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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
13 mars 2008 (13.03.2008)

(10) Numéro de publication internationale
WO 2008/029059 A2

(51) Classification internationale des brevets : Non classée

(21) Numéro de la demande internationale :
PCT/FR2007/051874

(22) Date de dépôt international :
5 septembre 2007 (05.09.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
06 53620 7 septembre 2006 (07.09.2006) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BARRE, Christian** [FR/FR]; 3, rue Gabriel Faure APT 34, F-35830 Betton (FR). **LE ROUZIC, Jean-Pierre** [FR/FR]; 9, rue Gustave Toudouze, F-35700 Rennes (FR).

(74) Mandataire : **FRANCE TELECOM/FTR & D/PIV/BREVETS**; GUILLERM Patrice, 38-40, rue du Général Leclerc, F-92794 Issy Les Moulineaux Cedex 9 (FR).

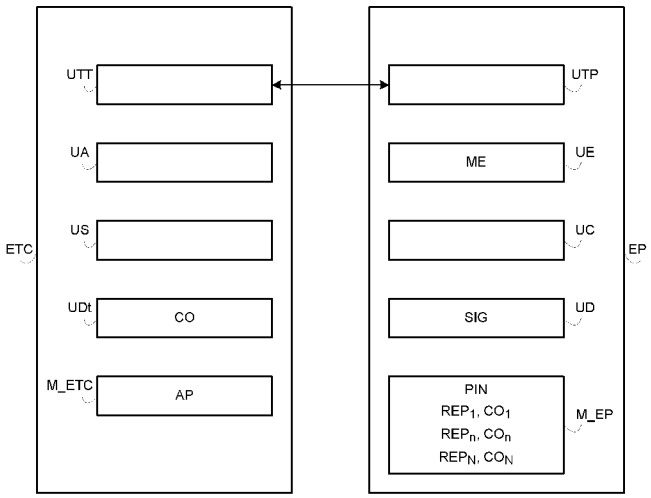
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

*[Suite sur la page suivante]*

(54) **Title:** SECURING OF CODE FOR PERSONAL ENTITY

(54) **Titre :** SÉCURISATION DE CODE POUR ENTITÉ PERSONNELLE




(57) **Abstract:** A system secures a personal code for a user of a personal entity (EP) containing data (SIG) and associated with a code processing entity (ETC). The personal entity establishes a ($REP\_CL_n$) graphical representation of characters that may be modified with each request for data. The representation is associated with first particulars of characters of the personal code and transmitted to the code processing entity. The code processing entity displays the representation so that the user selects therefrom characters representative of the personal code, determines second particulars of the selected characters and transmits the second particulars to the personal entity. The personal entity compares the first and second particulars so as to transmit the data requested if said particulars correspond.

*[Suite sur la page suivante]*

WO 2008/029059 A2

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Publiée :**

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

**(57) Abrégé :** Un système sécurise un code personnel d'un usager d'une entité personnelle (EP) contenant des données (SIG) et associée à une entité de traitement de code (ETC). L'entité personnelle établit une ($REP\_CL_n$) représentation graphique de caractères pouvant être modifiée à chaque demande des données. La représentation est associée à des premières coordonnées de caractères du code personnel et transmise à l'entité de traitement de code. L'entité de traitement de code affiche la représentation pour que l'usager y sélectionne des caractères représentatifs du code personnel, détermine des deuxièmes coordonnées des caractères sélectionnés et transmet les deuxièmes coordonnées à l'entité personnelle. L'entité personnelle compare les premières et deuxièmes coordonnées pour transmettre les données demandées si lesdites coordonnées correspondent.

# Sécurisation de code pour entité personnelle

La présente invention concerne une sécurisation d'un code personnel pour une entité personnelle, telle qu'une carte à puce. Le code est appelé également code PIN ("Personal Identity Number" en anglais) souvent saisi pour une transaction électronique, l'identification d'un usager, une non répudiation ou une gestion de droit numérique DRM ("Digital Right Management" en anglais).

L'invention concerne plus généralement la sécurisation de tout code personnel tel qu'un mot de passe à saisir dans un environnement non sécurisé.

L'identification formelle sécurisée d'un usager par exemple lors d'une transaction électronique entre deux terminaux dans un réseau de télécommunications peut nécessiter une carte à puce appartenant à l'usager et contenant des données secrètes. La carte est insérée dans un lecteur de carte de l'un des terminaux. Les données secrètes constituées par un code personnel unique, dit code PIN, sont saisies par l'usager sur une interface homme-machine du terminal.

Lors d'un vol ou d'une perte de la carte à puce, le code PIN a pour avantage de n'être connu que de l'usager de la carte et un tiers ne peut donc en faire usage. Cependant, des virus informatiques actifs dans les terminaux sont conçus pour détecter le code PIN saisi par l'usager par exemple et ainsi le transmettre à une autre entité électronique ou l'utiliser pour accéder directement aux données secrètes de la carte.

Pour remédier à cet inconvénient, on a déjà proposé lors de la fabrication ou de la

commercialisation de la carte, de préenregistrer plusieurs codes PIN différents dans la carte, chaque code étant enregistré pour une unique utilisation. Une liste de ces codes est adressée à l'usager de la carte sous pli confidentiel. Cependant, le nombre limité de codes PIN restreint le nombre d'utilisations de la carte. En outre, un nombre élevé de codes PIN préenregistrés est difficilement mémorisable par l'usager de la carte. La perte ou le vol de la liste de ces codes rend l'emploi de la carte obsolète.

Il est également bien connu d'inscrire un code confidentiel unique sur l'une des faces de la carte à puce et de le saisir par l'usager de la carte lors d'une transaction électronique, par exemple un achat en ligne sans l'utilisation de la carte à puce. Ce code imposé par le constructeur de la carte et connu du fournisseur de la carte, par exemple une banque, évite à un fraudeur ne possédant pas de carte à puce de créer un faux numéro de carte et d'initier des transactions sécurisées en ligne, celles-ci nécessitant la saisie du code inscrit sur la carte.

Actuellement, pour saisir de manière sécurisée le code PIN d'une carte à puce, un terminal doit être relié à un dispositif externe tel qu'un clavier dont les transactions entre le terminal et le dispositif sont limitées afin d'éviter toute contamination d'un virus dans le dispositif. Cette solution est peu ergonomique et très coûteuse.

Pour remédier aux inconvénients évoqués ci-dessus, un procédé pour sécuriser un code personnel d'un usager donnant accès à des données incluses dans

une entité personnelle, est caractérisé en ce qu'il comprend :

un établissement et un affichage d'une représentation graphique comprenant des caractères représentatifs du code personnel et associée à au moins une consigne,

une sélection desdits caractères par l'usager sur la représentation graphique affichée en fonction de ladite au moins une consigne,

une comparaison des premières coordonnées associées aux caractères sélectionnés par l'usager à des deuxièmes coordonnées de caractères représentatifs du code personnel associées à la représentation graphique, et

une transmission des données si les premières et deuxièmes coordonnées correspondent.

L'invention sécurise le code personnel d'un usager pour autoriser l'accès à des données incluses dans l'entité personnelle, telle qu'une carte à puce, après avoir établi une représentation graphique de caractères qui est affichée dans une entité de traitement de code, telle qu'un terminal, la représentation incluant des caractères représentatifs du code personnel. L'usager sélectionne des caractères qui sont représentatifs du code personnel dans la représentation graphique affichée et qui ne peuvent pas être prédits par un attaquant en surveillant les caractères sélectionnés de manière à en déduire un comportement répétitif de l'usager.

Selon une caractéristique de l'invention, le procédé comprend un établissement de la représentation graphique de caractères modifiée après

un nombre prédéterminé de demandes successives des données.

Pour plus de sécurité, la représentation graphique peut être modifiée à chaque demande des données de l'entité personnelle; en d'autres termes, la représentation graphique varie d'une demande de données à la suivante. Par exemple, la représentation graphique est modifiée par une modification de la disposition des caractères. Toutefois plus généralement, la représentation graphique est modifiée après un nombre prédéterminé de demandes successives des données, le nombre prédéterminé étant égal ou supérieur à 1. Par exemple, le nombre prédéterminé est inférieur à six. Un virus informatique actif dans l'entité de traitement de code ne peut alors déduire le code personnel de codes saisis par l'usager.

Selon une première réalisation de l'invention, la représentation graphique est une table ayant un nombre prédéterminé de cases dont certaines sont associées respectivement à des caractères alphanumériques incluant les caractères du code personnel et sont disposées aléatoirement dans la table.

Selon une deuxième réalisation de l'invention, la représentation graphique est associée à au moins une consigne, afin que l'usager y sélectionne les caractères du code personnel en fonction de ladite au moins une consigne. Les consignes peuvent être modifiées après le nombre prédéterminé de demandes successives des données. La représentation graphique peut comprendre plusieurs ensembles distincts de caractère dont un est à sélectionner selon les consignes pour que l'usager y sélectionne les caractères représentatifs du code personnel. En

variante, la représentation graphique peut alors comprendre plusieurs ensembles distincts de caractère dont au moins deux à sélectionner selon les consignes pour que l'usager y sélectionne les caractères représentatifs du code personnel.

L'invention concerne aussi un procédé pour sécuriser un code personnel d'un usager donnant accès à des données incluses dans une entité personnelle. Le procédé est caractérisé en ce qu'il comprend :

Un établissement d'une représentation graphique comprenant des caractères représentatifs du code personnel et associée à au moins une consigne,

une comparaison de premières coordonnées associées à des caractères représentatifs du code personnel et sélectionnés par l'usager sur la représentation graphique affichée en fonction d'au moins une consigne, à des deuxièmes coordonnées de caractères représentatifs du code personnel associées à ladite représentation graphique, et

une transmission des données si les premières et deuxièmes coordonnées correspondent.

Selon une caractéristique de l'invention, le procédé comprend un établissement de la représentation graphique de caractères modifiée après un nombre prédéterminé de demandes successives des données. En variante, la représentation graphique est modifiée par une modification de la disposition des caractères.

Selon des réalisations du procédé pour sécuriser un code personnel, la représentation graphique peut être une table ayant un nombre prédéterminé de cases, ou être associée à des consignes et comprendre plusieurs ensembles distincts de caractère, comme indiqué ci-dessus.

L'invention est également relative à une entité personnelle pour sécuriser un code personnel d'un usager donnant accès à des données incluses dans l'entité personnelle, caractérisée en ce qu'elle comprend :

Un moyen (UE) pour établir une représentation graphique ($REP_n$) comprenant des caractères (CR) représentatifs du code personnel et associée à au moins une consigne (CS1, CS2),

un moyen pour comparer des premières coordonnées associées à des caractères représentatifs du code personnel et sélectionnés par l'usager sur la représentation graphique affichée en fonction de ladite au moins une consigne à des deuxièmes coordonnées de caractères représentatifs du code personnel associées à ladite représentation graphique, et

un moyen pour transmettre les données si les premières et deuxièmes coordonnées correspondent.

L'entité personnelle comporte des moyens pour mettre en œuvre le procédé décrit précédemment.

L'invention se rapporte aussi à un produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un processeur. Le produit programme comprend des instructions pour la mise en œuvre des étapes suivantes:

un établissement et un affichage d'une représentation graphique comprenant des caractères représentatifs du code personnel et associée à au moins une consigne,

une sélection desdits caractères par l'usager sur la représentation graphique affichée en fonction de ladite au moins une consigne,

une comparaison des premières coordonnées associées aux caractères sélectionnés par l'usager à des deuxièmes coordonnées de caractères représentatifs du code personnel associées à la représentation graphique, et

une transmission des données si les premières et deuxièmes coordonnées correspondent.

L'invention concerne encore un procédé de traitement de code pour sélectionner par un usager un code personnel donnant accès à des données incluses dans une entité personnelle. Le procédé est caractérisé en ce qu'il comprend :

un affichage d'une représentation graphique comprenant des caractères représentatifs du code personnel et associée à au moins une consigne,

une sélection desdits caractères par l'usager sur la représentation graphique affichée en fonction de ladite au moins une consigne,

une détermination de premières coordonnées associées aux caractères sélectionnés par l'usager, et

une transmission des premières coordonnées déterminées à l'entité personnelle afin que l'entité personnelle compare les premières coordonnées transmises à des deuxièmes coordonnées de caractères représentatifs du code personnel associées à la représentation graphique et transmette les données demandées si les premières et deuxièmes coordonnées correspondent.

Selon des réalisations du procédé de traitement de code, la représentation graphique peut être

modifiée par une modification de la disposition des caractères, ou être une table ayant un nombre prédéterminé de cases, ou être associée à des consignes et comprendre plusieurs ensembles distincts de caractère, comme indiqué ci-dessus.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations de l'invention données à titre d'exemples non limitatifs, en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un bloc-diagramme schématique d'un système de sécurisation de code personnel comprenant une entité personnelle et une entité de traitement de code ;
- la figure 2 est un bloc-diagramme représentatif d'une architecture matérielle pour chaque entité du système de sécurisation de code personnel selon l'invention ;
- les figures 3, 4 et 5 sont des exemples de représentation graphique de caractères affichée selon l'invention ; et
- la figure 6 est un algorithme du procédé selon l'invention pour sécuriser un code personnel d'usager.

En référence à la figure 1, un système de sécurisation de code personnel d'usager d'entité personnelle, dit code PIN ("Personal Identity Number" en anglais), comprend une entité personnelle EP, telle qu'une carte à puce, associée avec ou sans contact à une entité de traitement de code ETC, telle qu'un terminal.

Une application cliente AP dans l'entité de traitement de code ETC est activée par l'usager de l'entité personnelle EP associée à l'entité de traitement de code ETC et ouvre un canal de communication avec une entité externe, appelée serveur de ressources, tel qu'un serveur d'achat en ligne à travers un réseau de télécommunications. Afin que l'usager puisse accéder via l'application à des ressources sécurisées du serveur, le serveur demande à l'application de lui transmettre des données telles qu'une signature identifiant l'usager. La signature est fournie par l'entité personnelle EP de l'usager et est accessible après une sélection du code personnel PIN de l'usager, par exemple sur un clavier relié à l'entité de traitement de code ETC.

Pour éviter qu'un tiers ne détecte le code personnel PIN de l'usager lors de sa sélection, l'invention établit une représentation graphique aléatoire, par exemple similaire à un clavier numérique, et des consignes de sélection afin que l'usager saisisse son code personnel à partir de cette représentation graphique, la représentation graphique pouvant être différente à chaque demande des données, ou modifiée après un nombre prédéterminé de demandes successives des données par exemple compris entre deux et cinq.

Dans la figure 2, on a représenté une architecture matérielle pour l'entité personnelle EP et l'entité de traitement de code ETC. L'architecture comprend une mémoire M, une unité de traitement équipée par exemple d'un microprocesseur P et piloté par des programmes d'ordinateur mémorisés dans une mémoire MPg mettant en œuvre les procédés selon

l'invention. Un module d'entrée Et et un module de sortie St tels que des interfaces de communication sont respectivement disposés en entrée et en sortie de l'unité de traitement P.

Afin d'éviter toute confusion entre des éléments inclus dans les architectures des entités, chaque élément de l'architecture d'une entité est désigné ci-après dans la description en combinaison avec le repère désignant l'entité auquel il appartient. Ainsi l'entité personnelle EP comprend un processeur P_EP, une mémoire M_EP, une mémoire de programme MPg_EP, un module d'entrée Et_EP et un module de sortie St_EP. L'entité de traitement de code ETC comprend un processeur P_ETC, une mémoire M_ETC, une mémoire de programme MPg_ETC, un module d'entrée Et_ETC et un module de sortie St_ETC.

Dans la figure 1, on a représenté l'entité de traitement de code ETC et l'entité personnelle EP sous forme de blocs fonctionnels dont la plupart assurent des fonctions ayant un lien avec l'invention et peuvent correspondre à des modules logiciels et/ou matériels.

L'entité de traitement de code ETC en tant que terminal comprend une unité de transmission UTT, une unité d'affichage UA, une unité de sélection US et une unité de détermination de coordonnées UDt. En se référant à la figure 2, l'unité de transmission UTT englobe les modules Et_ETC et St_ETC et l'unité de détermination de coordonnées UDt est mémorisée dans la mémoire de programme MPg_ETC.

La mémoire M_ETC comporte notamment une application cliente AP, telle qu'une application d'achat en ligne.

L'entité de traitement ETC peut être un assistant numérique personnel communicant PDA, un terminal domestique portable ou non comme une console de jeux vidéo ou un récepteur de télévision intelligent coopérant avec une télécommande à afficheur ou un clavier alphanumérique servant également de souris à travers une liaison infrarouge.

En variante, l'unité d'affichage UA et l'unité de sélection US, d'une part, et l'unité de détermination UDt d'autre part, sont respectivement deux terminaux distincts dont chacun possède une architecture analogue à celle représentée à la figure 2.

L'entité personnelle EP en tant que carte à puce comprend principalement une unité de transmission UTP pour échanger des messages avec l'unité de transmission UTT de l'entité de traitement de code ETC, une unité d'établissement UE d'une représentation graphique de caractère, une unité de comparaison de coordonnées de caractère UC et une unité de données UD.

La mémoire M_EP est une mémoire non volatile par exemple EEPROM ou Flash pour notamment mémoriser le code personnel PIN uniquement connu de l'usager de la carte.

Selon une réalisation de l'invention, l'unité d'établissement UE comprend un mécanisme d'établissement ME d'une représentation graphique $REP_n$ d'un clavier numérique dont chaque touche du clavier comprend un ensemble de pixel identifié par des coordonnées numériques, l'indice n étant compris entre 1 et un entier N a priori grand. Par exemple,

les coordonnées numériques de chaque touche du clavier sur un plan à deux dimensions comprennent une abscisse et une ordonnée dans un repère de référence sur l'écran de l'unité d'affichage UA.

La représentation graphique est transmise et affichable à l'usager dans l'entité de traitement de code ETC et doit être uniquement interprétable par l'usager et non directement par le processeur P_ETC de l'entité de traitement. La représentation $REP_n$ a pour particularité de pouvoir être différente par exemple à chaque demande d'un code personnel par l'entité personnelle.

Selon une première réalisation montrée à la figure 3, la représentation graphique $REP_n$ est une table TB ayant un nombre prédéterminé de cases dont certaines sont similaires à des touches de clavier TC et associées respectivement à des caractères alphanumériques. Par exemple, les caractères alphanumériques sont dix chiffres et deux lettres selon la figure 3. Les touches sont disposées aléatoirement dans la table à chaque affichage de celle-ci à l'usager, suite à une demande de données secrètes. Le nombre de cases de la table, par exemple égal à 16, est supérieur ou égal au nombre prédéterminé de caractères alphanumériques, chiffres lettres et/ou symboles. Les caractères alphanumériques incluent au moins les caractères du code personnel qui peuvent être sélectionnés sur l'écran par l'usager, par exemple au moyen d'un clavier classique ou d'une souris de l'entité de traitement, ou tactilement.

Selon une deuxième réalisation montrée à la figure 4, la représentation graphique $REP_n$ occupe presqu'une page d'écran PG1 incluant plusieurs ensembles de caractères alphanumériques, par exemple

au nombre de trois EN, EI et EG ayant des polices différentes : normale, italique et gras. Les caractères alphanumériques dans les ensembles sont disposés aléatoirement dans la page d'écran PG1 à chaque affichage de celle-ci, suite à une demande des données secrètes. Les caractères alphanumériques des ensembles EN, EI et EG incluent au moins les caractères du code personnel qui peuvent être sélectionnés sur l'écran par l'usager. La représentation est associée à des consignes de sélection CS1 qui peuvent varier à chaque affichage de la représentation graphique à l'usager, suite à une demande des données secrètes. Les consignes CS1 sont, par exemple, "Pour la saisie et la sélection de votre code personnel, considérez uniquement les caractères en italique" et donc de l'ensemble EI, ou "Pour la saisie et la sélection de votre code personnel, considérez uniquement les caractères en gras" et donc de l'ensemble EG, ou "Saisissez votre premier et troisième caractères en italique, votre deuxième caractère en gras et votre quatrième caractère en police normale" pour un code personnel à quatre caractères.

Selon une troisième réalisation montrée à la figure 5, la représentation graphique $REP_n$ est une page d'écran PG2 incluant plusieurs ensembles distincts de caractère alphanumérique respectivement affichés dans des zones ayant des hachures différentes et incluant au moins les caractères du code personnel qui peuvent être sélectionnés sur l'écran par l'usager. Par exemple, les ensembles sont au nombre de huit et contiennent chacun des caractères alphanumériques prédéterminés, en l'occurrence 10 chiffres, suite à une demande des données secrètes. Quelques uns des ensembles de

caractère hachurés sont à sélectionner selon des consignes de sélection CS2 pour que l'usager sélectionne des caractères représentatifs du code personnel PIN dans les ensembles sélectionnés. Les consignes de sélection CS2 qui peuvent varier à chaque affichage de la page d'écran PG2 à l'usager sont par exemple :

"Veuillez sélectionner votre deuxième chiffre dans la zone à hachure horizontale, puis votre quatrième chiffre dans la zone à gauche de la zone à hachure en pointillé. Vous ne devez pas sélectionner votre premier chiffre dans une zone à hachure oblique. Sélectionnez dans la zone au-dessus de la zone à hachure en pointillé votre troisième chiffre et enfin le dernier chiffre de votre code dans la zone au-dessus de la zone à hachure horizontale."

En variante et relativement aux deuxième et troisième réalisations, les consignes peuvent être transmises oralement ou sous pli confidentiel à l'usager.

Chaque représentation graphique $REP_n$ établie par le mécanisme ME est associée dans la carte à des coordonnées exactes $CO_n$ de touches qui sont à sélectionner successivement en correspondance avec la suite de caractères successifs composant le code personnel PIN de l'usager. Par exemple, les coordonnées exactes de touches relatives à un code personnel à quatre caractères comprennent quatre jeux de coordonnées successifs correspondant respectivement aux quatre touches dont les dénominations représentent les quatre caractères du code personnel.

Selon une implémentation du mécanisme d'établissement ME dans l'unité d'établissement UE,

des représentations $REP_1$ à $REP_N$ sont enregistrées dans la mémoire M_EP et sont associées respectivement à des coordonnées exactes $CO_1$ à $CO_N$ de touches à sélectionner représentatives du code personnel PIN de l'usager. Le mécanisme ME sélectionne aléatoirement dans la mémoire M_EP une représentation $REP_n$, afin de l'afficher à l'usager dans l'entité de traitement ETC. La représentation $REP_n$ sélectionnée par le mécanisme ME est différente d'un affichage à l'autre.

En variante, le mécanisme ME génère aléatoirement une représentation $REP_n$ à afficher à l'usager dans l'entité de traitement ETC et détermine aléatoirement dans cette représentation les coordonnées exactes $CO_n$ représentatives du code personnel PIN de l'usager, par exemple à raison d'un chiffre par ensemble de 10 chiffres pour quatre ensembles de 10 chiffres choisis aléatoirement parmi huit ensembles selon la figure 5.

L'unité de comparaison UC compare des premières coordonnées exactes $CO_n$ associées à une représentation graphique de caractère établie par l'unité d'établissement UE à des deuxièmes coordonnées déterminées et transmises par l'entité de traitement représentatives du code personnel qui ont été sélectionnées par l'usager en fonction de la représentation graphique affichée par l'entité de traitement. Si les premières et deuxièmes coordonnées correspondent, l'accès aux données de l'unité de données UD est autorisé. Les premières et deuxièmes coordonnées sont mises en correspondance via une relation logique telle qu'une addition d'un coefficient ou une multiplication par un coefficient. En variante les premières et deuxièmes coordonnées sont identiques.

L'unité de données UD contrôle par exemple une opération telle qu'une détermination d'une signature SIG pour authentifier l'usager de l'entité EP ou l'incrémentation d'un compteur, et comprend des données personnelles de l'usager.

L'entité personnelle EP peut être une carte à puce incluse dans un ordinateur portable ou un terminal mobile, une carte de paiement, une carte de porte-monnaie électronique, une carte de santé, un passeport électronique, ou toute autre carte à microprocesseur associée à un terminal fixe ou mobile. L'entité personnelle EP peut être tout dispositif électronique personnel contenant des données dont un code personnel donne l'accès.

En se référant maintenant à la figure 6, la sécurisation du code personnel de l'usager de l'entité personnelle EP comprend les étapes E1 à E11.

A l'étape E1, l'usager sélectionne l'application cliente AP de l'entité de traitement ETC activée par le processeur P_ETC afin, par exemple, d'accéder à une ressource sécurisée dans le serveur de ressources. L'application AP ouvre un canal de communication avec le serveur via l'unité de transmission UTT de l'entité de traitement et demande l'accès à la ressource sécurisée souhaitée par l'usager dans le serveur de ressources. Pour authentifier l'usager et lui autoriser un accès à la ressource, le serveur de ressources demande à l'application AP de lui transmettre des données secrètes telles qu'une signature identifiant l'usager.

A l'étape E2, l'application AP fournit une requête RQ1 contenant une demande de signature D_SIG

à l'entité personnelle EP via les unités de transmission UTT et UTP de l'entité de traitement de code ETC et de l'entité personnelle EP.

A la réception de la requête RQ1, à l'étape E3, le processeur P_EP active l'unité d'établissement UE qui va traiter la demande D_SIG. Le mécanisme ME établit une représentation graphique $REP_n$, par exemple selon la première réalisation, en sélectionnant de manière aléatoire dans la mémoire M_EP de l'entité personnelle EP l'une REPn des représentations graphiques $REP_1$ à $REP_N$, et les coordonnées exactes associées $CO_n$ des touches à sélectionner par l'usager.

A l'étape E4 suite à une interrogation périodique de l'entité de traitement ETC, l'unité d'établissement produit une réponse RP1 contenant la représentation $REP_n$. La réponse RP1 est transmise à l'entité de traitement ETC via les unités de transmission UTP et UTT de l'entité personnelle EP et de l'entité de traitement ETC.

Le processeur P_ETC de l'entité de traitement met en veille l'application AP et active l'unité d'affichage UA qui traite la réponse RP1. A l'étape E5, l'unité d'affichage UA extrait de la réponse RP1 la représentation $REP_n$ et l'affiche. L'usager sélectionne au moyen de l'unité de sélection US les touches de la représentation affichée $REP_n$ dont les dénominations correspondent aux caractères CR du code personnel, en respectant d'éventuelles consignes de sélection associées à la représentation $REP_n$ et affichées, ou transmises oralement ou sous pli confidentiel.

A chaque caractère CR du code personnel saisi au moyen de l'unité de sélection US sur la représentation $REP_n$, l'unité de détermination UDt

activée par le processeur P_ETC détermine les coordonnées représentatives de la touche dont la zone active a été sélectionnée. A la fin de la sélection, l'unité de détermination comprend des coordonnées CO représentatives de l'ensemble des coordonnées des touches correspondant aux caractères du code personnel PIN de l'usager.

L'unité de détermination UDt introduit les coordonnées CO des touches sélectionnées dans une requête RQ2 transmise à la carte, à l'étape E7.

A l'étape E8, le processeur P_EP de la carte active l'unité de comparaison de la carte qui extrait de la requête les coordonnées CO fournies par l'entité de traitement et les compare aux coordonnées exactes $CO_n$ associées à la représentation $REP_n$. Si les coordonnées CO et $CO_n$ correspondent, le processeur P_EP de la carte active l'unité de données UD afin d'accéder à des données par exemple en déterminant une signature SIG, à l'étape E9.

A l'étape E10, l'unité de données UD produit et transmet une réponse RP2 incluant la signature déterminée SIG à l'entité de traitement ETC. A la réception de la réponse RP2 par l'entité de traitement à l'étape E11, le processeur P_ETC de l'entité de traitement ETC réveille l'application cliente AP, et lui fournit la signature SIG extraite de la réponse RP2. L'application AP continue son traitement, par exemple en transmettant au serveur de ressources la signature SIG.

Si à l'étape E8, les coordonnées CO et $CO_n$ ne correspondent pas, alors le processeur P_EP de l'entité personnelle reboucle le procédé sur l'étape E3 pour afficher la représentation graphique précédente ou bien établir une autre représentation graphique à transmettre à l'entité de traitement ETC,

en dépendance du nombre prédéterminé de demandes successives des données sans modification de la représentation graphique. En variante, le processeur P_EP de l'entité personnelle reboucle le procédé sur l'étape E6, représenté par un trait en pointillé, afin de demander à l'usager via l'unité d'affichage UA de sélectionner à nouveau le code personnel. Le nombre de boucles peut être limité.

En variante, si les coordonnées CO et $CO_n$ sont différentes, alors le processeur P_EP de la carte fournit à l'entité de traitement ETC une notification de refus du code personnel qui provoque l'affichage d'un message de refus.

L'invention décrite ici concerne un procédé, une entité personnelle EP telle qu'une carte à puce et une entité de traitement de code ETC telle qu'un terminal associée à l'entité personnelle. Selon une implémentation, les étapes du procédé de l'invention sont déterminées par les instructions de programmes d'ordinateur incorporés respectivement dans l'entité personnelle EP et dans l'entité de traitement ETC. Les programmes comportent des instructions de programme qui, lorsque lesdits programmes sont exécutés respectivement dans l'entité personnelle et dans l'entité de traitement de code dont le fonctionnement est alors commandé par l'exécution des programmes, réalisent les étapes du procédé selon l'invention.

En conséquence, l'invention s'applique également à des programmes d'ordinateur, notamment des programmes d'ordinateur enregistrés chacun sur ou dans un support d'informations lisible par un ordinateur et tout dispositif de traitements de données, adapté à mettre en œuvre l'invention. Ces

programmes peuvent utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable pour implémenter le procédé selon l'invention.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker les programmes. Par exemple, le support peut comporter un moyen de stockage ou support d'enregistrement sur lequel sont enregistrés les programmes d'ordinateur selon l'invention, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore une clé USB, ou un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Les programmes selon l'invention peuvent être en particulier téléchargés sur un réseau de type internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel les programmes sont incorporés, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution des procédés selon l'invention.

REVENDICATIONS

1 - Procédé pour sécuriser un code personnel d'un usager donnant accès à des données (SIG) incluses dans une entité personnelle (EP), caractérisé en ce qu'il comprend :

Un établissement et un affichage (E5) d'une représentation graphique ($REP_n$) comprenant des caractères (CR) représentatifs du code personnel et associée à au moins une consigne,

une sélection (E5) desdits caractères (CR) par l'usager sur la représentation graphique affichée en fonction de ladite au moins une consigne,

une comparaison (E8) des premières coordonnées associées aux caractères sélectionnés par l'usager à des deuxièmes coordonnées de caractères représentatifs du code personnel associées à la représentation graphique, et

une transmission (E10) des données si les premières et deuxièmes coordonnées correspondent.

2 - Procédé conforme à la revendication 1, comprenant un établissement (E3) de la représentation graphique de caractères ($REP_n$) modifiée après un nombre prédéterminé de demandes successives des données (D_SIG).

3 - Procédé conforme à la revendication 1 ou 2, selon lequel la représentation graphique ($REP_n$) est modifiée par une modification de la disposition des caractères.

4 - Procédé conforme à l'une des revendications 1 à 3, selon lequel la représentation graphique ($REP_n$) est une table (TB) ayant un nombre

prédéterminé de cases dont certaines sont associées respectivement à des caractères alphanumériques incluant les caractères (CR) du code personnel et sont disposées aléatoirement dans la table.

5 - Procédé conforme à l'une des revendications 1 à 3, selon lequel la représentation graphique ($REP_n$) comprend plusieurs ensembles distincts de caractère (PG1) dont un est à sélectionner selon les consignes pour que l'usager y sélectionne les caractères représentatifs du code personnel.

6 - Procédé conforme à l'une des revendications 1 à 3, selon lequel la représentation graphique ($REP_n$) comprend plusieurs ensembles de caractère (PG2) dont au moins deux sont à sélectionner selon les consignes pour que l'usager sélectionne les caractères représentatifs du code personnel dans les ensembles sélectionnés.

7 - Entité personnelle (EP) pour sécuriser un code personnel d'un usager donnant accès à des données (SIG) incluses dans l'entité personnelle (EP), caractérisée en ce qu'elle comprend :

Un moyen (UE) pour établir une représentation graphique ($REP_n$) comprenant des caractères (CR) représentatifs du code personnel et associée à au moins une consigne (CS1, CS2),

un moyen (UC) pour comparer des premières coordonnées (CO) associées à des caractères (CR) représentatifs du code personnel et sélectionnés par l'usager sur une représentation graphique ($REP_n$) affichée en fonction de ladite au moins une consigne à des deuxièmes coordonnées ($CO_n$) de caractères

représentatifs du code personnel associées à ladite représentation graphique, et

un moyen (UD-UTP) pour transmettre les données si les premières et deuxièmes coordonnées correspondent.

8 - Produit programme d'ordinateur comprenant des instructions de code qui, lorsque le programme est exécuté, réalise les étapes du procédé définies dans l'une des revendications 1 à 6.

FIG. 1

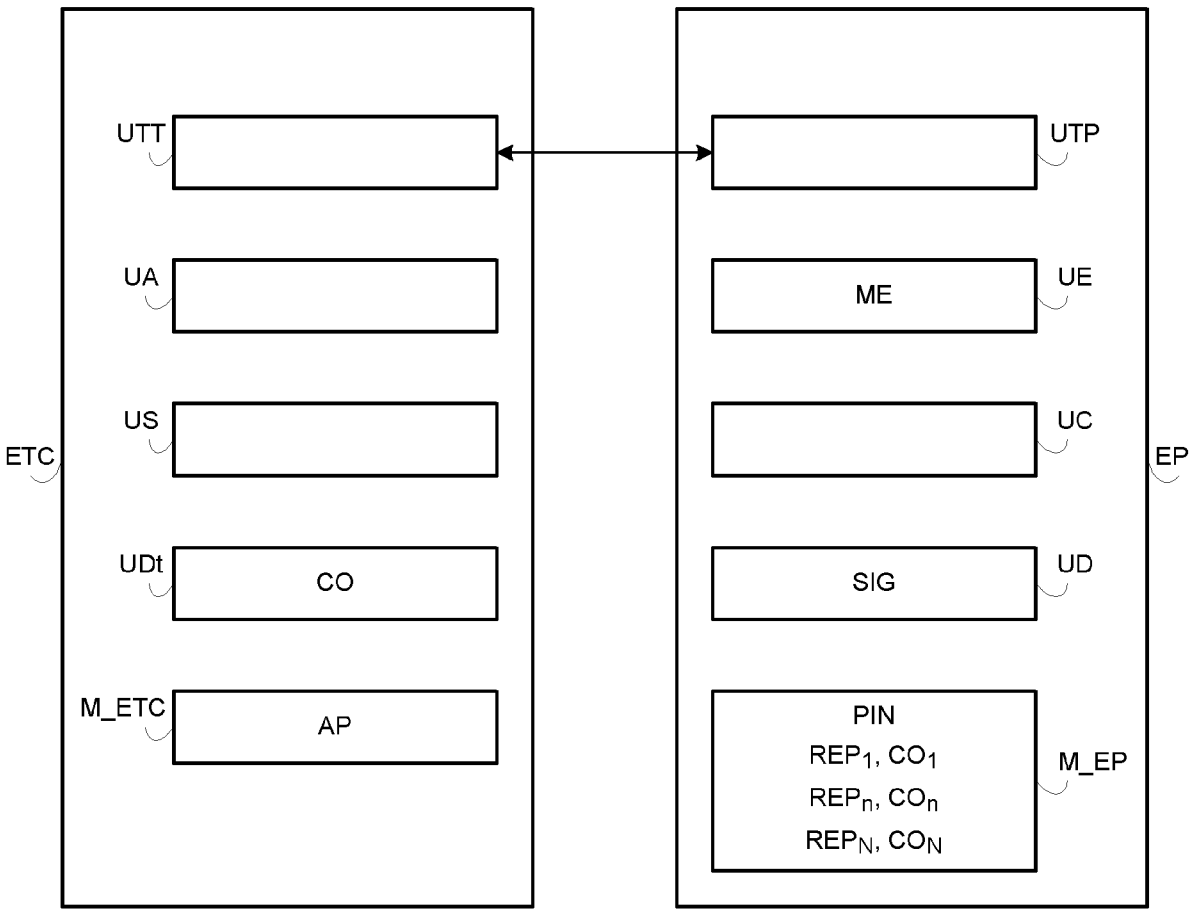

UTT
UTP
UA
ME
UE
US
UC
ETC
EP
UDt
CO
SIG
UD
M_ETC
AP
PIN
REP1, CO1
REPn, COn
REPN, CON
M_EP

FIG. 2

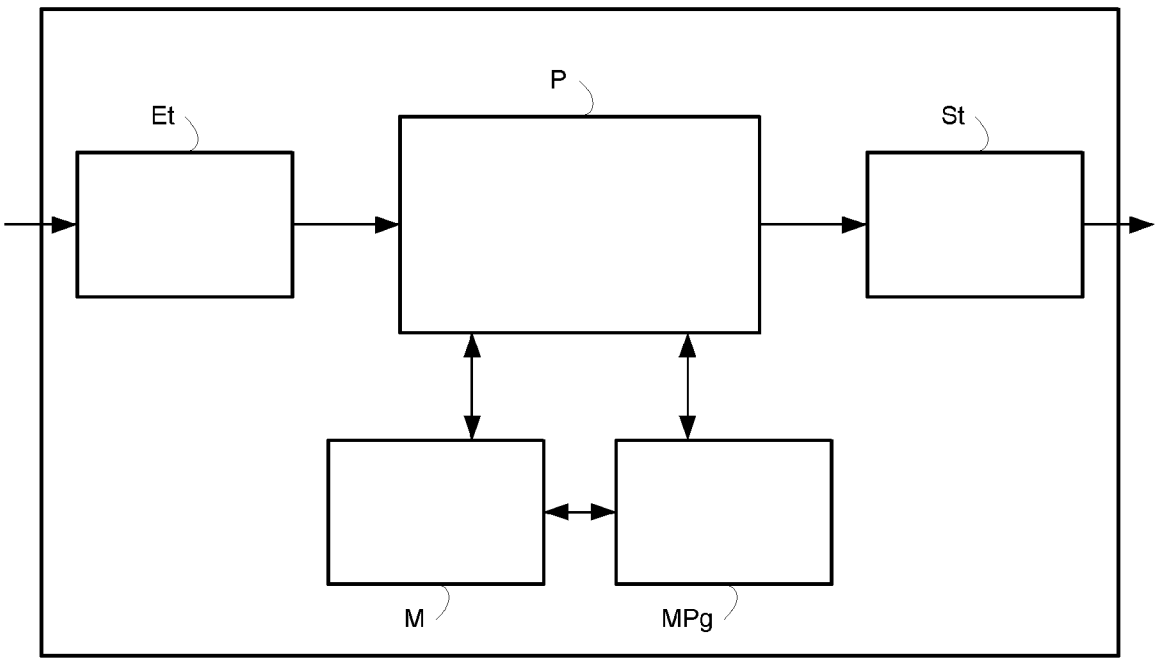


FIG. 3

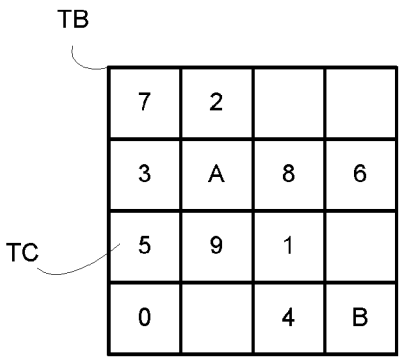

TB
TC
7 2
3 A 8 6
5 9 1
0 4 B

FIG. 4

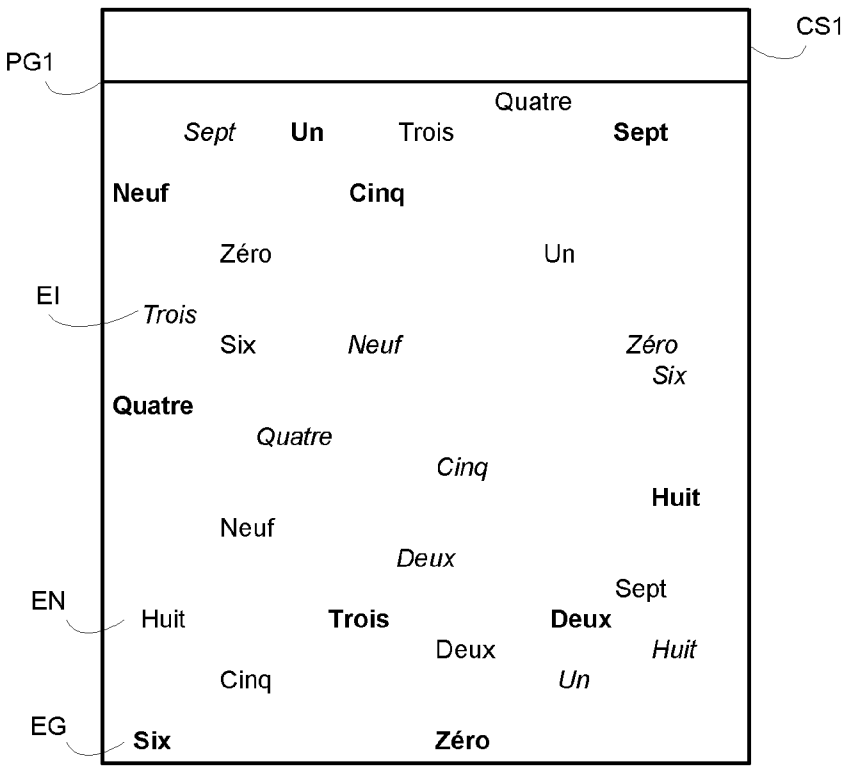
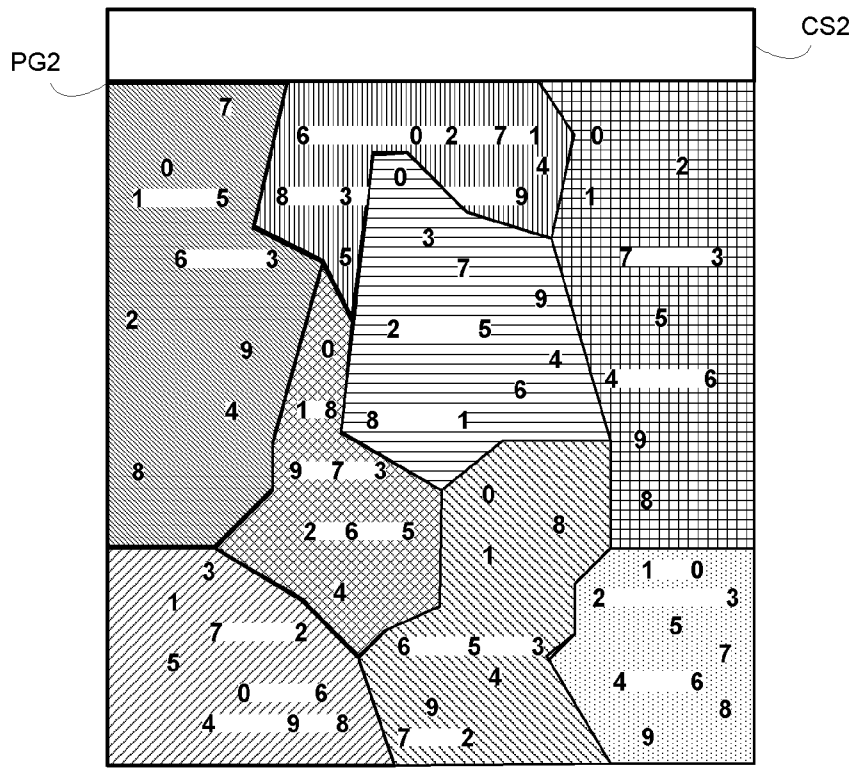
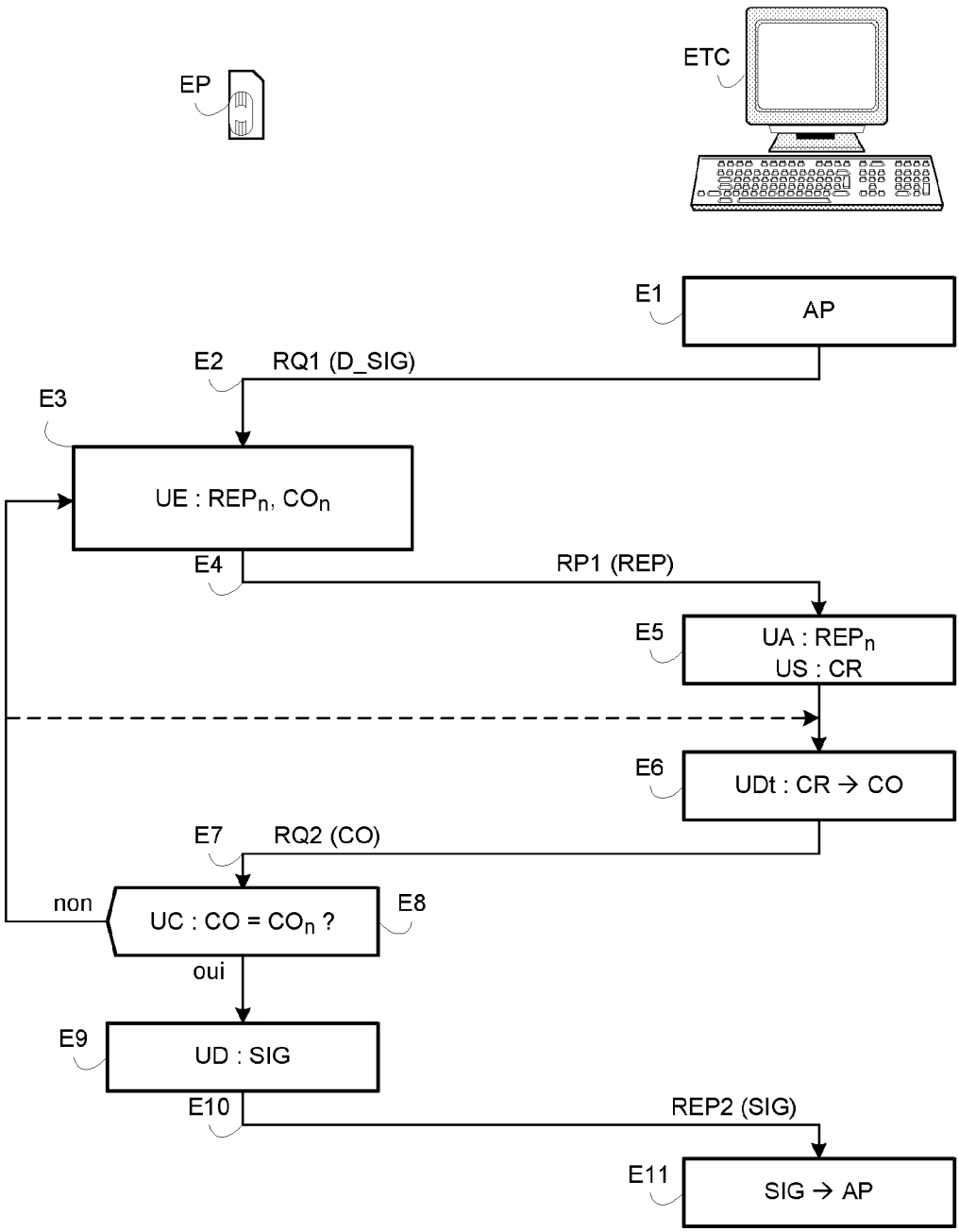

CS1
PG1
EI
EN
EG
Quatre
Sept Un Trois Sept
Neuf Cinq
Zéro Un
Trois
Six Neuf Zéro
Six
Quatre
Quatre
Cinq
Huit
Neuf
Deux
Sept
Huit Trois Deux
Deux Huit
Cinq Un
Six Zéro

FIG. 5



5/5

FIG. 6


EP
ETC
E1
AP
E2
RQ1 (D_SIG)
E3
UE : REPn, COn
E4
RP1 (REP)
E5
UA : REPn
US : CR
E6
UDt : CR → CO
E7
RQ2 (CO)
non
UC : CO = COn ?
E8
oui
E9
UD : SIG
E10
REP2 (SIG)
E11
SIG → AP