(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 961 330**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **10 02516**

(51) Int Cl[8] : ***G 06 Q 20/00*** *(2006.01), G 06 F 21/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 14.06.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 16.12.11 Bulletin 11/50.

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

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

(71) **Demandeur(s) :** *PAILLES JEAN CLAUDE* — FR.

(72) **Inventeur(s) :** PAILLES JEAN CLAUDE.

(73) **Titulaire(s) :** PAILLES JEAN CLAUDE.

(74) **Mandataire(s) :** PAILLES JEAN CLAUDE.

(54) PROCEDE DE SECURISATION DES INTERACTIONS UTILISATEUR SUR UN TERMINAL HOSTILE.

(57) Le domaine de l'invention est celui de la délivrance de biens ou de services sécurisés. Plus précisément, il concerne la sécurisation des interactions entre un utilisateur et un terminal personnel de cet utilisateur. Cette sécurisation est mise en oeuvre lors de la réalisation d'une transaction électronique entre l'utilisateur d'un terminal personnel et un prestataire. On considère comme terminal personnel un PC, un téléphone mobile ou tout équipement électronique pourvu d'une interface home-machine. On se place dans l'hypothèse d'un terminal personnel non sûr, car pouvant être affecté par des logiciels malicieux de type virus, mais disposant d'un « secure element » (SE) tel que par exemple une carte à puce. La figure ci-dessous illustre des attaques possibles sur ce type de terminal.

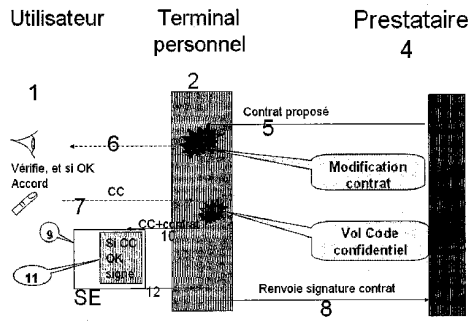

Figure 3 : attaques dans le terminal

FR 2 961 330 - A1

DESCRIPTION

Procédé de sécurisation des interactions utilisateur sur un terminal hostile

Le domaine de l'invention est celui de la délivrance de biens ou de services sécurisés. Plus précisément, il concerne la sécurisation des interactions entre un utilisateur et un terminal personnel de cet utilisateur. Cette sécurisation est mise en œuvre lors de la réalisation d'une transaction électronique entre l'utilisateur d'un terminal personnel et un prestataire. On considère comme terminal personnel un PC, un téléphone mobile ou tout équipement électronique pourvu d'une interface homme-machine. On se place dans l'hypothèse d'un terminal personnel non sûr, car pouvant être affecté par des logiciels malicieux de type virus.

Dans l'état de la technique, les transactions électroniques se conforment au modèle d'achat d'un bien ou d'un service décrit dans la figure 1, non limitatif de l'invention à savoir :

- L'utilisateur 1 (qui a un terminal personnel (2)) choisit un bien ou un service : ce choix peut se faire par exemple
  - pour le mode distant, dans un magasin virtuel au travers d'un réseau de communication (3) comme le réseau internet,; dans ce cas le terminal permet la « navigation » sur Internet par l'usage d'une application généralement nommée « browser »,
  - pour le mode local, dans un magasin réel, l'utilisateur paye à la caisse le bien, produit ou service choisit.
- Le terminal personnel reçoit un « contrat » (5) du prestataire (4) (dans notre exemple le prestataire est le marchand du bien ou du service en cours d'achat) , résumant les caractéristiques principales de la transaction, et l'affiche (6).
- L'utilisateur vérifie le contrat (6) au travers de l'interface homme/machine de son terminal personnel, s'il est d'accord, confirme son accord, en saisissant son code confidentiel de transaction (7) (dénommé CC dans la suite du document) sur l'interface homme/machine de son terminal personnel (par exemple le clavier de son téléphone). Il est le seul à connaître ce code, qui est généralement fourni par un prestataire ou opérateur de paiement, et cette action de saisie constitue donc une preuve de son accord.
- Le terminal personnel renvoie alors une signature (8) calculée après vérifications, notamment du CC. Cet accord peut avoir une valeur juridique probante dans certains types de transactions.

Ce modèle s'applique au paiement de contact ou à distance, à la signature électronique, aux enchères...etc. Dans le cas du paiement de contact, il faut un moyen de communication local entre le terminal personnel (le mobile) et le terminal prestataire qui peut être basé sur différentes technologies standardisées, telles que le NFC, Bluetooth , Zigbee, ou code barre 2D[1]... Dans la suite on évoque plutôt le NFC comme domaine privilégié d'application de l'invention, mais elle s'étend de façon immédiate aux domaines correspondants à ces autres technologies.

Une transaction se traduit donc par une signature électronique prouvant au marchand ou prestataire l'accord du client et engageant celui-ci. Le calcul de la signature, la vérification du

[1] NFC : Near Field Communication : technique standardisée conférant aux mobiles la capacité d'être utilisés comme une carte sans contact, ou un terminal sans contact
Bluetooth : www.bluetooth.org; Zigbee : http://www.zigbee.org/; code barre 2D ou Flashcode: :norme ISO/IEC 18004,

CC et des vérifications complémentaires peuvent être faites directement dans le terminal personnel. Cette vérification au niveau du terminal personnel est sujette à caution car les terminaux grands publics ne sont généralement pas des terminaux sécurisés du fait de leurs couts et de la complexité des composants constituants lesdits terminaux personnels, il est très difficile aujourd'hui d'évaluer sur le plan de leur sécurité intrinsèque les terminaux personnels, et ceux ci restent malheureusement exposés aux risques des logiciels malveillants, chevaux de troie, virus ou bot-net, etc.

Au niveau de l'état de l'art, on résout ce problème de sécurisation en adjoignant un « secure element » SE aux terminaux personnels, dans lequel seront confinés l'ensemble des éléments et tâches sensibles en termes de sécurité (clef de chiffrement et authentification, algorithme de chiffrement, PIN code etc...). Dans le cadre des terminaux personnels de type téléphones mobiles les SE les plus couramment utilisés sont les cartes USIM (sur une base UICC), ou les cartes SD^{tm} sécurisées. Avec les PC ce peut être une carte à puce traditionnelle si le PC a un lecteur de cartes adéquat, mais plus simplement ce peut être une clé USB de sécurité. Le SE peut également être partie intégrante du terminal, mais constitué de telle façon que ses données et programmes soient protégés : c'est le cas par exemple avec les normes TCG[2].

La figure 2 schématise un état de l'art des échanges pour la réalisation d'une transaction électronique(TE) entre le prestataire fournisseur du bien ou du service, le terminal personnel(2) et le SE (9) de l'utilisateur client (1) requérant la transaction électronique(TE), dans les deux cas : à gauche le terminal est un PC relié à un serveur prestataire via internet ; à droite le terminal est un mobile relié à un terminal prestataire lors d'une transaction NFC[3], ou relié à un serveur prestataire via internet. Ces deux cas sont équivalents du point de vue de la matière de l'invention. Le terminal reçoit de la part du prestataire un contrat décrivant la nature de la transaction (par exemple : achat d'un bien ou d'un service) et le présente à l'utilisateur sur son interface homme/machine. Le terminal, après saisie par l'utilisateur client sur l'interface homme/machine du terminal du CC, envoie au SE (9) et à l'application de signature (11) embarquée dans le SE, le CC accompagné du contrat, par le message (10); l'application (11) vérifie le CC , peut réaliser certains tests complémentaires dépendant de l'application considérée, puis calcule si le contrôle est positif une signature qu'il renvoie au terminal : message (12). Le terminal renvoie alors au serveur ou terminal prestataire cette signature par le message (8). Au niveau de l'état de l'art antérieur on constate que cette solution met à l'abri les données (clés, algorithmes, contrôles) les plus sensibles mais ne protège en rien l'ensemble de la réalisation de la transaction électronique contre des attaques par virus destinées par exemple à tromper l'utilisateur sur le montant qui va réellement lui être prélevé lors d'un paiement, ou des attaques destinées à lui voler son CC. Ce constat reste malheureusement valide lorsque l'on prend l'hypothèse que le SE est intrinsèquement sûr.

Dans la mesure où l'on ne peut avoir une confiance totale en le terminal, on peut alors craindre qu'il ne devienne la cible d'attaques par virus ou chevaux de Troie le transformant en terminal « hostile ». Au niveau de l'état de l'art antérieur, les attaques possibles sont de deux ordres, tel que représenté sur la figue 3 :

- Attaque sur l'intégrité du contrat, par exemple faire croire à l'utilisateur qu'il va payer 10€ alors que le montant de la transaction signée serait de 100€. C'est le cas dans la figure 3 si le contrat proposé en 5 stipule par exemple 100€, mais que le virus modifie le contrat affiché en 6 en changeant 100€ en 10 €. Pour être intéressante, ce type d'attaque doit se faire en collusion entre le prestataire et l'émetteur du virus, et ce scénario n'est pas

[2] TCG : Trusted Computing Group : http://www.trustedcomputinggroup.org/

[3] NFC : Near Field Communication : technique standardisée conférant aux mobiles la capacité d'être utilisés comme une carte sans contact, ou un terminal sans contact

totalement irréaliste, notamment avec la catégorie de virus appelés « botnet ». De plus, la simple possibilité technique de mener une telle attaque remettrait complètement en cause l'image de sécurité qui doit être attachée aux types de transactions considérés.

- Attaque sur la confidentialité CC, toute capture de ce CC au moment de la saisie de celui-ci par l'utilisateur sur l'interface homme/machine du terminal personnel à l'insu de l'utilisateur permet de « forcer » ou simuler son « accord » sur des transactions fictives. Dans ce cas, l'utilisateur n'a plus aucun contrôle sur les transactions qu'il génère involontairement !

Il est important de se protéger contre de telles attaques, qui peuvent paraître un peu théoriques, que l'on soit dans un contexte PC ou Mobiles. Même si leur mise en œuvre n'est pas simple, elles pourraient, par le biais des médias, résulter en une dégradation importante de la confiance du public, ou même remettre en cause certaines caractéristiques contractuelles des applications attaquées, et donc avoir des conséquences business extrêmement néfastes.

Le but de l'invention est de contrer les attaques décrites figure 3, sans imposer des contraintes particulières au terminal ni requérir l'usage de terminaux certifiés d'un point de vu sécurité. Au niveau de l'état de l'art antérieur, ce type de sécurisation mis en œuvre sans usage de terminaux certifiés est très difficile à réaliser et à déployer, les terminaux personnels de type mobile ou PC ne pouvant interdire le chargement et l'installation de logiciels applicatifs choisis par leur utilisateur ou un tiers malicieux (virus).

Dans l'invention on résout ce problème de sécurité transactionnelle en mettant en œuvre un concept de « Zone d'Interaction Sécurisée », dénommée ZIS, telle que représentée dans un exemple non limitatif de transaction d'achat d'un billet de train figure 7.
La ZIS est ici un objet graphique présenté sur l'écran du terminal de l'utilisateur, par exemple constituant une fenêtre graphique pour un terminal de type PC ou constituant un bandeau sur l'écran d'un terminal de type téléphone mobile. Cet objet graphique permet d'afficher le contenu du contrat relatif à une transaction d'achat d'un billet, ou tout au moins ses éléments importants :

- En y intégrant une variabilité de structure et de présentation entre deux transactions différentes, rendant son contenu non prédictible par un attaquant et donc en empêchant toute attaque automatisée contre l'usager du terminal (au travers d'un logiciel malicieux par exemple).
- En rendant difficile des modifications lors d'une attaque automatisée (par un logiciel malicieux dans le terminal) contre l'usager du terminal.
- Mais en gardant certaines caractéristiques de forme ou de présentation permettant une reconnaissance par l'utilisateur de la validité et de l'origine des informations de cette ZIS
- En permettant de plus à l'utilisateur de confirmer son accord par introduction de son code confidentiel de confirmation de transaction CC.

L'invention a donc pour objet un procédé de sécurisation de transaction électronique entre un utilisateur et un prestataire ledit procédé comportant au moins les étapes suivantes :

- L'émission par ledit prestataire par l'intermédiaire d'un contrat envoyé dans un message vers le terminal du dit utilisateur et transmis par le terminal à un élément de sécurité SE,
- Fourniture par ledit élément de sécurité SE des éléments de la transaction au terminal pour affichage à l'utilisateur et acceptation de la transaction,
- Collecte par ledit terminal de l'acceptation ou du refus par l'utilisateur du contrat proposé,

- Transmission par ledit terminal de l'acceptation vers l'élément de sécurité SE pour traitement en vue d'une émission d'un message d'acceptation signé (ou refus) , au travers du terminal, vers le prestataire

ledit procédé étant caractérisé en ce que :

- Le contrat fourni par le SE au terminal pour affichage à l'utilisateur est un objet graphique appelé ZIS, et conçu pour être protégé en intégrité,
- L'objet ZIS est constitué par un assemblage variable des représentations graphiques des éléments constitutifs du contrat entre le prestataire et l'utilisateur,
- L'objet ZIS est de plus perturbé par l'ajout d'éléments graphiques non constitutifs du contrat,
- l'élément de sécurité SE procède à une analyse de l'acceptation de l'utilisateur (ou du refus) et calcule le cas échéant un message de validation et d'acceptation signé de la transaction,

Dans une variante, le procédé selon l'invention est aussi caractérisé en ce que la ZIS peut être un objet multimédia non limité à des informations graphiques : son (pour vocaliser des champs tels que le montant) ou même vidéo (pour présenter par exemple des données du contrat telles que la description de la prestation achetée).

Différents modes de réalisation sont possibles, correspondant à différentes revendications secondaires ; ces différents modes sont :

- mode local : les traitements sont réalisés totalement dans le SE, ce qui suppose une architecture logicielle et une cinématique des échanges décrite ci-après ;
- la puissance de calcul du SE étant limitée, deux modes de réalisation optimisés dans ce cas sont décrits ci-après
- mode distant : les traitements sont réalisés dans un serveur distant, sur la demande du SE ce qui constitue un autre type de cinématique possible

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci sont présentées à titre indicatif et nullement limitatif de l'invention. Les figures montrent :

Figure 4 : le principe de réalisation de la ZIS : schématise les échanges entre prestataire, terminal, et SE liés au concept de ZIS, objet de l'invention.

Figure 5 : la cinématique des échanges dans le cas CS : détaille la figure 4 dans le cas du mode de saisie de l'acceptation sécurisée par le code secret CS.

Figure 6 : la cinématique des échanges dans le cas CVD : détaille la figure 4 dans le cas du mode de saisie de l'acceptation de l'utilisateur sur un clavier virtuel dynamique.

Figure 7 : un exemple de représentation graphique d'un contrat

Figure 8 : un exemple de deux transactions différentes sur les mobiles de deux utilisateurs différents, illustrant la variabilité/invariance de la ZIS

Figure 9 : Serveur distant pour le calcul de la ZIS, adaptant la cinématique de la figure 4 à ce cas particulier.

La ZIS est générée par un élément de confiance suite à la réception par celui-ci du message 5, message correspondant au contrat proposé par le prestataire. Cet élément de confiance est soit le SE lui-même, soit un serveur distant accessible par un moyen de communication du terminal de

l'utilisateur, ce moyen permettant d'établir un canal sécurisé entre le terminal de l'utilisateur et le SE lorsque le réseau de transport utilisé est ouvert et public comme les réseaux de type Internet.

Le format/structure de la ZIS (position des champs, fond, couleurs, orientations...) est variable pour chacun des utilisateurs pour chaque transaction. Dans une mise en œuvre alternative de l'invention la structure de la ZIS pourrait être définie par l'utilisateur, ce qui lui permettrait de participer à la vérification de l'authenticité et de l'intégrité des informations présentées dans la ZIS du fait du respect de la structure préalablement définie. Cette description spécifique de l'utilisateur impose alors au SE (qui est la propriété d'un utilisateur) ou au serveur distant (qui est commun à un ensemble d'utilisateurs) la gestion de données de format et de structure de la ZIS associée à cet utilisateur. Dans une mise en œuvre secondaire de l'invention une interface appropriée permet sur le terminal de l'utilisateur, après une phase d'authentification, de définir et structurer sa propre ZIS en y insérant les éléments de son choix, éléments correspondant aux capacités de génération par le SE des ZIS. L'objet de cette variation pour chacune des transactions de la structure de la ZIS est de rendre très difficile les attaques automatiques sur des formats non connus à priori et ne pouvant pas être prédits du fait des algorithmes de générations mis en œuvre par le composant SE.

L'invention repose donc sur un procédé de génération de l'objet ZIS et sa prise en compte dans les différentes étapes de la transaction : cet objet a donc les particularités suivantes :

a. une attaque de l'intégrité de la ZIS (par exemple pour modifier le montant ou description de la prestation) nécessiterait une analyse complexe pour en comprendre les différents champs de contenu, et réaliser des modifications pertinentes et consistantes.
b. Le contrôle de l'acceptation de l'utilisateur se fait grâce à un code confidentiel (CC) classique. Le vol de l'authentifiant de l'utilisateur (CC) est contré
    - o par l'utilisation d'un code secret CS généré aléatoirement par le SE, visualisé selon les principes a/ ci-dessus, et que seul l'utilisateur est capable de lire, et donc de taper sur le clavier en plus de son code confidentiel
    - o ou/et par une technique de saisie sur un clavier virtuel dynamique visualisé selon les principes a/ ci-dessus.

    Le choix de l'une ou l'autre des méthodes et de la valeur du CC se fait lors de l'enregistrement de l'utilisateur et la personnalisation du SE.

Plus précisément les caractéristiques suivantes sont appliquées:

Génération de la ZIS

- Le calcul de la ZIS par le SE (9) peut se limiter aux portions de la ZIS qui sont à protéger, de façon à minimiser les calculs à faire dans le SE (9).
- La ZIS (ou les portions de la ZIS à protéger) est un objet graphique sur l'écran du terminal personnel, reprenant entre autres principes les notions de « captcha » ; la cinématique associée est décrite par la figure 4
- Elle est générée par le SE (9), qui est un élément de confiance, par une application Appli_ZIS (14) s'exécutant dans le SE (9) qui reçoit le contrat grâce au message (13) envoyé par le terminal au SE (9) après réception du message (5) contenant le contrat envoyé par le prestataire (4) au terminal (2). Elle est envoyée par le SE (9) au terminal (2) sous forme d'une suite de pixels, afin de rendre difficile pour un virus dans le terminal (2) toute modification significative .
- La ZIS est authentifiable par le client grâce à ses propriétés graphiques

- Elle ne peut être modifiée par un virus dans le terminal:
  - Une modification significative nécessiterait une compréhension des informations dans la fenêtre
  - Ceci nécessiterait une analyse de l'image, segmentation/ transformation 2D/séparation des champs, et reconnaissance de caractères dans des temps limités à quelques secondes qui est le délai maximum que doit respecter l'utilisateur pour accepter ou refuser le contrat.

Confirmation de l'accord :

Selon la figure 4, si l'utilisateur est d'accord, il fournit à son terminal le code confidentiel CC (message 7). Le SE (9) contient une application Appli_ZIS (11) qui contrôle le CC, effectue certains contrôles complémentaires propres à l'application considérée, et calcule la signature qu'il renvoie au terminal par le message (12) . L'invention décrit deux méthodes pour la saisie et le contrôle du code confidentiel, et qui toutes deux préviennent une attaque de type vol du CC, correspondant à deux modes de réalisation de l'invention décrits ci-dessous. Ces deux méthodes peuvent être utilisées simultanément.

- **Code secret CS :**
  Les interactions relatives à ce mode sont décrites figure 5. Un code secret CS est généré aléatoirement en même temps que la ZIS par l'application Appli_ZIS (14) dans le SE (9). L'Appli_ZIS envoie à l'Appli_SIG par le message (16) les données nécessaires pour conclure la transaction, donc valeur du CS généré et les données du contrat obtenues en (13). Le CS fait partie des éléments graphiques de la ZIS, et ne peut donc être lu par un virus dans le terminal. La ZIS et ce CS sont transmis au terminal par le message (15), et le terminal l'affiche sur l'écran : (6). La figure 7 donne un exemple de représentation graphique de la ZIS où apparaît le CS avec la valeur « 143 » ; mais un autre utilisateur pourrait avoir une ZIS totalement différente du point de vue du fond et de la présentation des différents champs.
  - L'utilisateur s'il est d'accord renseigne les champs CC et CS (avec ce qu'il lit sur l'écran : « 143 ») : message (7)
  - Le SE contrôle CC (donnée permanente enregistrée à la personnalisation) et le CS (donnée générée par l'application Appli_ZIS (14) et envoyée à l'application Appli_SIG (11) dans le message (16) . Si un virus « vole » le CC, le CS étant variable à chaque transaction, ce virus ne peut seul « forcer » l'accord du client. L'application (11) peut réaliser des contrôles ou traitements complémentaires spécifiques du type de transaction, puis elle élabore une signature des éléments du contrat reçus dans le message (16). Cette signature vaut accord de l'utilisateur, et est envoyée en (12) au terminal, qui la renvoie en (8) au prestataire
  - notons de plus que cette façon de procéder permet aussi de contrer une attaque par rejeu : le logiciel malveillant dans le terminal (2) ré-utiliserait une ZIS d'une transaction précédente, puisque le CS change à chaque transaction. C'est la raison pour laquelle elle peut aussi être utilisée avec la méthode décrite ci-après.

  Ce procédé s'adapte aisément au cas où le CC est remplacé par une caractéristique biométrique propre à l'utilisateur, mesurée sur le terminal. Dans les messages (7) et (10), il faut alors remplacer la donnée CC par une donnée caractéristique de la donnée biométrique mesurée, et qui est vérifiée par l'application Appli_SIG (11). Des exemples de caractéristique biométrique particulièrement adaptée au contexte de l'invention sont l'empreinte digitale, la dynamique de frappe au clavier, la reconnaissance de visage....

- **Clavier virtuel dynamique (CVD)**

De façon à éviter l'espionnage par un logiciel malveillant des caractères du CC saisis sur le clavier du terminal, on utilise ici un clavier dynamique (la position des touches est varaible à chaque transaction) dessiné sur l'écran du terminal (2) à l'intérieur de la ZIS. Ce mode de réalisation peut être combiné avec le mode précédent.

- Le clavier dynamique (c'est-à-dire l'ordre des touches du clavier numérique affiché à l'écran) est généré aléatoirement dans le SE (9) par l'application Appli_ZIS (14) et transmis au terminal (message 15) ; le terminal affiche la fenêtre graphique et le clavier dynamique sur l'écran : 6. L'Appli_ZIS envoie à l'Appli_SIG par le message (16) les données nécessaires pour conclure la transaction, donc la description du CVD généré et les données du contrat obtenues en (13).
- L'utilisateur, s'il est d'accord, saisit en (7) son CC sur le clavier virtuel. Le terminal transmet les positions des clics (coordonnées x,y des clics) en (10). Les positions des clics sont reconnues par l'application Appli_SIG (11) par rapport au clavier dynamique généré dans l'étape précédente par l'Appli_ZIS (14), et envoyé à l'application (11) par le message (16). Il s'agit par exemple d'une table contenant un ensemble d'éléments {symbole ; position x,y ; dimension touche} où symbole est un des symboles { 1 2 3 4 5 .....} . L'application (11) en déduit donc les chiffres du CC tapé par l'utilisateur, qu'elle compare au CC enregistré à la personnalisation du SE.
- Si ce contrôle du CC est positif, l'application Appli_SIG (11) peut réaliser des contrôles ou traitements complémentaires spécifiques du type de transaction, puis elle élabore une signature des éléments du contrat reçus dans le message (16). Cette signature vaut accord de l'utilisateur, et est envoyée en (12) au terminal, qui la renvoie en (8) au prestataire

Génération de la fenêtre graphique

Pour rendre la reconnaissance et la modification par software dans le terminal (2) difficile, une ou plusieurs des méthodes suivantes peuvent être utilisées, tel que représenté sur la figure 7 . Les caractéristiques de la ZIS sont variables en fonction de l'utilisateur, qui peut en choisir certaines ; elles sont fixées lors de la personnalisation du SE pour un utilisateur donné :

- ordre et position des champs,
- polices de caractère utilisées,
- orientation caractère de certains champs, espacement, superposition
- fond : motif se mélangeant (notamment même couleur) que les textes dont la reconnaissance doit être empêchée.
- redondance (par exemple le montant qui est un champ particulièrement important peut être dupliqué) ; ainsi une modification partielle par un virus serait détectée par l'utilisateur qui verrait que les deux montants ne sont pas identiques)
- dessin par l'utilisateur de sa propre police de caractère (c'est le cas de la figure 7 pour les champs montant et code de sécurité).
- Perturbation aléatoire pour éviter que des logiciels malveillants puissent agir par corrélation/reconnaissance de forme (cas de la figure 7)

Dépendance du mobile et indépendance de la transaction

La sécurité de la ZIS nécessite que l'utilisateur ait une connaissance préalable de sa présentation à l'écran, afin de détecter toute tentative d'attaque par un virus qui utiliserait une ZIS standard.

Donc la ZIS s'affiche tel que représenté sur la figure 8, et dans le cas du mode de réalisation de la protection du code confidentiel basé sur le CS (l'adaptation à l'autre mode (CVD) est immédiate).

- De façon spécifique pour chaque utilisateur : des couleurs, des textures, des formes de la ZIS varient d'un mobile à l'autre : par exemple la clé qui symbolise une

transaction sécurisée apparaît dans une couleur et une position différente sur les mobiles des utilisateurs 1 et 2 de la figure 8. Ces caractéristiques sont donc dépendantes du mobile de l'utilisateur considéré.

- Pour un utilisateur, de façon semblable d'une transaction à l'autre. donc l'utilisateur pourra reconnaître des couleurs, des textures, des formes qu'il retrouve à chaque transaction, comme représenté à la figure 8
- Notons que ces principes de bon sens n'empêchent pas d'introduire des perturbations graphiques dans la ZIS pour un utilisateur donné et diverses transactions, dans le but d'éviter des attaques par corrélation.
- Le seul principe à respecter est que ces variations n'empêchent pas l'utilisateur de détecter un comportement anormal des logiciels de traitement des transactions, révélant une attaque. Un exemple est donné figure 7. les zones montant et CS utilisent une police de caractère spécifique à l'utilisateur, sur un fond de motif variable, et de plus, des trait variables se superposent à ces zones sans en altérer la lisibilité par un oeil humain, tout en rendant toute corrélation et reconnaissance de caractère quasi impossible.

L'ensemble des paramètres correspondant aux caractéristiques de la ZIS invariantes pour un utilisateur donné, sont inscrites lors de l'enregistrement de cet utilisateur, dans son SE.

Une variante de l'invention utilise l'audio

Il est possible en plus ou en remplacement d'afficher le contrat sur l'écran PC ou Mobile, de vocaliser certains de ses champs. Cette vocalisation doit être faite au maximum dans le SE, qui doit envoyer au terminal des indications sur les formants des messages à prononcer, donc un ensemble (ton, durée, transition avec le phonème suivant). C'est la raison pour laquelle on se limite en pratique à la vocalisation de champs numériques tels que le montant financier, car une synthèse alphanumérique complète du contrat serait en dehors des possibilités du SE.

Là aussi il est nécessaire de garder le principe de la dépendance du mobile et d'indépendance de la transaction : le bruit de fond, la tonalité utilisée.., seront spécifiques d'un utilisateur particulier, et permettront donc à celui-ci d'être alerté par tout changement par rapport à ce à quoi il est habitué.

La confirmation de l'accord de l'utilisateur est identique à ce qui est décrit précédemment.

Une autre variante de l'invention utilise la vidéo

Certains champs peuvent être présentés avec défilement, selon des paramètres imposés par le SE au terminal.

La confirmation de l'accord de l'utilisateur est identique à ce qui est décrit précédemment

Un mode de réalisation de l'invention se base sur les principes suivants pour calculer la ZIS dans le SE (9) par l'application (14)

Afin de limiter la charge de calculs du SE (qui est une simple puce de carte à puce) qui pourraient être rédhibitoire sans une implémentation appropriée. Par ailleurs, ce traitement peut se limiter à la portion de la ZIS qui doit être protégée, le reste pouvant être fait dans le terminal : dans la figure 7, seuls deux champs sont protégés : le montant, et le CS auquel est rajouté le montant

- Les données graphiques sont figées à la personnalisation de la puce, puisque ces données sont constantes pour un utilisateur donné. Ces données sont :
  a. Taille de la fenêtre ZIS (ou de la portion de ZIS) : n, m
  b. Fond : n. m pixels

c. Les paramètres d'un champ sont :
    1. Son identifiant
    2. Position de l'origine du champ dans la ZIS (ou de la portion de ZIS),
    3. police de caractères utilisée,
    4. nombre de caractères,
    5. dx,dy = valeurs de décalage entre caractères (dy=0 pour une variation horizontale)
    6. orientation du caractère (parmi un nombre restreint d'orientations : -20°, 0°,+20°)
d. Police de caractères : on se limite par exemple aux dix chiffres pour le montant d'une transaction de paiement, ou le CS. Lorsque des orientations variables sont permises, (3 dans le cas précédent) la police est décrite autant de fois que de possibilité (trois) dans le cas précédent.
    1. Dimension rectangle contenant les caractères
    2. Valeurs des pixels du rectangle

- Il n'y a pas de transformation géométrique à effectuer lors de la transaction (translation, rotation, échelle) : en effet, le calcul des pixels de la ZIS (ou de la portion de ZIS)
- Affichage : c'est une simple fonction d'assemblage qui se base sur une primitive de calcul de pixel de position (x,y) dans la ZIS (ou de la portion de ZIS)
    - en déduire avec les paramètres c2 et c5 le champ concerné, et s'il n'y en a pas, en déduire le pixel avec le paramètre b, et fin
    - en déduire le caractère concerné avec le paramètre c5
    - avec les paramètres c3 et c6 en déduire le pictogramme du caractère
    - en déduire avec le paramètre d1 les coordonnées relatives x' y' par rapport au caractère
    - avec le paramètre d2, calculer pixel avec le pixel du caractère ou le pixel (x,y) du fond si le pixel n'est pas sur le tracé du caractère.
    - Fin : passer au pixel suivant : si x<n, (x+1,y), et sinon si y<m, (0,y+1) ou sinon le calcul de la ZIS (ou de la portion de ZIS) est terminé.

Un autre mode de réalisation :

Il se base sur la création par l'utilisateur de sa propre police de caractères : il dessine sur un moyen d'entrée graphique les symboles graphiques représentant les 10 chiffres. Ceci peut se faire facilement sur n'importe quel « smart-phone », puisque leurs écrans sont graphiques et pointables avec un stylet.

On comprend que ce mode de réalisation répond bien au principe de dépendance du mobile et indépendance des transactions, permettant à l'utilisateur de détecter toute présence de logiciel malveillant. En effet aucun algorithme de reconnaissance de caractères utilisé par ce logiciel malveillant ne peut fonctionner avec des polices de caractère totalement imprévisibles, comme c'est bien le cas dans cette variante.

La figure 7 se place dans cette hypothèse : on voit que les chiffres qui apparaissent dans le montant et le CS ne correspondent pas à des polices habituelles !

Cas de l'audio

Etant donné le contexte très limité de synthèse vocale dans lequel on se place (vocalisation uniquement de données numériques) la technique des « phonèmes » est classique et éprouvée, et implémentable dans un SE.

Implémentation distante grâce à un canal sécurisé avec un serveur de confiance

Le SE, dans le cas de la SIM, peut établir une communication sécurisée avec un serveur distant, comme présenté sur la figure 9. Cette sécurité s'entend de bout en bout . Les standards ETSI ETSI TS 102 484 V7.1.0 (2008-07) *Technical Specification :* Smart Cards; Secure channel between a UICC and an end-point terminal décrivent une telle possibilité, et ETSI TS 102 225 *Technical Specification* Smart Cards; Secured packet structure for UICC based applications décrivent cette fonctionnalité.

La ZIS peut donc être réalisée non par le SE lui-même, mais par un serveur de confiance (17), non attaquable, avec lequel le SE et le terminal communiquent via le réseau internet filaire (cas des PCs) ou radio (cas des mobiles) :

- Le SE établit un canal sécurisé (18) de bout en bout, à travers le terminal, permettant de véhiculer du SE vers le serveur les données du contrat en toute sécurité, ainsi que la description du CVD ou la valeur du CS générés par l'Appli_ZIS (14). Le vol de ces données permettrait à un logiciel malveillant sur le terminal (2) de forcer l'accord de l'utilisateur, d'où l'importance du canal sécurisé à ce niveau.
- Le serveur renvoie (19) vers le terminal de visualisation les données graphiques de la ZIS (sans sécurité, à ce niveau, du fait des propriétés d'intégrité de la ZIS décrites précédemment)
- Le terminal affiche la ZIS : (6).
- Le reste des échanges est identique aux cinématiques précédentes.

Notons que cette variante s'adapte bien au cas d'une ZIS multimédia, car dans ce cas, la puissance de calcul du serveur peut s'accommoder d'une absence totale de restriction en ce qui concerne le format multimédia utilisé. Le message 19 peut être une vidéo avec le son associé, envoyé dans un des formats classiques existant sur Internet.

Revendications

1. Procédé de sécurisation de transaction électronique entre un utilisateur (1) et un prestataire (4), ledit procédé comportant au moins les étapes suivantes :

   - L'émission par ledit prestataire (4) d'un contrat envoyé dans un message (5) vers le terminal (2) du dit utilisateur (1) et transmis par le terminal (2) grâce à un message (13) à un élément de sécurité SE (9),
   - Renvoi par ledit élément de sécurité SE (9) des éléments de la transaction au terminal (2) dans un message (15) pour affichage (6) par le terminal (2) vers l'utilisateur (1) et acceptation (ou refus) (7) par celui-ci de la transaction,
   - Saisie sur ledit terminal (2) de l'acceptation (ou du refus) (7) par l'utilisateur (1) du contrat affiché en (6),
   - Transmission par ledit terminal (2) de l'acceptation (ou du refus) (10) vers l'élément de sécurité SE pour traitement en vue d'une émission d'un message d'acceptation signé (ou refus) (12) vers le terminal (2), puis (8) du terminal (2) vers le prestataire (4).

ledit procédé étant caractérisé en ce que :

   - Le contrat fourni (15) par le SE (9) au terminal (2) pour affichage à l'utilisateur est un objet graphique appelé ZIS, et conçu pour être protégé en intégrité,
   - L'objet ZIS est constitué par un assemblage variable des représentations graphiques des éléments constitutifs du contrat (5) entre le prestataire (4) et l'utilisateur (1),
   - L'objet ZIS est de plus perturbé par l'ajout d'éléments graphiques non constitutifs du contrat,
   - l'élément de sécurité SE procède à une analyse de l'acceptation de l'utilisateur (ou du refus) et calcule le cas échéant un message de validation et d'acceptation signé de la transaction (12)
   - la cohérence avec les éléments constitutifs du contrat affichés dans la ZIS et l'acceptation signée est assurée par le SE.

2- Procédé selon la revendication 1, caractérisé en ce que ladite étape de calcul de la ZIS par le SE se limite aux portions de la ZIS qui sont à protéger.

3- Procédé selon les revendications 1 à 2 caractérisé en ce que ladite étape d'acceptation des termes du contrat (5) présenté en (6) à l'utilisateur (1) sur l'écran du terminal (2) comprend une étape de saisie (7) d'un code confidentiel (CC) par l'utilisateur (1). Le CC et son mode de contrôle décrit ci-après sont des données de personnalisation du SE (9).

4- Procédé selon les revendications 1 à 3 caractérisé en ce que la protection de la ZIS (ou d'une portion de la ZIS) contre des modifications malveillantes par des logiciels dans le terminal (2) est assurée par au moins un des éléments suivants :

   - la portion de la ZIS à protéger est représentée au moyen de formats et de particularités graphiques aléatoires, ainsi qu'un sous ensemble des éléments constitutifs du contrat dont la représentation dépend de choix pré-établis par l'utilisateur.
   - La portion de ZIS à protéger est envoyée en (15) par le SE (9) pour être visualisée par le terminal (2) sous forme d'une suite de pixels.
   - la ZIS est facilement interprétée par l'utilisateur, mais un logiciel malveillant dans le terminal (2) peut très difficilement la modifier sans alerter l'utilisateur (1).

5- Procédé selon les revendications 1 à 4, caractérisé en ce que la phase d'acceptation par le client de la transaction proposée est enrichie des étapes suivantes :

- L'application Appli_ZIS (14) du SE (9) ajoute à la ZIS un code de sécurité (CS) qu'elle a chois aléatoirement pour la transaction en cours,
- l'application Appli_ZIS (14) envoie par un message (16) la valeur du code de sécurité CS à l'application signature (11).
- Le code CS est lu et saisi par l'utilisateur en (7) lors de la phase d'acceptation.
- L'application de signature reçoit en (10) les CC et CS introduits en (7) par l'utilisateur et contrôle le CC d'après les données de personnalisation du SE (9) et le CS par rapport au CS contenu dans le message (16).

6- Procédé selon la revendication 5 caractérisé en ce que la phase d'acceptation par l'utilisateur utilise une technique biométrique en lieu et place du CC.

7- Procédé selon les revendications 1 à 4, caractérisé en ce que la phase d'acceptation par le client de la transaction proposée correspond aux étapes suivantes :

- les éléments d'un CVD (clavier virtuel dynamique, dont le positionnement des touches est variable aléatoirement à chaque transaction) sont générés dans le SE (9) par l'application Appli_ZIS (14) dans les éléments constitutifs de la ZIS.
- L'application Appli_ZIS (14) transmet les indications sur la position des touches virtuelles à l'application signature (11) du SE (9) par le message (16).
- La saisie sur le clavier virtuel dynamique du CC (7) se traduit par une série de « clics » dont les coordonnées sur l'écran sont transmises en (10) à l'application signature (11).
- L'application de signature contrôle l'acceptation de l'utilisateur par la correspondance entre la position des « clics » collectés et ceux provenant du message 16.

8-Procédé selon les revendications 1 à 7, caractérisé en ce que l'application Appli_ZIS (14) implémente une technique de minimisation des traitements graphiques pour le calcul de la ZIS (ou des parties protégées de la ZIS) basée sur l'assemblage de pixels provenant de différentes zones rectangulaires, sans calculs géométriques complexes, et utilise des données de personnalisation introduites dans le SE (9) de façon spécifique à un utilisateur (1) donné :

- représentation graphique des chiffres ou lettres utilisés dans la ZIS
- choix parmi une pluralité de choix possibles de caractéristiques de constitution de la ZIS

9- Procédé selon les revendications 1à 7, caractérisé en ce que toute ou partie des informations de la ZIS sont présentées sous une forme audio à l'utilisateur.

10- Procédé selon les revendications 1à 7, caractérisé en ce que ladite étape de calcul de la ZIS par le SE(9) est sous-traitée à un serveur de confiance externe au travers des étapes suivantes :

- établissement d'un canal sécurisé (18) entre le SE (9) et un serveur externe (17)
- émission sur ce canal par le SE (9) vers le serveur externe (17) des données du contrat proposé en (5) et reçues du terminal en (13).
- émission du serveur externe (17) vers le terminal (2) par le message (19) des données graphiques de la ZIS.
- émission du serveur (17) vers le SE (9) des données de sécurisation de la saisie du CC, selon les revendications 5 ou 6. à travers le canal sécurisé (18).

11- Procédé selon les revendication 1 à 7 et 10, caractérisé en ce que la ZIS calculée par le serveur ZIS (17) peut être un objet multimédia (audio, et/ou image fixe et/ou vidéo), sans aucune des restrictions nécessitées par les éventuelles faibles capacités de calcul des SE.

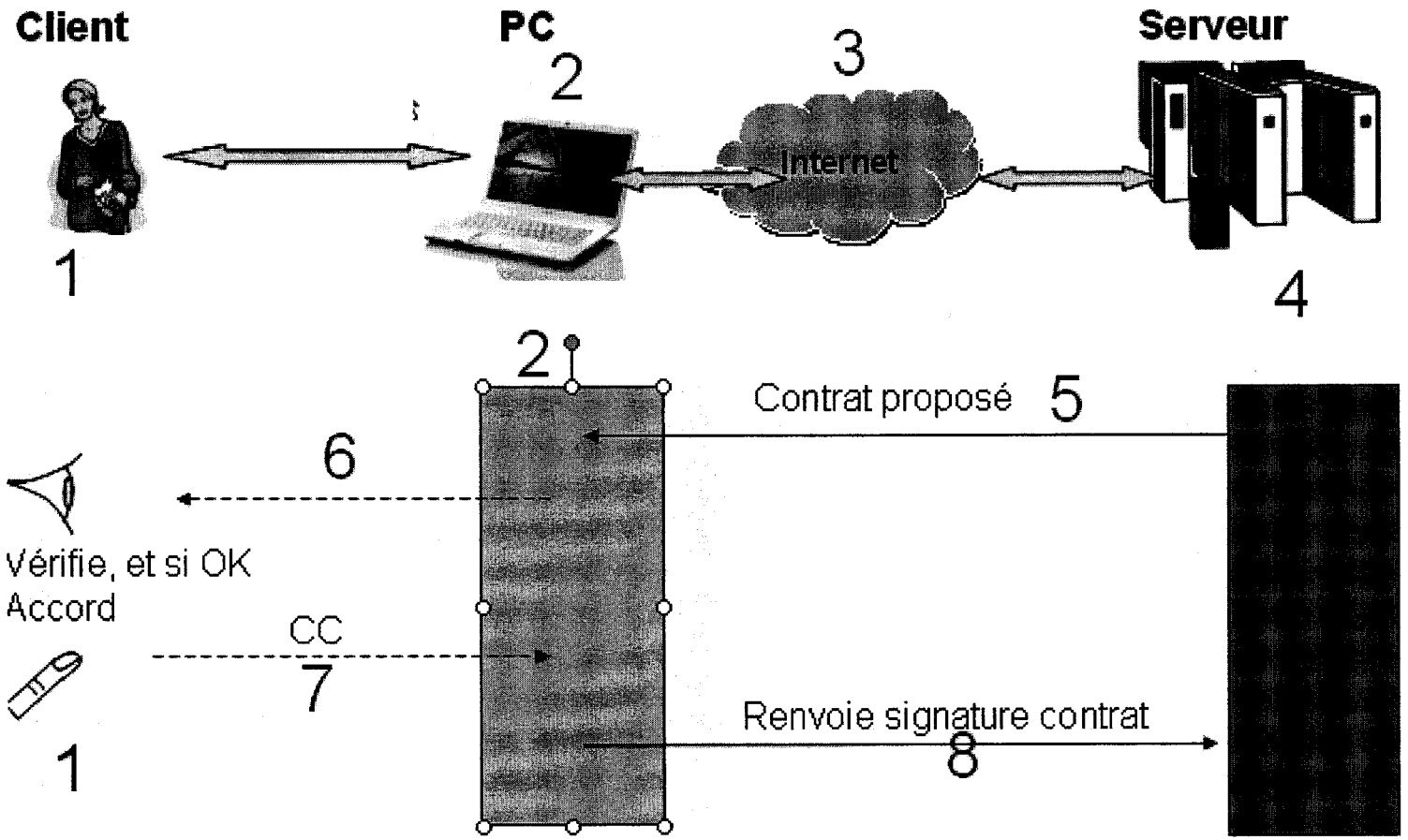

Figure 1 : modèle de transaction

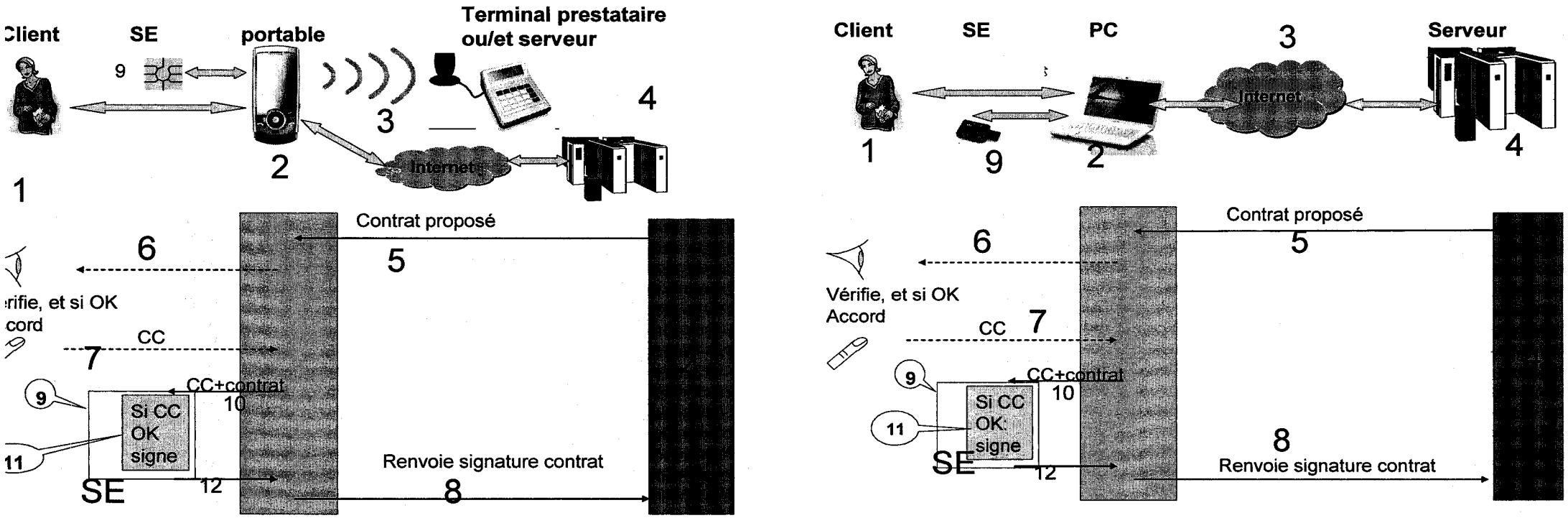

Figure 2 : organisation de transactions électroniques typiques

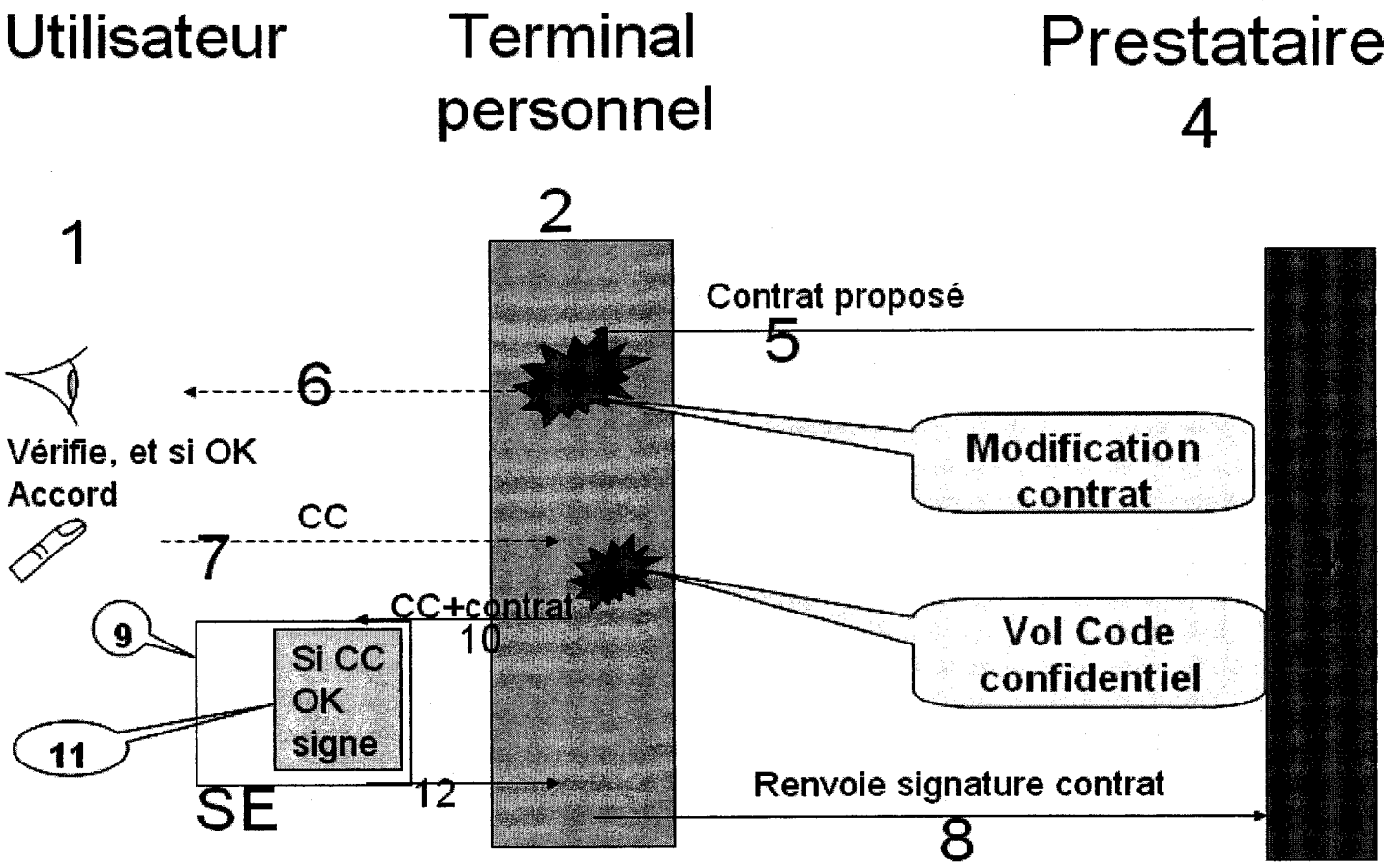

Figure 3 : attaques dans le terminal

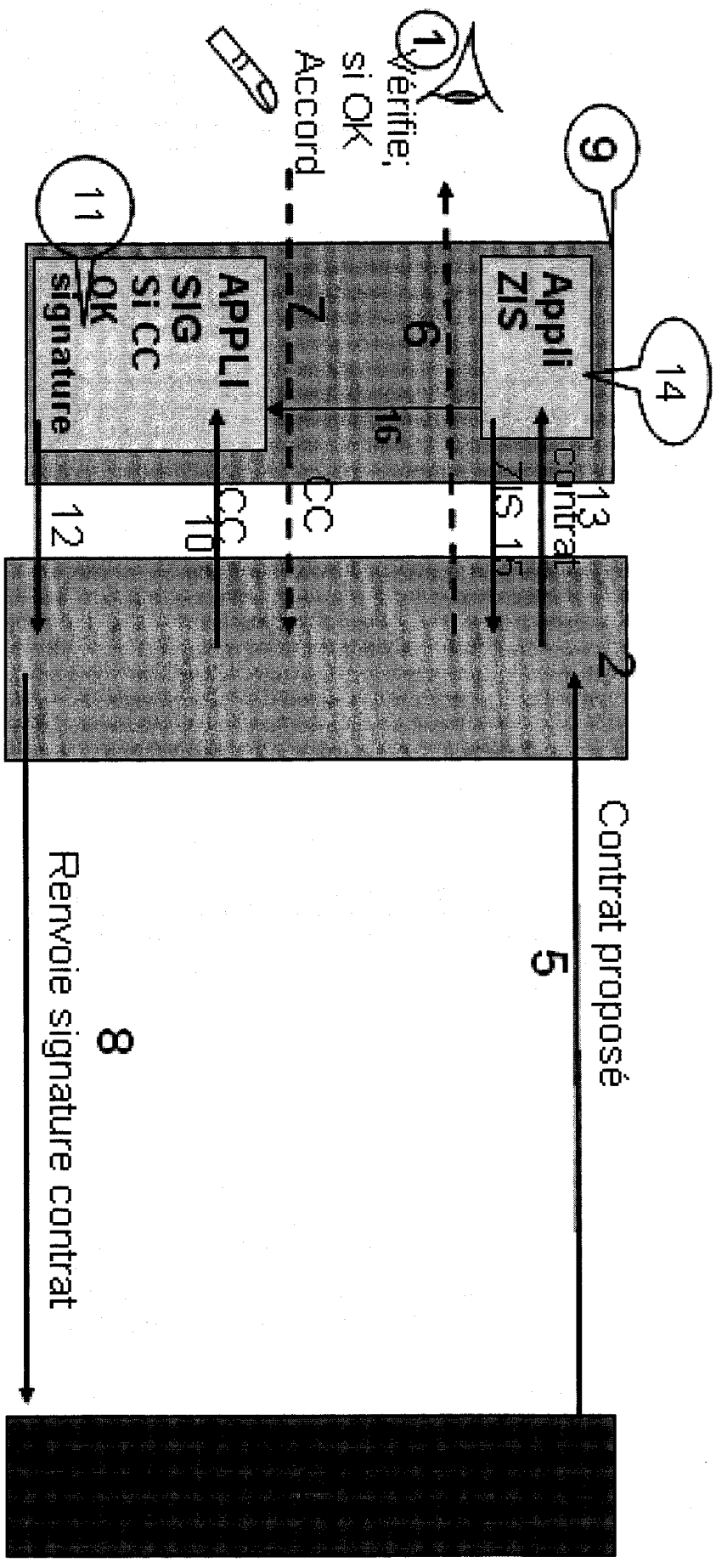

Figure 4: principe de réalisation de la ZIS

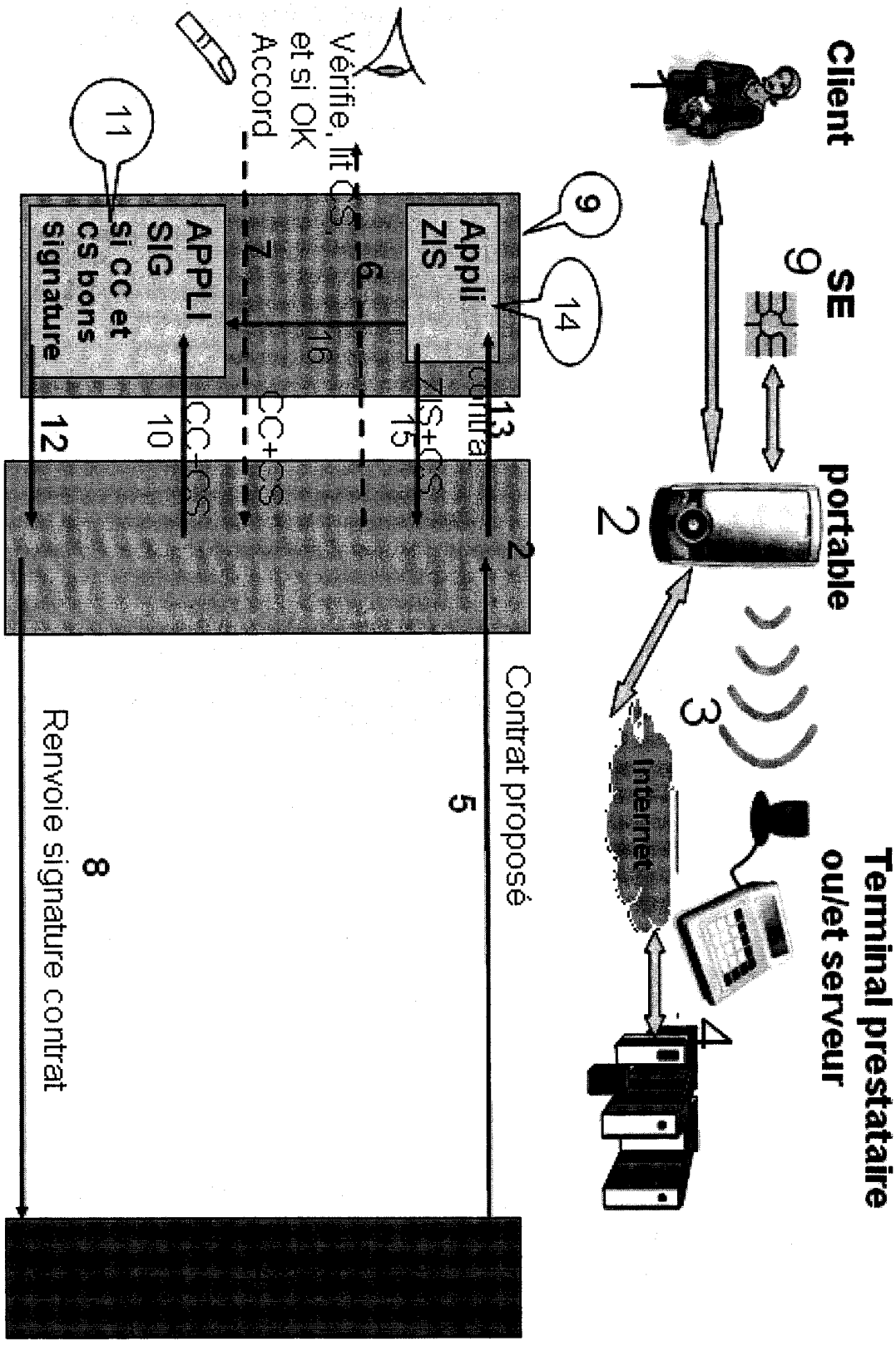

Figure 5: cinématique des échanges dans le cas CS

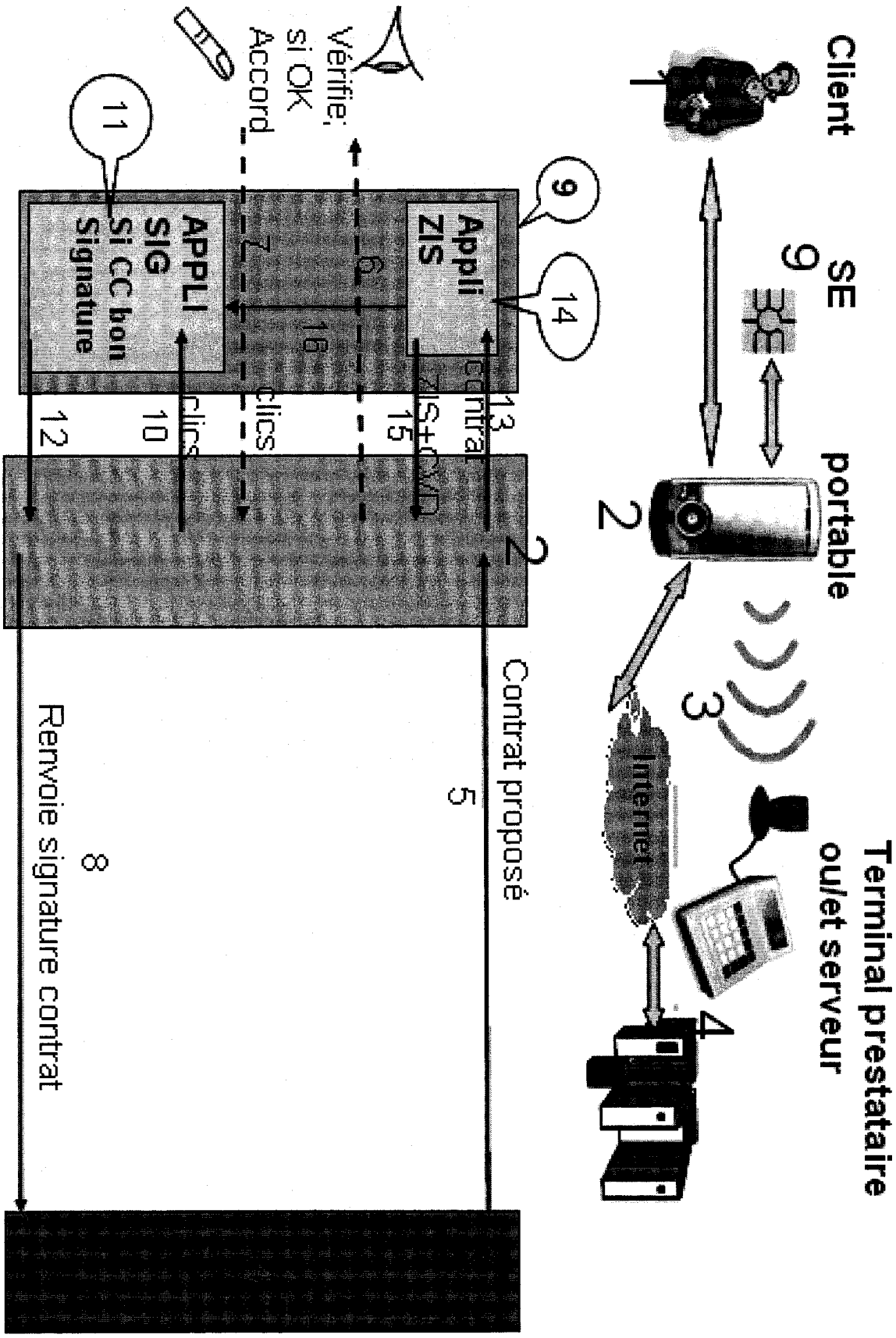

Figure 6: cinématique des échanges dans le cas CVD

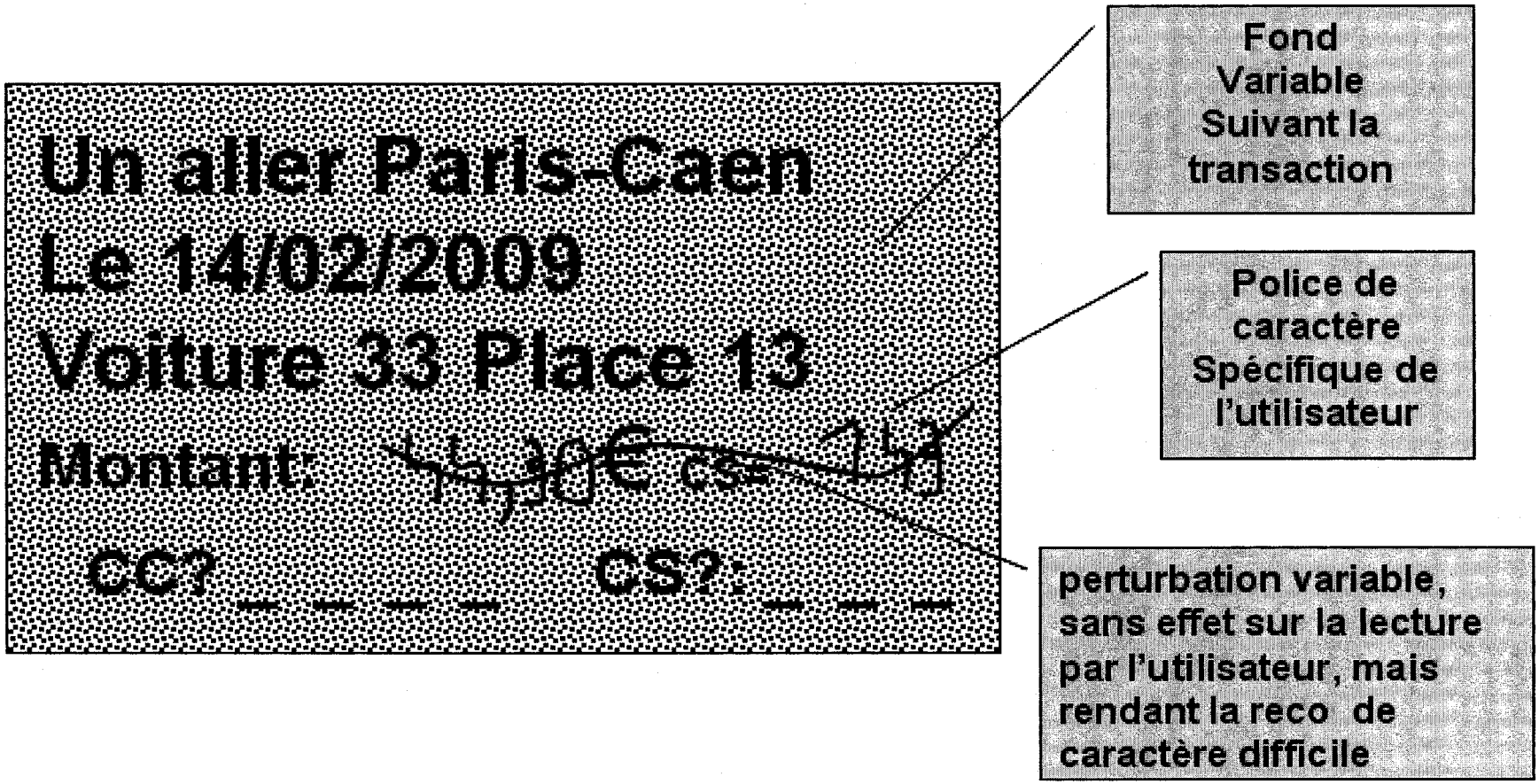

Figure 7: exemple de présentation graphique d'un contrat

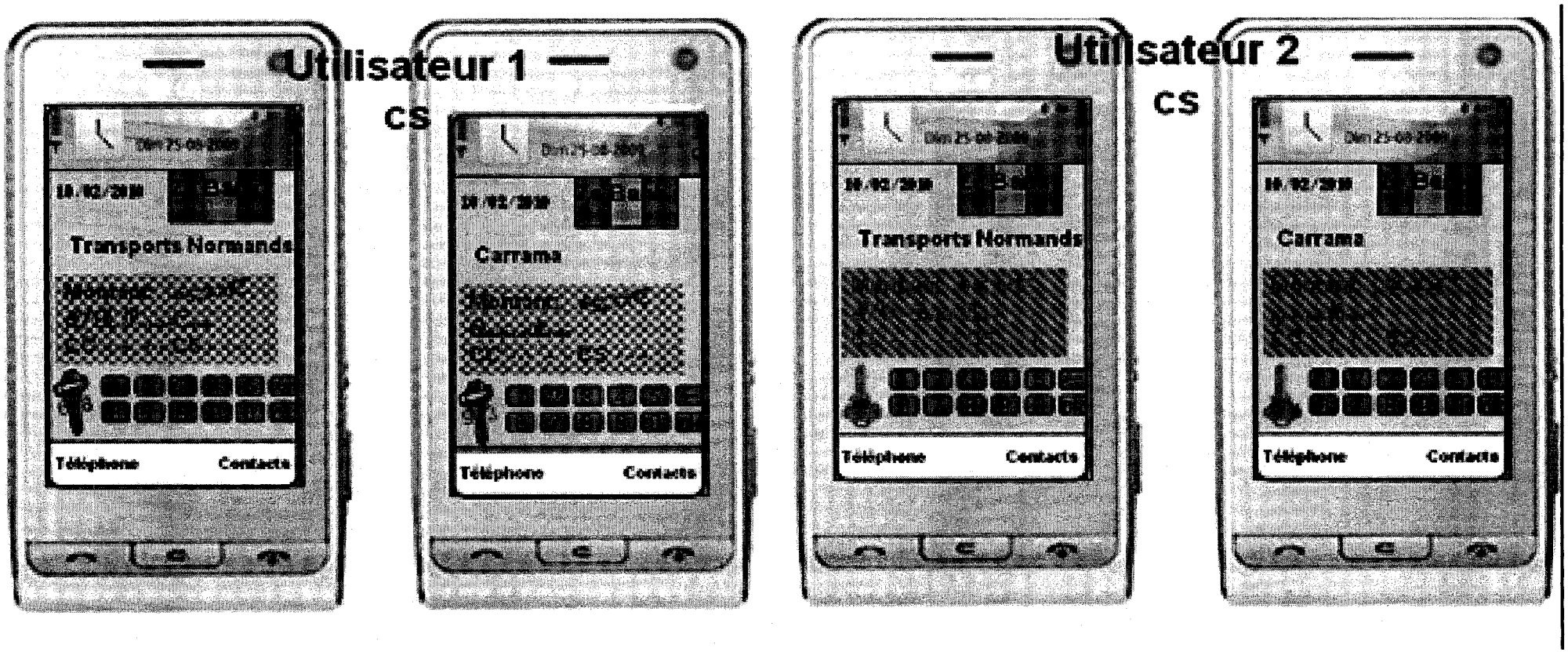

Figure 8: exemple de deux transactions différentes sur les mobiles de deux utilisateurs différents

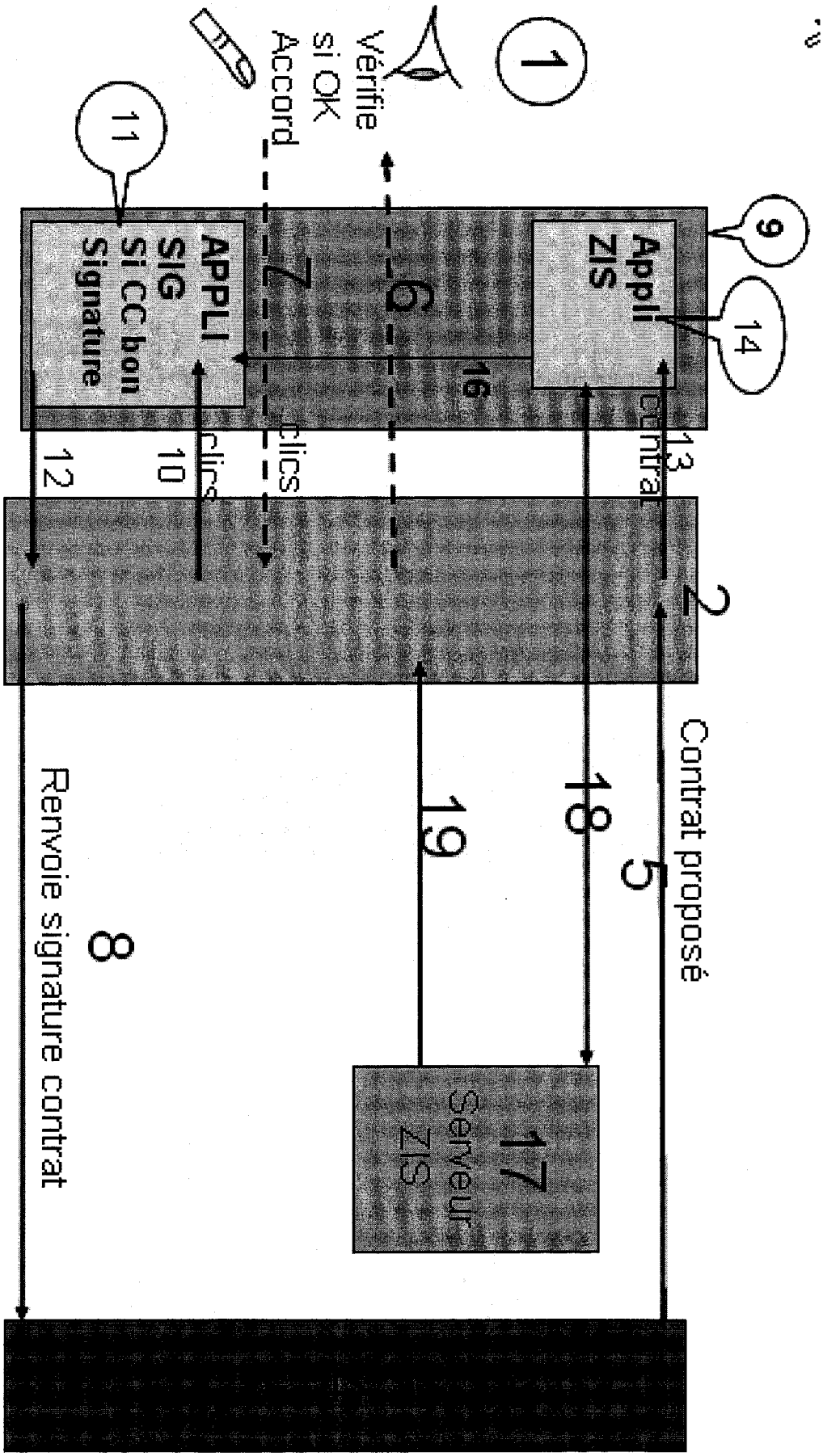

Figure 9: serveur distant pour le calcul de la ZIS

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE PARTIEL

établi sur la base des dernières revendications déposées avant le commencement de la recherche

voir FEUILLE(S) SUPPLÉMENTAIRE(S)

N° d'enregistrement national

FA 742901
FR 1002516

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées	Classement attribué à l'invention par l'INPI
X	WO 2007/056808 A1 (EWISE SYSTEMS PTY LTD [AU]; CHAZAN MARK MERVYN [AU]; GRINBERG ALEXANDE) 24 mai 2007 (2007-05-24) * abrégé; figures 3-5 * * page 5, ligne 2 - page 7, ligne 31 * * page 10, ligne 32 - page 14, ligne 9 * -----	1,5,6,8,9	G06Q20/00 G06F21/00
X	EP 1 843 288 A1 (ELCA INF S A [CH]) 10 octobre 2007 (2007-10-10) * abrégé; figure 5 7 8 * * alinéa [03 5] * * alinéa [18 19] * * alinéa [23 25] * * alinéa [0039] - alinéa [0048] * -----	1,5,6,8,9	
X	EP 2 043 021 A1 (FIDUCIA IT AG [DE]) 1 avril 2009 (2009-04-01) * abrégé; figure 2 * * alinéa [0007] - alinéa [0014] * * alinéa [0024] - alinéa [0028] * * alinéas [0030], [0032] * -----	1,5,6,8,9	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
A	JUN XU ET AL: "Mandatory human participation: a new authentication scheme for building secure systems", COMPUTER COMMUNICATIONS AND NETWORKS, 2003. ICCCN 2003. PROCEEDINGS. T HE 12TH INTERNATIONAL CONFERENCE ON DALLAS, TX, USA 20-22 OCT. 2003, PISCATAWAY, NJ, USA,IEEE, 20 octobre 2003 (2003-10-20), pages 547-552, XP010695028, ISBN: 978-0-7803-7945-9 * le document en entier * -----	1,5,8,9	G06Q G06F
A	US 6 195 698 B1 (LILLIBRIDGE MARK D [US] ET AL) 27 février 2001 (2001-02-27) * abrégé; figure 3 4 9 * * colonne 9, ligne 18 - ligne 40 * -----	9	

Date d'achèvement de la recherche	Examinateur
4 mars 2011	Bauer, Rodolphe

CATÉGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C35)

RECHERCHE INCOMPLÈTE
FEUILLE SUPPLÉMENTAIRE C

Numéro de la demande

FA 742901
FR 1002516

Certaines revendications n'ont pas fait l'objet d'une recherche parce qu'elles se rapportent à des parties de la demande qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectuée, en particulier:

Revendications susceptibles de faire l'objet de recherches complètes:
5-9

Revendications ayant fait l'objet de recherches incomplètes:
1

Revendications n'ayant pas fait l'objet de recherches:
2-4, 10, 11

Raison pour la limitation de la recherche:

Les revendications 2-4, 10-11 ne sont pas claires au point qu'une recherche ne peut être effectuée. Etant donné qu'il n'est pas possible de déterminer quels ensembles de caractéristiques sont définis par ces revendications, il n'est pas possible de déterminer quelle serait l'importance de documents qui pourraient être trouvés. Il n'a pas été possible d'interpréter précisément l'objet de ces revendications, même à la lumière de la description.

ABSENCE D'UNITÉ D'INVENTION
FEUILLE SUPPLÉMENTAIRE B

Numéro de la demande

FA 742901
FR 1002516

La division de la recherche estime que la présente demande de brevet ne satisfait pas à l'exigence relative à l'unité d'invention et concerne plusieurs inventions ou pluralités d'inventions, à savoir :

1. revendications: 5, 6, 8, 9(complètement); 1(en partie)

Procédé de sécurisation d'une transaction électroniques dans lequel un code de sécurité est transmis à un utilisateur, ledit code n'étant pas déchiffrable par un ordinateur,

1.1. revendications: 5, 6, 8(complètement); 1(en partie)

ledit code étant sous une forme d'image codée, et l'utilisateur retransmet pour valider la transaction ä la fois le code tel que lu combiné soit à un code confidentiel, soit à une donnée biométrique.

1.2. revendications: 9(complètement); 1(en partie)

ledit code étant sous une forme sonore.

---

2. revendications: 7(complètement); 1(en partie)

Procédé de sécurisation d'une transaction électronique dans lequel une interface sécurisée est transmise à un utilisateur et l'utilisateur interagit avec cette interface pour valider la transaction, ladite interface graphique permettant l'entrée sécurisée d'un code confidentiel

---

Prière de noter que toutes les inventions mentionnées sous point 1, qui ne sont pas nécessairement liées par un concept inventif commun, ont pu être recherchées sans effort particulier justifiant une taxe additionnelle.
La première invention a été recherchée.

L'utilisation de "CAPTCHAs"/ pour sécuriser les transactions bancaires est bien connue de l'homme du métier et des documents cités.
Le groupe 1.1 se tourne vers une réalisation impliquant un élément graphique qui sera associé à un code connu et/ou dépendant de l'utilisateur. le problème résolu est celui de l'implémentation sur une interface graphique.
Le groupe 1.2 ne fait plus intervenir forcément d'élément graphique, mais fait intervenir une autre réalisation basée sur des sons. Le problème résolu est celui de l'adaptation d'un procédé à des interfaces non-graphiques.
Le groupe 2 n'implique pas la saisie d'un code lu/entendu, mais une forme d'encryptage du code confidentiel basé sur une interface graphique. Le problème à résoudre est celui de trouver un encryptage du code et de l'interface résistant à une attaque du type "man in the middle" automatique. Dans ce cas, l'implémentation se fait sans qu'un code de sécurité n'ait à être transmis, lu par l'utilisateur et renvoyé. Le problème est de trouver une alternative dans la manière d'implémenter la confirmation, qui ne nécessite pas l'envoi dans les deux sens d'une

EPO FORM P0418

ABSENCE D'UNITÉ D'INVENTION
FEUILLE SUPPLÉMENTAIRE B

Numéro de la demande

FA 742901
FR 1002516

La division de la recherche estime que la présente demande de brevet ne satisfait pas à l'exigence relative à l'unité d'invention et concerne plusieurs inventions ou pluralités d'inventions, à savoir :

information identique.

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1002516 FA 742901

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 04-03-2011
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2007056808 A1	24-05-2007	AU 2006315079 A1	24-05-2007
		US 2008319902 A1	25-12-2008
EP 1843288 A1	10-10-2007	EP 2005379 A1	24-12-2008
		FR 2899709 A1	12-10-2007
		WO 2007113669 A1	11-10-2007
EP 2043021 A1	01-04-2009	DE 102007045981 A1	02-04-2009
US 6195698 B1	27-02-2001	AUCUN	

EPO FORM P0465