléphone 200 vers l'application 110 de la carte SIM 100 est ensuite effectuée, avec la sécurité du mécanisme *d'Access Control.* Les données

sont ensuite transmises, éventuellement signées et chiffrées, par la connexion sécurisée 1000, au serveur d'autorisation de paiement 310, au cours d'une étape E19. Ce transfert concerne le montant de la transaction, le numéro PAN, la date le lieu et le cryptogramme. Le serveur 310 vérifie les données de transaction et décide d'autoriser la transaction ou de la refuser. Il peut aussi estimer nécessaire de demander une autorisation à l'émetteur du moyen de paiement, et dans ce cas il contacte le serveur 340, au cours d'une étape E20, afin d'obtenir une telle autorisation, qu'il reçoit au cours d'une étape E21. Si la transaction est autorisée, une étape E22 est effectuée, au cours de laquelle le serveur 310 adresse sa réponse par la connexion sécurisée 1000 à la carte SIM 100. Un ticket est envoyé par le serveur 310, par SMS, à destination de la carte SIM 210, au cours d'une étape E23. Le ticket indique le résultat de la transaction.

L'invention n'est pas limitée aux modes de réalisation présentés, mais concerne toutes les variantes dans le cadre de la portée des revendications. Notamment, le réseau 300, au lieu d'être un réseau de téléphonie mobile, peut être un réseau étendu (par exemple Internet) auquel le téléphone 200 (ou une tablette tactile ou un autre dispositif électronique mobile) accède via une connexion Wi-Fi.

REVENDICATIONS

1. Entité électronique sécurisée (100) comportant une interface de communication (105), **caractérisée en ce qu**'elle comporte des moyens, pour, quand elle est connectée par ladite interface de communication (105) à un dispositif électronique portable (200) disposant de moyens de connexion à un réseau de télécommunications (300),

- authentifier un serveur de vérification de transaction (310) distant dans le réseau de télécommunications (300) et s'authentifier auprès dudit serveur distant (310),
- puis établir une connexion sécurisée (1000), via le réseau de télécommunications, avec ledit serveur distant (310),
- et recevoir (E18), via ladite interface de communication (105), des données relatives à une transaction envisagée (2000) avec un dispositif tiers (400) et les transmettre (E19), via la connexion sécurisée (1000), au serveur distant (310) pour qu'il les analyse en vue de prendre une décision quant à une éventuelle autorisation de la transaction.

2. Entité électronique sécurisée selon la revendication 1, qui, pour authentifier le serveur de vérification (310) dans le réseau de télécommunications (300), envoie (E9) via ladite interface de communication (105) un premier élément d'authentification d'échange encrypté avec une clé privée de l'entité électronique sécurisée (100), reçoit (Eli) dudit serveur de vérification (310) un deuxième élément d'authentification d'échange associé au serveur de vérification, et effectue une comparaison entre les premier et deuxième éléments d'authentification d'échange.

3. Entité électronique sécurisée selon la revendication 1 ou la revendication 2, qui, pour s'authentifier auprès dudit serveur distant, transmet (E9), via ladite interface de communication (105), un paramètre d'identification au service de paiement, encrypté avec une clé privée de l'entité électronique sécurisée (100).

4. Entité électronique sécurisée selon l'une des revendications 1 à 3, configurée pour que la connexion sécurisée (1000) soit une connexion de type SMS, CAT-TP ou HTTP.

5. Entité électronique sécurisée selon l'une des revendications 1 à 4, qui comprend des moyens pour communiquer via ladite interface de communication (105) avec une application (210) d'un dispositif électronique portable à l'aide d'un mécanisme d'accès sécurisé.

6. Entité électronique sécurisée selon l'une des revendications 1 à 5, dont l'interface de communication (105) est adaptée pour la communication entre l'entité électronique sécurisée et une interface de communication à courte portée du dispositif électronique portable (200).

7. Entité électronique sécurisée selon l'une des revendications 1 à 6, comprenant des moyens pour prendre en compte une information reçue du dispositif électronique portable indiquant que l'entité électronique sécurisée (100) n'a pas pu être authentifiée par un serveur distant (310).

8. Entité électronique sécurisée selon l'une des revendications 1 à 7, comportant de plus des moyens pour fournir, audit dispositif électronique portable, un élément mémorisé lors d'une précédente utilisation, pour permettre à l'utilisateur du dispositif électronique portable de vérifier qu'il utilise une application du dispositif électronique portable qu'il a déjà utilisée auparavant.

9. Entité électronique sécurisée selon l'une des revendications 1 à 8, comportant de plus des moyens pour vérifier l'identité d'un utilisateur du dispositif électronique portable.

10. Serveur de vérification de transaction (310) comportant une connexion à un réseau de télécommunications (300), **caractérisé en ce qu'**il comporte des moyens pour,

- s'authentifier auprès d'une entité électronique sécurisée (100) d'un dispositif électronique distant (200) dans le réseau de télécommunications (300) et authentifier ladite entité électronique sécurisée (100),
- puis établir une connexion sécurisée, via ledit réseau, avec ladite entité électronique sécurisée (100),

- et recevoir (E19), via la connexion sécurisée (1000), des données d'une transaction envisagée (2000), et traiter ces données pour prendre une décision quant à une éventuelle autorisation de la transaction.

11. Serveur selon la revendication 10, qui pour authentifier l'entité électronique sécurisée (100), reçoit (E10), du dispositif électronique distant (200) et par ledit réseau, une signature cryptée, et effectue une vérification de la signature.

12. Serveur selon la revendication 10 ou la revendication 11, qui pour s'authentifier auprès de l'entité électronique sécurisée (100), reçoit (E10) du dispositif électronique distant (200) un élément d'authentification d'échange accompagné d'une signature, effectue une vérification de la signature, et, en cas de vérification positive, réémet (Eli), à destination de l'entité électronique sécurisée (100), ledit élément d'authentification d'échange.

13. Procédé de paiement d'une somme d'argent d'un acquéreur (U2) à un commerçant (Ul), comprenant des étapes

- d'authentification d'un dispositif électronique portable associé au commerçant auprès d'un serveur de vérification de transaction distant, à l'aide d'une entité électronique portable sécurisée

- de saisie par le commerçant (Ul) d'un montant à payer sur le dispositif électronique portable associé au commerçant

- d'établissement d'une communication à courte portée entre le dispositif électronique portable associé au commerçant et un dispositif électronique portable associé à un acquéreur et sélection (Fl), sur le dispositif électronique portable associé à l'acquéreur, d'un environnement de paiement

- de transfert, par une connexion sécurisée (1000) établie à l'aide de l'entité électronique portable sécurisée, de données de transaction au serveur distant,

- de vérification sur le serveur distant, des données de transaction pour savoir si la transaction doit être autorisée, incluant notamment les étapes (E16) de gestion du risque terminal de la norme EMV.

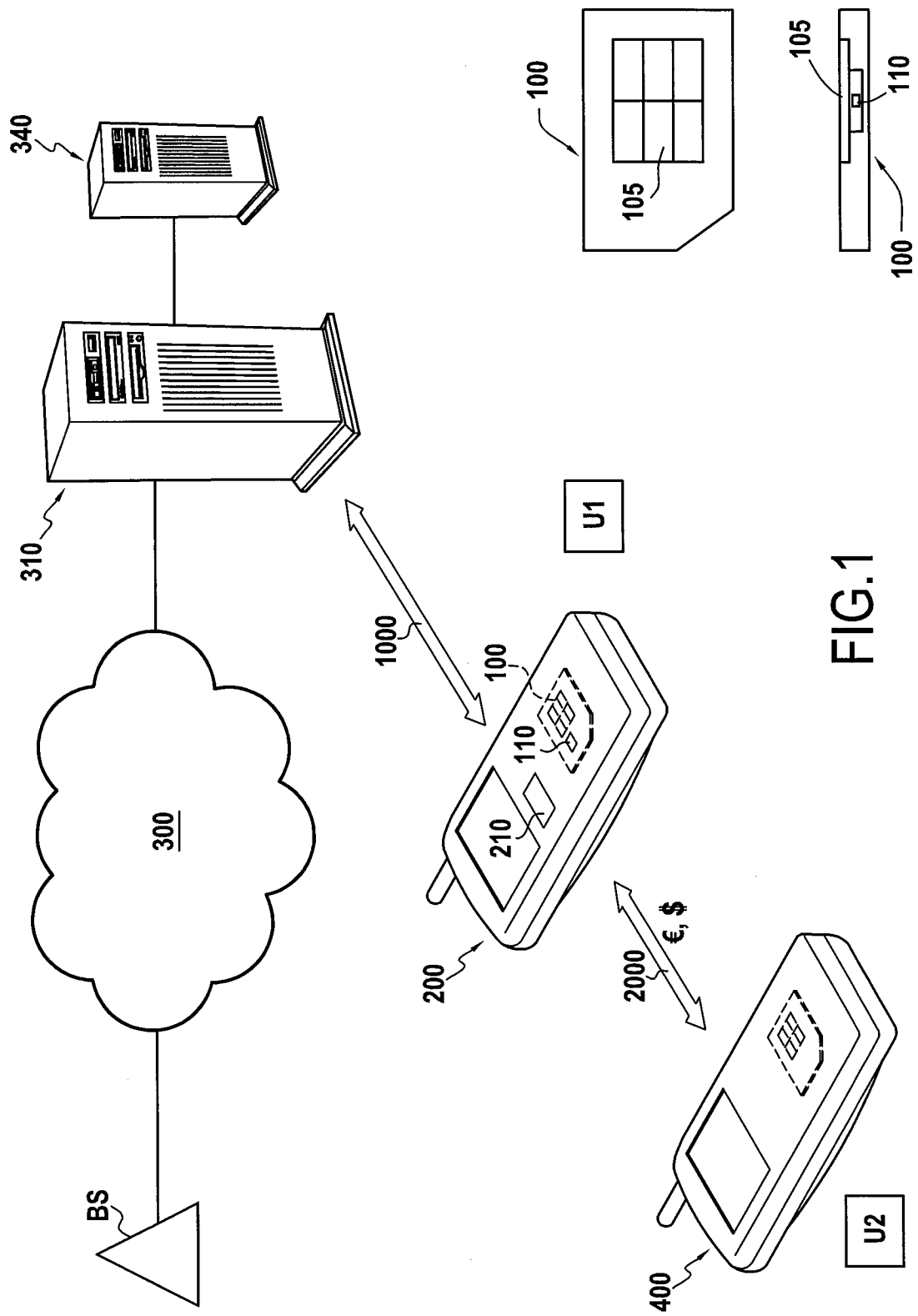
340
310
300
BS
1000
100
110
210
200
U1
2000
€, $
400
U2
100
105
105
110
100

FIG.1

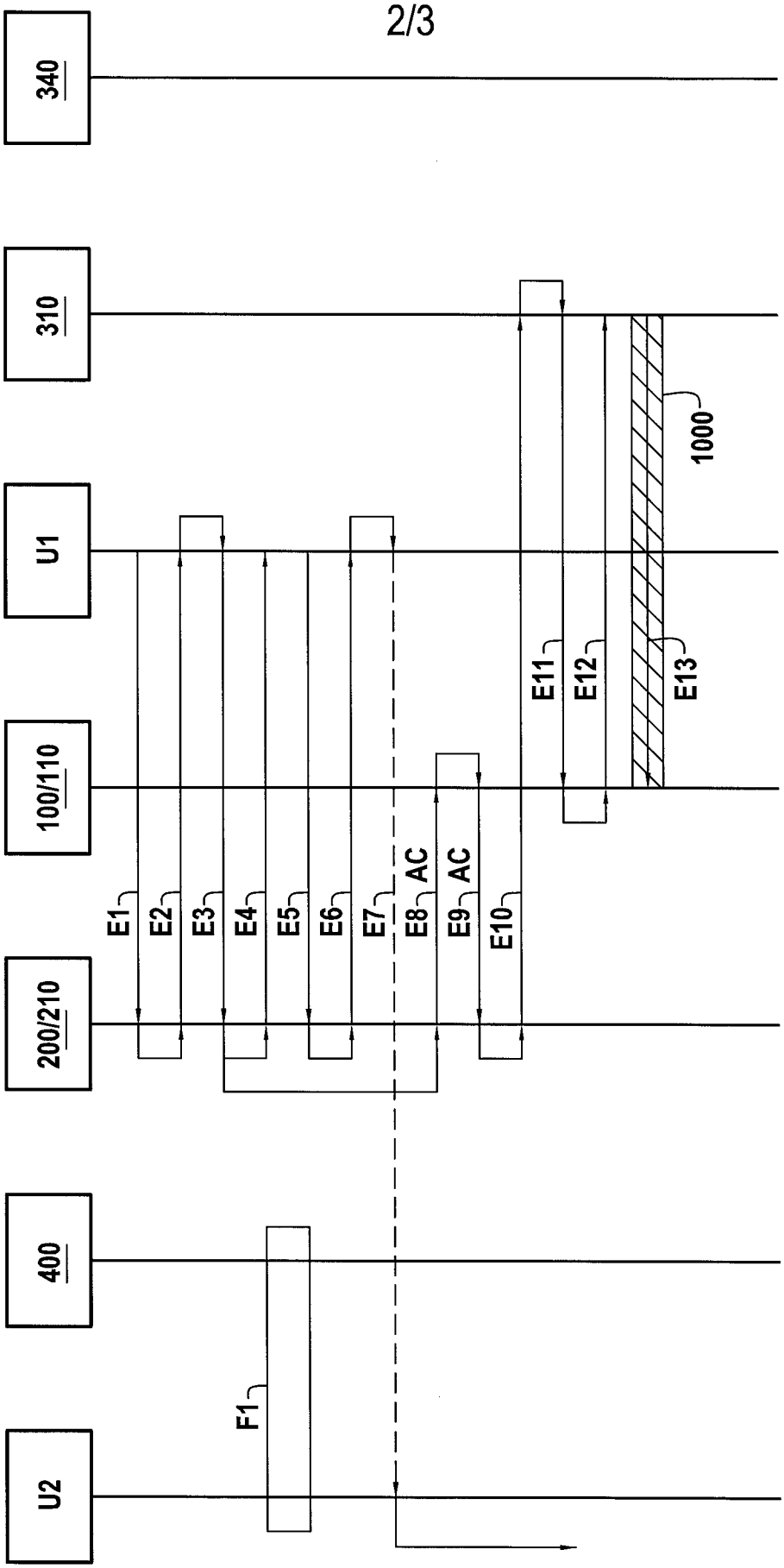
340
310
U1
100/110
200/210
400
U2
1000
E1
E2
E3
E4
E5
E6
E7
AC
E8
AC
E9
E10
E11
E12
E13
F1

FIG.2

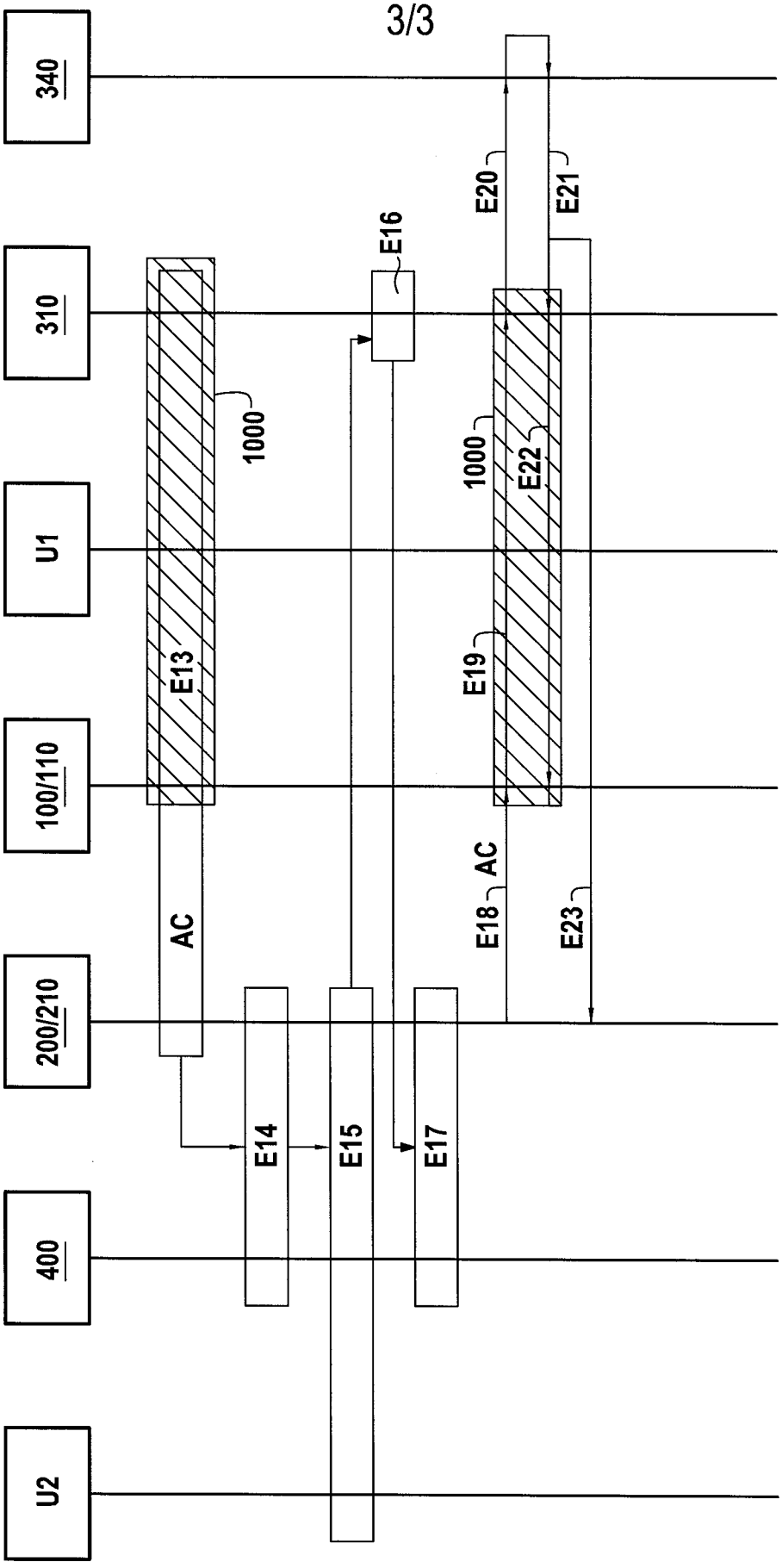
340
310
U1
100/110
200/210
400
U2
E13
E14
E15
E16
E17
E18
E19
E20
E21
E22
E23
AC
AC
1000
1000

FIG.3

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2013/051630

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/32
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification **System** followed **by** classification **symbols)**
G06Q

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 053 553 Al (OBERTHUR TECHNOLOGI ES [FR]) 29 Apri l 2009 (2009-04-29) paragraphs [0030] , [0048] ; cl aims 1-4,8	1-13
X	EP 2 075 751 Al (AXALT0 SA [FR]) 1 July 2009 (2009-07-01) paragraphs [0127] , [0151] , [0178] ; cl aim 1; f i gure 1	1-13
X	EP 2 053 554 Al (OBERTHUR TECHNOLOGI ES [FR]) 29 Apri l 2009 (2009-04-29) paragraphs [0058] - [0061] , [0075] ; cl aims 8-11	1-13
A	US 2011/231319 Al (BAY0D JOSE IGNACIO BAS [ES] ET AL) 22 September 2011 (2011-09-22) cl aims 1-8	1-13

-/- ·

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Spécial catégories of cited documents :

"A" document defining the gênerai 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" documentwhich may throw doubts on priority claim(s) orwhich is cited to establish the publication date of another citation or other spécial 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 ortheory 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
27 August 2013	05/09/2013

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	Cl osa, Dani el

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2013/051630

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/128442 A2 (L0G0M0TI0N SRO [SK] ; FLOREK MI ROSLAV [SK] ; MASARYK MICHAL [SK] ; RI FFEL) 11 November 2010 (2010-11-11) cited in the appli cation the whole document	1-13
A	W0 2008/063990 A2 (YUAN GONG YI [CN] ; LEB0WITZ GARY [US]) 29 May 2008 (2008-05-29) cited in the appli cation the whole document	1-13

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2013/051630

Patent document oited in searoh report	Publication date	Patent family member(s)	Publication date
EP 2053553 Al	29-04-2009	EP 2053553 Al	29-04-2009
		FR 2922670 Al	24-04-2009
		US 2009119214 Al	07-05-2009
EP 2075751 Al	01-07-2009	EP 2075751 Al	01-07-2009
		WO 2009077380 Al	25-06-2009
EP 2053554 Al	29-04-2009	EP 2053554 Al	29-04-2009
		FR 2922669 Al	24-04-2009
		US 2009106159 Al	23-04-2009
US 2011231319 Al	22-09-2011	NONE	
W0 2010128442 A2	11-11-2010	AU 2010244100 Al	15-12-2011
		CA 2739858 Al	11-11-2010
		CN 102460520 A	16-05-2012
		EP 2462567 A2	13-06-2012
		JP 2012526306 A	25-10-2012
		KR 20120030408 A	28-03-2012
		RU 2011148267 A	10-06-2013
		US 2011021175 Al	27-01-2011
		US 2011022482 Al	27-01-2011
		US 2011112968 Al	12-05-2011
		WO 2010128442 A2	11-11-2010
W0 2008063990 A2	29-05-2008	US 2008114699 Al	15-05-2008
		W0 2008063990 A2	29-05-2008

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2013/051630

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/32
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)
G06Q

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	EP 2 053 553 A1 (OBERTHUR TECHNOLOGIES [FR]) 29 avril 2009 (2009-04-29) alinéas [0030], [0048]; revendications 1-4,8	1-13
X	EP 2 075 751 A1 (AXALTO SA [FR]) 1 juillet 2009 (2009-07-01) alinéas [0127], [0151], [0178]; revendication 1; figure 1	1-13
X	EP 2 053 554 A1 (OBERTHUR TECHNOLOGIES [FR]) 29 avril 2009 (2009-04-29) alinéas [0058] - [0061], [0075]; revendications 8-11	1-13
A	US 2011/231319 A1 (BAYOD JOSE IGNACIO BAS [ES] ET AL) 22 septembre 2011 (2011-09-22) revendications 1-8	1-13

-/- .

[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
27 août 2013	05/09/2013

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	Closa, Daniel

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2013/051630

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	WO 2010/128442 A2 (L0G0M0TI0N SRO [SK] ; FLOREK MI ROSLAV [SK] ; MASARYK MICHAL [SK] ; RI FFEL) 11 novembre 2010 (2010-11-11) cité dans la demande le document en entier	1-13
A	W0 2008/063990 A2 (YUAN GONG YI [CN] ; LEB0WITZ GARY [US]) 29 mai 2008 (2008-05-29) cité dans la demande le document en entier	1-13

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2013/051630

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 2053553 A1	29-04-2009	EP 2053553 A1	29-04-2009
		FR 2922670 A1	24-04-2009
		US 2009119214 A1	07-05-2009
EP 2075751 A1	01-07-2009	EP 2075751 A1	01-07-2009
		WO 2009077380 A1	25-06-2009
EP 2053554 A1	29-04-2009	EP 2053554 A1	29-04-2009
		FR 2922669 A1	24-04-2009
		US 2009106159 A1	23-04-2009
US 2011231319 A1	22-09-2011	AUCUN	
WO 2010128442 A2	11-11-2010	AU 2010244100 A1	15-12-2011
		CA 2739858 A1	11-11-2010
		CN 102460520 A	16-05-2012
		EP 2462567 A2	13-06-2012
		JP 2012526306 A	25-10-2012
		KR 20120030408 A	28-03-2012
		RU 2011148267 A	10-06-2013
		US 2011021175 A1	27-01-2011
		US 2011022482 A1	27-01-2011
		US 2011112968 A1	12-05-2011
		WO 2010128442 A2	11-11-2010
WO 2008063990 A2	29-05-2008	US 2008114699 A1	15-05-2008
		WO 2008063990 A2	29-05-2008