(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 959 896**

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

(21) **N° d'enregistrement national :** **10 53523**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2006.01), G 06 F 21/22*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 06.05.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 11.11.11 Bulletin 11/45.

(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) :** *4G SECURE Société par actions simplifiée* — FR.

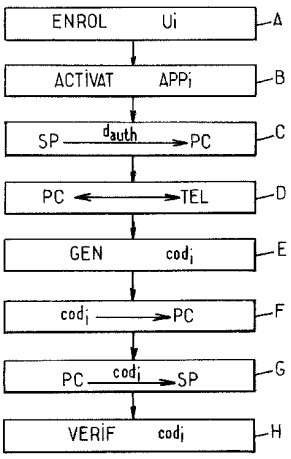
(72) **Inventeur(s) :** LIBERMAN JOHANN, CHATZIKOMNINOS PANOS, AUBERT JEAN PASCAL, DELESTRE BENOIT et HALLEPEE DIDIER.

(73) **Titulaire(s) :** 4G SECURE Société par actions simplifiée.

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) PROCEDE D'AUTHENTIFICATION D'UN UTILISATEUR REQUERANT UNE TRANSACTION AVEC UN FOURNISSEUR DE SERVICE.

(57) La présente invention concerne un procédé d'authentification d'un utilisateur (Ui) requérant une transaction auprès d'un fournisseur de service (SP), le procédé comportant la génération (E) d'un code d'autorisation (codi) spécifique à l'utilisateur et à la transaction requise à partir d'une donnée d'authentification (d_{auth}) lue sur un écran au moyen d'un terminal mobile (TEL) et l'envoi (F) du code d'autorisation généré au fournisseur de service afin d'authentifier l'utilisateur. Elle concerne également un serveur d'authentification (AS) correspondant, ainsi qu'un système d'authentification comprenant un tel serveur d'authentification.



FR 2 959 896 - A1

PROCEDE D'AUTHENTIFICATION D'UN UTILISATEUR REQUERANT UNE TRANSACTION AVEC UN FOURNISSEUR DE SERVICE

La présente invention concerne le domaine de l'authentification, en particulier dans un contexte de sécurisation des accès et de services en ligne proposés dans le cadre de transactions bancaires.

Le besoin d'identifier un utilisateur requérant un service, d'une part, et d'authentifier cet utilisateur, d'autre part, est vraiment apparu avec le développement de l'internet et des services mobiles. Alors que l'identification consiste à communiquer une identité, l'authentification consiste à apporter la preuve de cette identité.

En matière de sécurité des systèmes d'information, une authentification est dite « forte » lorsqu'elle utilise une procédure d'identification requérant la concaténation d'au moins deux éléments ou « facteurs » d'authentification choisis parmi ce que l'entité à authentifier connaît, ce qu'elle détient ou ce qu'elle est.

L'authentification forte est une des fondations essentielles permettant de garantir l'autorisation ou contrôle d'accès à un service (i.e. qui peut y avoir accès), la confidentialité (i.e. qui peut voir le service), l'intégrité (i.e. qui peut modifier le service) et la traçabilité (i.e. qui y a accédé).

Par ailleurs l'usage d'une véritable technologie d'authentification forte se doit de garantir la non-répudiation, à savoir l'élément primordial à l'imputabilité des actions à une entité, qu'elle soit un individu ou une organisation, et ce de manière unique. Une entité authentifiée de manière forte ne peut pas nier avoir eu accès à un système ou signé un document dans la mesure où elle est la seule à détenir le secret le permettant.

Les techniques basées sur un "secret partagé", lesquelles sont souvent assimilées abusivement à des techniques d'authentification forte de haut niveau, ne permettent pas d'assurer la non-répudiation.

En particulier, la méthode classique d'authentification unique symbolisée par un couple identifiant/mot de passe, qui est actuellement le système le plus couramment utilisé pour identifier un utilisateur, présente un certain nombre de faiblesses en matière de sécurisation.

Ces différents niveaux d'authentification (simple ou forte) doivent être choisi en fonction du niveau de contractualisation qu'une entité souhaite appliquer et des effets juridiques ainsi produits.

En particulier, il est entendu ici par contractualisation de la procédure, le fait de conférer à une procédure électronique une valeur contractuelle assortie d'une capacité de gestion de la preuve en cas de conflit.

Eu égard aux exigences de sécurisation des accès exigés par différentes autorités de tutelles dans les différents domaines, les trois couches suivantes de service de confiance sont à considérer : l'authentification, la signature électronique et l'horodatage. Cependant, et comme indiqué précédemment, il n'est pas facile de pouvoir répondre à l'ensemble des exigences indispensables à la mise en œuvre de ces trois couches de confiance.

Dans le cadre de l'authentification, le choix d'une méthode d'authentification adaptée à chaque besoin (par exemple pour une clientèle particulier ou professionnelle, pour l'accès banque en ligne notamment et sécurisation des services financiers) sera basé sur un certain niveau de contractualisation défini au moyen d'une analyse de risque fonction du coût des moyens d'authentification à mettre en œuvre, du coût lié aux différents risques (sensibilité de l'application, des données, etc...) et des bénéfices attendus pour l'utilisateur (en fonction de son niveau d'expertise).

A titre d'exemple, on peut citer les différents niveaux de contractualisation suivants :

Niveau de contractualisation 1 :

Ce premier niveau, meilleur que l'identification par simple paire d'identifiant/mot de passe, repose sur l'implémentation d'une solution d'authentification de bas niveau, assimilable à une pseudo authentification forte.

Niveau de contractualisation 2 :

Ce niveau peut être définit lorsque des moyens organisationnels et techniques sont mis en œuvre afin de garantir au mieux l'identité des différents

acteurs (il peut s'agir par exemple des utilisateurs et/ou tiers autorisés d'un service e-banque ou e-coffre).

Ce niveau nous permet d'entrer dans la sphère de l'authentification forte, mais de 1er degré sans pour autant que l'on puisse parler de « preuve au sens juridique du terme »

Niveau de contractualisation 3 :

Un troisième niveau de contractualisation peut être défini lorsque l'on rentre dans le périmètre de l'authentification forte où le degré d'authentification (2ème degré) est recevable juridiquement même si en cas de contestation la preuve de sa fiabilité reste à apporter par celui qui le met en œuvre.

Niveau de contractualisation 4 :

Le dernier niveau de contractualisation, que l'on qualifiera de présumé fiable, permet, outre les exigences que se doit de remplir un système d'authentification forte, de garantir la non répudiation.

Avec ce niveau de contractualisation, les conditions techniques et organisationnelles devant êtres remplies sont nombreuses et difficiles à réunir, mais la valeur juridique d'un tel procédé est présumé fiable. C'est le niveau d'authentification forte le plus élevé. Ce niveau de contractualisation est celui que l'on rencontre lorsque l'on décide de mettre en œuvre un système de « signature électronique qualifiée » présumée fiable.

Il existe aujourd'hui une panoplie de moyens permettant de s'authentifier de manière sécurisée comme les clefs USB, les jetons (« Token » en anglais), les lecteurs de cartes, etc…

Tous ces moyens, en plus d'être tous aussi couteux les uns que les autres, ne permettent pas d'éviter toutes les attaques de pirates identifiées. De plus des moyens logistiques importants sont nécessaires pour livrer ces moyens et les rendre opérationnels chez l'utilisateur.

Un objet de la présente invention est de répondre aux problèmes ci-avant.

En particulier, la présente invention vise à fournir un système d'authentification convivial, intuitif, ergonomique, sécurisé et utilisable par un maximum de clients.

La présente invention vise également à créer un contexte transactionnel sécurisé à même d'assurer le transport, le chiffrement/déchiffrement de données dynamiques et la présentation de ces données à un serveur pour le traitement, la validation, l'horodatage et l'archivage légal de cette transaction dans des usages nécessitant un haut niveau de confiance.

La présente invention vise en particulier à permettre des usages et des services nécessitant un haut niveau de sécurité, comme le paiement et la signature électronique, assortis d'une option de non répudiation.

La présente invention propose à cet effet un procédé d'authentification d'un utilisateur requérant une transaction auprès d'un fournisseur de service, le procédé comportant la génération d'un code d'autorisation spécifique à l'utilisateur et à la transaction requise à partir d'une donnée d'authentification lue sur un écran au moyen d'un terminal mobile et l'envoi du code d'autorisation généré au fournisseur de service afin d'authentifier l'utilisateur.

Le caractère spécifique du code d'autorisation ainsi générée empêche sa réutilisation par un utilisateur malveillant au cours d'une transaction ultérieure.

Avantageusement, la donnée d'authentification lue est interprétée dans le terminal mobile au moyen d'une application personnalisée spécifique à l'utilisateur et téléchargée à partir d'un serveur d'authentification.

Dans un mode de réalisation particulier, l'application personnalisée téléchargée dans le terminal mobile génère le code d'autorisation à partir de la donnée d'authentification lue, ce qui limite de multiplier les transferts aussi bien de la donnée d'authentification que du code d'autorisation.

Dans un autre mode de réalisation particulier, le procédé comprend la transmission de la donnée d'authentification lue du terminal mobile au serveur d'authentification, la génération du code d'autorisation à partir de la donnée

d'authentification dans le serveur d'authentification, et la transmission du code d'autorisation généré au terminal mobile. Ce mode de réalisation allège les calculs devant être effectués au niveau du terminal mobile.

Avantageusement, un lien de téléchargement pointant vers l'application personnalisée générée est envoyé à l'utilisateur et le procédé comprend alors en outre une étape d'activation au cours de laquelle le terminal mobile télécharge l'application personnalisée au moyen du lien de téléchargement, ce qui permet de laisser à l'utilisateur le choix du moment où il désire activer l'application personnalisée.

De manière avantageuse, l'étape d'enrôlement comprend alors la transmission d'un code d'activation au terminal mobile, ledit code d'activation étant utilisé lors de l'étape d'activation pour activer l'application personnalisée téléchargée.

Plus particulièrement, l'étape d'enrôlement comprend une étape de vérification de l'identité de l'utilisateur avant la transmission du code d'activation, ladite transmission n'étant effectuée que si ladite vérification est effectuée de façon positive.

D'une manière avantageuse, l'étape d'activation comprend la transmission d'au moins une donnée confidentielle spécifique à l'utilisateur au terminal mobile, ladite donnée confidentielle étant utilisée pour chiffrer la donnée d'authentification dans le terminal mobile avant sa transmission au serveur d'authentification et/ou pour déchiffrer le code d'autorisation reçu par le terminal mobile. Les transferts de la donnée d'authentification au serveur d'authentification, d'une part, et du code d'autorisation au terminal mobile, d'autre part, sont ainsi sécurisés.

Dans un mode de réalisation avantageux, la donnée confidentielle et/ou l'application personnalisée est générée n en fonction d'au moins une donnée interne d'identification générée, par le fournisseur de service, à partir d'au moins une donnée personnelle d'identification envoyée par l'utilisateur au fournisseur de service.

Ce mode de réalisation offre un degré supplémentaire de protection dans la mesure où les données personnelles transmises par l'utilisateur ne sont pas directement utilisées pour générer l'application personnalisée.

Dans un mode particulièrement avantageux de réalisation, la donnée d'authentification est générée par le fournisseur de service de façon spécifique à l'utilisateur et à la transaction requise, ce qui empêche la réutilisation d'un telle donnée d'authentification par un utilisateur malveillant au cours d'une transaction ultérieure.

Dans un autre mode particulier de réalisation, l'étape d'envoi du code d'autorisation comprend la lecture du code d'autorisation affiché par le terminal mobile par des moyens de lecture d'un ordinateur et l'envoi du code d'autorisation lu vers le fournisseur de service. Il est ainsi possible de transmettre ce code d'autorisation sans passer par une saisie humaine, ce qui permet l'utilisation d'un code d'autorisation sous forme de code-barres par exemple.

La présente invention propose par ailleurs un serveur d'authentification comprenant un module de réception arrangé pour recevoir une donnée d'authentification et au moins une donnée interne d'identification, des moyens de calcul arrangés pour générer un code d'autorisation en fonction de la donnée d'authentification reçue et d'au moins une des donnée internes d'identification reçues, et un module d'émission arrangé pour émettre le code d'autorisation généré vers un terminal mobile.

Suivant un troisième aspect, la présente invention propose un système d'authentification d'un utilisateur requérant une transaction auprès d'un fournisseur de service, le système comprenant un écran arrangé pour afficher une donnée d'authentification reçue du fournisseur de service, un terminal mobile disposant de moyens de saisie de la donnée d'authentification affichée sur l'écran et arrangé pour retourner un code d'autorisation spécifique à l'utilisateur et à la transaction requise, et des moyens de saisie permettant l'envoi du code d'autorisation au fournisseur de service afin d'authentifier l'utilisateur.

Avantageusement, ce système d'authentification comprend en outre un serveur d'authentification tel que décrit ci-avant.

Dans un mode de réalisation particulier, le système d'authentification comprend un serveur de service arrangé pour fournir le service requis par l'utilisateur, ledit serveur de service comprenant un module de réception arrangé pour recevoir au moins une donnée personnelle de l'utilisateur et le code d'autorisation émis par l'utilisateur, des moyens de calcul arrangé pour générer au moins une donnée interne d'identification à partir d'au moins une des données personnelles reçues, et un module d'émission arrangé pour envoyer la donnée interne d'identification générée au serveur d'authentification.

D'autres caractéristiques et avantages de l'invention apparaîtront encore à la lecture de la description qui va suivre. Celle-ci est purement illustrative et doit être lue en regard des dessins annexés sur lesquels :

- la figure 1A représente les étapes d'un procédé d'authentification selon le principe de la présente invention ;
- La figure 1B illustre un système selon un premier mode de réalisation de type « off-line » mettant en œuvre le procédé d'authentification de la présente invention ;
- la figure 2A représente les sous-étapes de l'étape d'enrôlement du procédé d'authentification selon le principe de la présente invention ;
- la figure 2B représente un premier mode de réalisation du système mettant en œuvre l'étape d'enrôlement du procédé d'authentification selon le principe de la présente invention ;
- la figure 2C représente un deuxième mode de réalisation du système mettant en œuvre l'étape d'enrôlement du procédé d'authentification selon le principe de la présente invention ;
- La figure 3A illustre les sous-étapes constitutives de l'étape d'activation de l'application personnalisée selon un mode de réalisation de la présente invention ;

- La figure 3B illustre un système mettant en œuvre l'étape d'activation de l'application personnalisée du procédé d'authentification selon le principe de la présente invention ;
- la figure 4A illustre les sous-étapes constitutives de l'étape de génération du code d'autorisation d'un procédé d'authentification selon un deuxième mode de réalisation de type « on-line »;
- La figure 4B illustre un premier mode de réalisation du système mettant en œuvre le procédé d'authentification selon le deuxième mode de réalisation de type « on-line », où le code d'autorisation est généré dans un serveur d'authentification AS distinct du serveur du fournisseur de services ; et
- La figure 4C illustre un deuxième mode de réalisation du système mettant en œuvre le procédé d'authentification selon le deuxième mode de réalisation de type « on-line », où le code d'autorisation est généré dans le serveur du fournisseur de services sur lequel des fonctionnalités d'authentification ont été installées.

Sur la **figure 1A** sont illustrées les étapes d'un procédé d'authentification selon le principe de la présente invention.

Ce procédé peut démarrer avec une étape A d'enrôlement d'un utilisateur Ui auprès d'un fournisseur de services avec lequel il désire effectuer une transaction.

A cette occasion, l'utilisateur Ui va envoyer à ce fournisseur de service (par exemple à un serveur SP géré par ce fournisseur de service) un certain nombre de données personnelles d'identification (dénommées ici « d_{id}»), par exemple en les saisissant sur son ordinateur par le biais d'une application client associée au serveur SP du fournisseur de services.

De telles données personnelles d_{id} servent à identifier formellement l'utilisateur Ui lorsque celui s'inscrit à un service.

Une fois que le serveur SP a reçu ces données personnelles, celles-ci sont contrôlées par le fournisseur de service, afin de pouvoir garantir ultérieurement que l'utilisateur Ui est bien le véritable utilisateur.

Un tel contrôle peut être fait sur la base de données déjà connues si l'utilisateur est déjà connu (grâce à des données présentes sur un relevé bancaire, par exemple), par un appel téléphonique d'un opérateur, ou par la demande de la copie de la carte d'identité d'un nouvel utilisateur.

Une fois vérifiées, ces données personnelles sont stockées de manière sécurisée, par exemple dans le serveur SP du fournisseur de service ou dans un autre serveur délégué à cette tâche.

Suite à l'enrôlement de l'utilisateur Ui auprès du fournisseur de services, une étape B d'activation d'une application personnalisée, générée spécifiquement pour l'utilisateur Ui, sur un terminal mobile appartenant à l'utilisateur Ui peut être effectuée à ce stade, afin de permettre à l'utilisateur Ui d'utiliser son terminal mobile dans la procédure d'authentification auprès du fournisseur de services. Un exemple d'une telle étape d'activation est décrit plus loin.

Une fois l'utilisateur Ui enrôlé auprès du fournisseur de services et muni d'un terminal mobile disposant d'une application personnalisée utilisable pour permettre son authentification, l'utilisateur Ui est prêt à effectuer une transaction nécessitant une authentification avec le fournisseur de services.

Pour cela, le procédé comporte une étape C d'affichage d'une donnée d'authentification (dénommée d_{auth} par la suite) sur un écran auquel a accès l'utilisateur Ui. Un tel écran peut être naturellement l'écran connecté à l'ordinateur personnel de l'utilisateur Ui auquel cas la donnée d'authentification d_{auth} est transmise au préalable du serveur SP du fournisseur de services à cet ordinateur personnel pour être affichée sur cet écran.

L'envoi de cette donnée d'authentification peut être conditionné à la réception, par le serveur SP, d'une requête en transaction émanant de l'ordinateur personnel de l'utilisateur Ui. Par exemple, l'utilisateur Ui peut utiliser son ordinateur personnel pour accéder à une application client associée au fournisseur de services (par exemple par le biais du site internet de ce fournisseur) et indique son intention d'effectuer une transaction. Suite à cette indication, le serveur SP génère et envoie la donnée d'authentification à l'ordinateur personnel de l'utilisateur Ui.

La donnée d'authentification d_{auth} affichée lors de l'étape C peut prendre la forme d'un code-barres en deux dimensions, d'un tag ou mot de passe à une seule utilisation (« One-Time Password » ou OTP en anglais).

De préférence, lorsqu'un code-barres en deux dimensions ou un tag est employé, la représentation graphique de ce code-barres en deux dimensions ou de ce tag respecte les standards couramment utilisés, comme par exemple QR-Code, Datamatrix, PDF 417, Microsoft tag.

Avantageusement, la donnée d'authentification d_{auth} transmise par le fournisseur de services est générée spécifiquement pour la transaction requise, en fonction de données liées à la transaction et éventuellement de données personnelles reçues de l'utilisateur.

D'une manière avantageuse, cette donnée d'authentification d_{auth} est à usage unique et est générée à chaque transaction de façon à être différente pour chaque transaction requise. Ainsi, la connaissance éventuelle de cette donnée d'authentification par interception d'un utilisateur malveillant ne lui permet pas d'utiliser cette information pour les transactions ultérieures.

A la suite de l'affichage de la donnée d'authentification d_{auth}, l'utilisateur Ui utilise son terminal mobile pour y entrer cette donnée d'authentification, lors d'une étape D de lecture, afin qu'elle soit interprétée par l'application personnalisée préalablement activée lors de l'étape B.

Dans un premier mode de réalisation, cette donnée d'authentification d_{auth} est lue par l'utilisateur Ui, lequel l'entre manuellement sur son terminal mobile. Ce premier mode de réalisation est en particulier adapté lorsque le terminal mobile de l'utilisateur ne dispose pas de moyens de lecture propres tels qu'un appareil photo.

Dans un autre mode de réalisation destiné à limiter l'interaction avec l'utilisateur, potentielle source d'erreur, la donnée d'authentification d_{auth} est lue directement par le terminal mobile, lequel dispose de ses propres moyens de lecture. Ainsi, lorsque le terminal mobile dispose d'un appareil photo, l'utilisateur Ui peut prendre une photo de la donnée d'authentification affichée sur l'écran, et l'application activée dans le logiciel va utiliser le cliché pris pour retrouver les données pertinentes dans la donnée d'authentification et les interpréter.

Suite à la lecture de la donnée d'authentification d_{auth} et son interprétation dans le terminal mobile de l'utilisateur Ui, un code d'autorisation cod_i est généré, puis affiché par le terminal mobile, lors d'une étape E de génération de code. Ce code cod_i sert à authentifier l'utilisateur Ui auprès du fournisseur de services.

Similairement à ce qui a été dit au sujet de la donnée d'authentification, le code d'autorisation cod_i peut prendre la forme d'une image, d'un code-barres en deux dimensions, d'un tag ou mot de passe à une seule utilisation (« One-Time Password » ou OTP en anglais).

Cette étape E de génération du code d'autorisation peut être implémentée selon différents mode de réalisation.

Dans un premier mode de réalisation dit « off-line », le code d'autorisation cod_i est généré intégralement par l'application personnalisée installée sur le terminal mobile, ce qui permet d'utiliser ce terminal mobile sans que celui-ci ne soit forcément connecté au réseau mobile et limite les transferts de données sensibles pouvant être récupérées par un tiers malveillant.

Dans un tel mode, l'application personnalisée interprète la donnée d'authentification lue et génère à partir de la donnée interprétée un code d'autorisation qui est affiché par le terminal mobile.

L'application personnalisée, outre la donnée d'authentification cod_i, peut également utiliser un code secret confié à l'utilisateur pour générer le code d'autorisation, ce qui permet de renforcer le caractère spécifiquement lié à l'utilisateur de ce code d'autorisation.

Si l'on prend l'exemple d'un utilisateur ayant téléchargé l'application personnalisée auprès de son établissement financier et venant de se connecter à son site de banque en ligne, lorsque celui veut accéder à ses comptes personnels, il va lancer l'application personnalisée et rentrer son code secret. Si le code d'autorisation généré se présente sous la forme d'une image, l'utilisateur présente ensuite cette image devant l'espace réservé à celui sur le site internet. L'image est alors automatiquement transférée au serveur de la banque afin de permettre ou non sa connexion.

Dans un autre mode de réalisation dit « on-line », le code d'autorisation cod_i est généré dans un serveur distinct du terminal mobile, qui se contente

alors d'interpréter la donnée d'authentification lue et éventuellement de la mettre en forme et de la chiffrer avant de la transmettre à ce serveur, lequel génère le code d'autorisation cod_i en fonction de la donnée d'authentification d_{auth} qu'il reçoit via le terminal mobile et renvoie ce code d'autorisation au terminal mobile où il est affiché.

Le mobile peut, selon les cas, directement transmettre ce code d'autorisation, ou le traduire et le traiter avant de le transmettre au serveur d'authentification.

Une fois ce code d'autorisation généré et affiché sur le terminal mobile, une étape F de saisie de ce code cod_i, sur l'ordinateur personnel de l'utilisateur Ui, est alors effectuée.

Similairement à ce qui a été décrit pour l'étape D de lecture de la donnée d'authentification, un premier mode de réalisation de cette étape de saisie consiste en ce que l'utilisateur Ui lise lui-même ce code d'autorisation et le rentre manuellement auprès de son ordinateur personnel, ce qui est adapté au cas où l'ordinateur personnel de l'utilisateur ne dispose pas de ses propres moyens de lecture.

Dans un tel cas de figure, il convient d'utiliser un code d'autorisation lisible par un être humain, par exemple un mot de passe à usage unique (OTP), c'est-à-dire relativement simple comme un code constitué de caractères alphanumériques.

Un autre mode de réalisation est possible, dans lequel l'ordinateur personnel de l'utilisateur dispose de ses propres moyens de lecture, par exemple d'une webcam ou n'importe quelle caméra numérique connectée à l'ordinateur, auquel cas il est alors possible de saisir directement le code d'autorisation par simple lecture du code d'autorisation affiché par le terminal mobile au moyen de ces moyens de lecture, suivie d'une reconnaissance de formes afin de retrouver le code d'autorisation.

Dans un tel cas de figure, il est avantageux d'utiliser un code d'autorisation sous forme d'image, de code-barres en deux dimensions ou de tag. Le code d'autorisation est alors illisible directement par un être humain, ce qui permet d'éviter que le code d'autorisation soit visuellement intercepté par un utilisateur malveillant pouvant regarder l'écran du terminal mobile.

Une fois le code d'autorisation saisi sur l'ordinateur personnel de l'utilisateur Ui, les données transactionnelles ainsi que le code d'autorisation sont envoyés (étape G) vers le serveur SP du fournisseur de services qui va effectuer la vérification (étape H) de ce code afin d'authentifier l'utilisateur Ui et permettre la transaction si cette authentification est correcte.

La **figure 1B** illustre un système selon un premier mode de réalisation de type « off-line », mettant en œuvre le procédé d'authentification de la présente invention tel que décrit précédemment sur la figure 1A.

Un tel système comprend un serveur SP appartenant au fournisseur de services connecté, par exemple par le biais du réseau internet, à l'ordinateur personnel (« PC ») de l'utilisateur Ui. Cet ordinateur personnel dispose d'un écran (« SCN ») qui va servir à afficher la donnée d'authentification d_{auth} envoyée par le serveur SP.

Outre les éléments précités, la présente invention utilise un terminal mobile TEL tel qu'un téléphone mobile, un smartphone, un baladeur numérique, etc... appartenant à l'utilisateur Ui et sur lequel est installée une application capable d'interpréter la donnée d'authentification.

Sur cette figure 1B les différents échanges effectués lors du procédé décrit à la figure 1A sont décrits. En particulier, les flux de données correspondant à l'étape préalable A d'enrôlement, l'étape C d'envoi d'une donnée d'authentification, l'étape D de lecture de cette donnée par le terminal mobile, l'étape F de saisie du code d'autorisation sur l'ordinateur personnel et l'étape G d'envoi du code saisi vers le serveur SP sont indiqués.

La **figure 2A** illustre les sous-étapes de l'étape A d'enrôlement selon un mode de réalisation de la présente invention utilisant un serveur d'authentification AS.

Lors d'une première sous-étape A1, l'utilisateur Ui envoie au serveur SP du fournisseur de services un certain nombre de données personnelles d'identification d_{id}, par exemple en les saisissant sur son ordinateur par le biais d'une application client associée au serveur SP du fournisseur de services.

Ces données personnelles d'identification d_{id}, une fois reçues par le serveur SP, sont mémorisées lors d'une sous-étape A2 de mémorisation.

Ensuite, lors d'une sous-étape A3, le serveur SP du fournisseur de services envoie une requête req à un serveur d'authentification AS afin que celui-ci génère un certain nombre d'éléments servant à l'authentification de l'utilisateur.

Dans un premier mode de réalisation, ce serveur d'authentification AS peut correspondre au serveur SP du fournisseur de services sur lequel des fonctionnalités supplémentaires d'authentification ont été installées. Avec ce premier mode de réalisation où les fonctionnalités d'authentification, d'identification et de fourniture de services sont intégrées au sein d'un même serveur, tous les échanges entre modules d'authentification et de fourniture de services se font au sein d'un même environnement sécurisé, ce qui accentue la sécurisation du système.

Dans un deuxième mode de réalisation, ce serveur d'authentification AS est un serveur distinct du serveur SP du fournisseur de services, auquel cas les fonctionnalités d'authentification sont délibérément séparées des fonctionnalités de transaction et de fourniture de services, ce qui permet une gestion de l'authentification par un opérateur distinct du fournisseur de services, lequel n'a pas forcément les compétences techniques ni la capacité à gérer cette authentification.

Dans ce deuxième mode de réalisation, la requête req s'accompagne d'un certain nombre de données d_{int} d'identification internes de l'utilisateur, basées sur les données personnelles d'identification reçues par le serveur SP mais différentes de celles-ci, afin de permettre la génération des éléments servant à l'authentification de l'utilisateur dans le serveur d'authentification AS, tout en garantissant l'anonymat de celui-ci auprès de ce serveur.

Ainsi, dans la mesure où les seules données personnelles sensibles de l'utilisateur sont stockées en espace sécurisé auprès du serveur SP du fournisseur de services, elles sont hors de portée des malwares qui pourraient avoir accès au serveur d'authentification AS.

Suite à la réception de la requête req, le serveur d'authentification AS génère (sous-étape A4) d'une part l'application personnalisée APP_i qui va

servir à interpréter la donnée d'authentification d_{auth} et qui est destinée à être installée sur le terminal mobile TEL_i de l'utilisateur.

Une telle application personnalisée APP_i peut, par exemple, contenir un certain nombre d'éléments personnalisés permettant de personnaliser l'application afin de la rendre spécifique à l'utilisateur Ui. Par exemple, cette application personnalisée peut contenir la signature du mot de passe de l'utilisateur ainsi qu'un algorithme permettant de vérifier ce mot de passe.

Ces éléments personnalisés et spécifiques à l'utilisateur Ui sont implémentés « en dur » (i.e. ils ne sont pas modifiables) dans l'application personnalisées et sont propre à l'utilisateur.

Dans un mode avantageux de réalisation permettant l'activation différée de cette application personnalisée, cette application APP_i contient également un algorithme de vérification d'un code PIN d'activation.

La durée de validité de l'application personnalisée APP_i est par ailleurs configurable par l'opérateur du serveur d'authentification AS en fonction du fournisseur de services concerné et selon les besoins de ce fournisseur de services.

Le serveur d'authentification AS peut également générer, toujours lors de cette sous-étape A4 de génération, un certain nombre de données confidentielles suivantes, désignées par l'abréviation « $scrt_i$ » dans la figure 2A, en fonction des données d'identification reçues par le serveur AS :

- identifiant et mot de passe de l'utilisateur ;
- code PIN d'activation de l'application personnalisée ;
- clé de stockage des informations à destination du terminal mobile ;
- une ou plusieurs clé(s) de chiffrement des échanges entre le terminal mobile TEL et le serveur d'authentification AS ;
- une ou plusieurs clé(s) de signature de l'utilisateur, si nécessaire.

Ces données confidentielles $scrt_i$ sont spécifiques à l'utilisateur Ui et sont générées à partir des données internes d_{int} qui ont été elles-mêmes générées à partir des données personnelles d'identification d_{id} de l'utilisateur, par exemple en même temps que l'application personnalisée APP_i. Ces données confidentielles $scrt_i$ sont destinées à être transmises au terminal mobile TEL de l'utilisateur Ui.

Chaque utilisateur Ui distinct s'enrôlant auprès du fournisseur de services dispose donc de données confidentielles $scrt_i$ distinctes des autres utilisateurs. Ainsi, la copie de l'application personnalisée APP_i sur un autre terminal mobile que celui de l'utilisateur Ui est inutile sans les données confidentielles $scrt_i$ générées par le serveur AS.

De même, la copie des données confidentielles $scrt_i$ sur un autre terminal mobile que celui de l'utilisateur Ui rend ces données confidentielles $scrt_i$ non interprétables par cet autre terminal mobile.

Dans un mode de réalisation avantageux où une donnée confidentielle $scrt_i$ comprend une clé de chiffrement servant à chiffrer les échanges entre le terminal mobile TEL et le serveur d'authentification AS, cette clé de chiffrement est composé au moins d'une première clé pour l'utilisateur Ui et d'une deuxième clé pour le serveur d'authentification AS.

Dans un mode de réalisation particulier de l'enrôlement de l'utilisateur où l'application personnalisée APP_i générée est directement téléchargée, le procédé se poursuit par une étape A5 de téléchargement de l'application personnalisée APP_i dans le terminal mobile de l'utilisateur Ui. Cette application personnalisée APP_i peut y être activée ultérieurement au moyen d'un code PIN d'activation si cette option d'activation ultérieure est choisie.

Dans un autre mode de réalisation alternatif où le téléchargement de l'application personnalisée APP_i par le terminal mobile n'a pas lieu directement lors de l'enrôlement de l'utilisateur, l'étape A5 comprend alors, non plus le téléchargement, mais l'envoi d'un lien de téléchargement pointant vers l'application personnalisée APP_i au le terminal mobile de l'utilisateur Ui, après la génération de cette application personnalisée.

Un tel lien de téléchargement, par exemple une URI, peut être envoyé par l'intermédiaire d'un SMS, d'un email ou d'une connexion local de type WiFi ou Bluetooth.

Ce mode de réalisation alternatif permet à l'utilisateur de décider du moment du téléchargement proprement dit. La mise à disposition du lien par SMS permet un processus immédiat sans avoir besoin de connaître la disponibilité de l'utilisateur et ne nécessite pas une couverture de réseau, contrairement au téléchargement direct.

Ensuite, dans un mode de réalisation avantageux présentant un niveau de sécurité accrue, une étape A7 d'envoi d'un code PIN d'activation (généré lors de l'étape A4) au terminal mobile est réalisée. Ce code PIN d'activation permet de garantir l'authentification de bout en bout, sans faille initiale, depuis l'inscription au service jusqu'à l'utilisation ultérieure, afin de certifier que seul l'utilisateur Ui a pu effectuer ces opérations.

L'envoi de ce code PIN d'activation peut être conditionné à la vérification, par le serveur d'authentification AS, de l'identité de l'utilisateur lors d'une étape A6 de vérification précédant un tel envoi. Une telle vérification peut consister par exemple en l'envoi au serveur d'authentification AS d'une image de la carte d'identité de l'utilisateur Ui, via une webcam de l'ordinateur de cet utilisateur ou l'appareil photo de son terminal mobile TEL, et la vérification par le serveur AS que les données affichées sur cette image correspondent bien à l'utilisateur Ui.

Ainsi, dans un mode de réalisation avantageux de l'invention, à l'issue de cette étape d'enrôlement, le terminal mobile TEL dispose d'un lien pour télécharger une application personnalisée capable de gérer l'authentification de l'utilisateur Ui ainsi que d'un code PIN d'activation permettant d'activer une telle application personnalisée.

Lorsque les serveurs SP et AS sont distincts, le serveur SP du fournisseur de services stocke les données personnelles de l'utilisateur Ui, qui ne sont connues que de ce serveur SP pour garantir leur confidentialité et, inversement, le serveur AS d'authentification n'a la connaissance que des données d'identifications internes transmises avec la requête du fournisseur de services. Cette séparation des données entre différents serveurs permet de garantir une meilleure résistance aux attaques.

La **figure 2B** illustre un premier mode de réalisation d'un système mettant en œuvre l'étape A d'enrôlement selon le principe de la présente invention, telle que décrite précédemment.

Un tel système, outre les éléments déjà décrits sur la figure 1B, comprend en outre un serveur d'authentification AS qui va générer l'application

personnalisée et certaines données confidentielles associés à l'utilisateur Ui sur requête reçu du serveur SP du fournisseur de services.

Sur cette figure 2B, les différents échanges effectués lors de l'étape d'enrôlement décrite à la figure 2A sont illustré.

En particulier, les flux de données correspondant à la sous-étape d'envoi A1 des données personnelles au serveur SP du fournisseur de services, la sous-étape A3 d'envoi d'une requête en génération de l'application personnalisée au serveur d'authentification AS, la sous-étape A5 d'envoi du lien de téléchargement de l'application personnalisée au terminal mobile et la sous-étape A6 d'envoi du code PIN d'activation de l'application personnalisée au terminal mobile sont indiqués.

Dans ce premier mode de réalisation, le serveur d'authentification AS est distinct du serveur SP du fournisseur de service. Ce mode de réalisation est particulièrement adapté aux applications pour lesquelles le fournisseur de service ne souhaite pas gérer lui-même l'authentification des transactions et préfère déléguer cette fonction à un opérateur tiers.

La **figure 2C** illustre un deuxième mode de réalisation d'un système mettant en œuvre l'étape A d'enrôlement selon le principe de la présente invention, telle que décrite précédemment.

Un tel système se différencie du système selon le premier mode de réalisation de la figure 2B en ce que le serveur d'authentification AS correspond au serveur SP du fournisseur de service. En d'autres termes, un même serveur est utilisé aussi bien pour effectuer l'authentification que pour fournir un service.

Un tel serveur peut prendre la forme d'un serveur SP apte à fournir un service sur lequel sont installées les fonctionnalités d'authentification nécessaires aux étapes d'authentification décrites dans la présente demande sous forme de modules complémentaires, par exemple sous la forme de modules logiciels complémentaires.

Dans ce mode de réalisation, tous les flux de données correspondant à la sous-étape d'envoi A1 des données personnelles au serveur SP du fournisseur de services, la sous-étape A3 d'envoi d'une requête en génération

de l'application personnalisée au serveur d'authentification AS, la sous-étape A5 d'envoi du lien de téléchargement de l'application personnalisée au terminal mobile et la sous-étape A6 d'envoi du code PIN d'activation de l'application personnalisée au terminal mobile transitent donc par un unique serveur (désigné par « SP=AS »).

Ce deuxième mode de réalisation est particulièrement adapté aux applications pour lesquelles le fournisseur de service souhaite gérer lui-même l'authentification des transactions, pour des raisons de sécurisation. Cela peut par exemple être le cas quand le fournisseur de service est un opérateur bancaire permettant des transactions en ligne.

La **figure 3A** illustre les sous-étapes de l'étape B d'activation de l'application personnalisée selon un mode de réalisation de la présente invention.

Lors d'une première sous-étape B1, l'utilisateur Ui télécharge l'application personnalisée dans son terminal mobile au moyen du lien de téléchargement qui lui a été envoyé préalablement lors de l'étape A d'enrôlement.

Une fois cette application personnalisée téléchargée dans le terminal mobile TEL, l'activation de l'application personnalisée peut être effectuée ensuite lors d'une sous-étape B2, et ce avantageusement au moyen d'un code PIN reçu préalablement lors de l'étape A d'enrôlement.

Dans un mode de réalisation particulier, des données confidentielles générées lors de l'étape A d'enrôlement sont également téléchargées lors d'une sous-étape B3.

Parmi ces données confidentielles, des données spécifiques permettant l'identification et l'authentification des transactions de l'utilisateur Ui sont téléchargées.

Avantageusement, ces données confidentielles peuvent comprendre également une ou plusieurs clé(s) privée(s) de chiffrement, ces clés étant alors utilisées pour chiffrer les données échangées ensuite entre le serveur AS et le terminal mobile TEL, par exemple au moyen d'un procédé de chiffrement asymétrique.

Ces données confidentielles sont stockées de manière sécurisée aussi bien dans le terminal mobile TEL que dans le serveur AS, par exemple de manière cryptée.

Avantageusement, les données confidentielles stockées dans le serveur d'authentification AS sont stockées dans des boîtiers HSM (pour Hardware Security Module en anglais) permettant d'éviter d'éventuelles compromissions internes chez l'opérateur exploitant le serveur AS. Sur le terminal mobile, les données confidentielles sont cryptées avant d'être stockées dans des espaces sécurisés du terminal mobile.

Une fois l'activation de l'application personnalisée ainsi que l'éventuelle transmission de données confidentielles effectuées, une sous-étape B4 d'enregistrement de l'authentification initiale du terminal mobile est réalisée.

Cette sous-étape B4 d'enregistrement de l'authentification initiale permet de garantir légalement que l'authentification ne puisse pas être remise par la suite, ce qui affaiblirait alors la valeur légale de l'ensemble du procédé d'authentification.

Cette étape d'authentification initiale peut être réalisée grâce à l'envoi d'un certain nombre de données d'authentification initiale d_{init} du terminal mobile de l'utilisateur Ui au serveur d'authentification AS.

Par exemple, l'utilisateur Ui peut être requis de présenter une pièce d'identité à la camera de son terminal mobile. Le cliché de cette pièce d'identité, pris par cette caméra, est ensuite chiffré et transmis au serveur AS où il est stocké. Un tel processus peut être complètement dématérialisé ou nécessiter l'intervention humaine pour la vérification de l'identité de l'utilisateur Ui.

La **figure 3B** illustre le système mettant en œuvre l'étape B d'activation de l'application personnalisée selon le principe de la présente invention, telle que décrite précédemment.

Sur cette figure 3B, les différents échanges effectués lors de l'étape d'activation décrite à la figure 3A sont illustrés.

En particulier, les flux de données correspondant à la sous-étape d'envoi B1 de téléchargement de l'application personnalisée dans le terminal

mobile TEL, la sous-étape B3 de téléchargement des données confidentielles dans le terminal mobile TEL et la sous-étape B4 d'enregistrement de l'authentification initiale auprès du serveur d'authentification AS sont indiqués.

Le serveur SP du fournisseur de services ainsi que l'ordinateur PC de l'utilisateur Ui ne sont pas concernés par cette étape d'activation.

La **figure 4A** illustre les sous-étapes d'un deuxième mode de réalisation de type « on-line » de l'étape E de génération du code d'autorisation.

Dans ce deuxième mode de réalisation « on-line », une fois que la donnée d'authentification d_{auth} a été lue par le terminal mobile, elle est transmise au serveur d'authentification AS lors d'une étape E1 de transmission.

Dans un premier mode particulier de réalisation, la donnée d'authentification peut être transmise directement au serveur AS, telle qu'elle est lue par le terminal mobile, ce qui simplifie et accélère le traitement au niveau du terminal mobile. Dans ce premier mode de réalisation, le terminal mobile n'a pour fonction que de lire la donnée d'authentification et tous les autres traitements sont réalisés sur le serveur d'authentification AS.

Dans un deuxième mode particulier de réalisation, la donnée d'authentification peut être interprétée et traitée au moins en partie dans le terminal mobile en vue de son transfert vers le serveur AS. En particulier, lorsqu'une paire de clés privée et publique de chiffrement a été téléchargées à partir de ce serveur d'authentification AS lors de l'étape B d'activation, la donnée d'authentification peut être chiffrée, par exemple avec un procédé de chiffrement asymétrique, avant d'être transmise au serveur AS afin d'empêcher quiconque d'accéder à cette donnée d'authentification.

Dans un troisième mode particulier de réalisation, tout le processus de génération du code d'autorisation peut être effectué dans le terminal mobile, auquel cas le serveur d'authentification AS ne sert qu'à effectuer des fonctions n'ayant pas de rapport avec la génération du code d'autorisation, comme le stockage de ce code ou la gestion de la traçabilité des transactions faites par l'utilisateur.

Une fois effectuée la transmission de la donnée d'authentification d_{auth} au serveur d'authentification AS, il est possible d'effectuer une étape d'identification de l'utilisateur Ui lors d'une étape optionnelle d'identification E2, afin de s'assurer que cette donnée d'authentification d_{auth} est bien transmise par l'intermédiaire de cet utilisateur.

Une sous-étape E3 d'authentification de la transaction requise par l'utilisateur peut ensuite être réalisée.

Le code d'autorisation cod_i proprement dit est alors généré dans le serveur d'authentification AS au cours d'une étape E4 de génération.

Une fois ce code d'autorisation généré, celui-ci est transmis (étape E5 de transmission du code) du serveur d'authentification AS au terminal mobile TEL, éventuellement sous une forme chiffrée grâce à une ou plusieurs clé(s) générée(s) durant l'étape B d'activation de l'application personnalisée, pour y être affiché.

La valeur du code d'autorisation générée permet de certifier que la donnée d'authentification a bien été comprise et sert à authentifier l'utilisateur.

Dans ce deuxième mode de réalisation de type « on-line » du procédé d'authentification, une fois le code d'autorisation saisi dans l'ordinateur de l'utilisateur Ui (étape F) et une fois les données transactionnelles transmises, avec le code d'autorisation saisi, de l'ordinateur personnel vers le serveur du fournisseur de services (étape G), il est avantageux d'effectuer, après la transaction proprement dite, une étape d'horodatage de la transaction afin de conserver une preuve de l'heure et la date à laquelle a été effectuée la transaction.

Dans le cas du mode de réalisation « on-line », un tel horodatage peut être effectué par le serveur d'authentification AS, dans une logique de traçabilité de la transaction.

La **figure 4B** illustre le système mettant en œuvre le procédé d'authentification selon un premier mode de réalisation de type « on-line » où le code d'autorisation est généré dans un serveur d'authentification AS distinct du serveur du fournisseur de services.

En particulier, les flux de données correspondant aux étapes d'enrôlement (étape A), d'envoi d'une donnée d'authentification (étape C), de lecture de cette donnée d'authentification (étape D), de saisie du code d'autorisation par l'ordinateur de l'utilisateur (étape E) et de transmission de la transaction au serveur du fournisseur de services (étape G) sont similaires à ceux décrits dans le mode de réalisation « off-line » et illustrés sur la figure 1B.

Ce premier mode de réalisation « on-line » se caractérise en ce que le terminal mobile transfère la donnée d'authentification au serveur d'authentification AS lors de la sous-étape E1, les différentes sous-étapes d'identification de l'utilisateur, d'authentification de la transaction et de génération du code d'autorisation cod_i (sous-étapes E2 à E4) étant alors réalisées dans ce serveur d'authentification AS avant que le code d'autorisation cod_i soit transmis au terminal mobile lors de la sous-étape de transmission E5.

Dans ce mode de réalisation particulier, une fois la transaction réalisée, elle peut être horodatée par le serveur SP du fournisseur de services, afin de servir de preuve à la disposition du fournisseur de services s'il y a lieu. L'historique des transactions horodatées est ainsi conservé au sein du serveur SP du fournisseur de services.

La **figure 4C** illustre le système mettant en œuvre le procédé d'authentification selon un deuxième mode de réalisation de type « on-line » où le code d'autorisation est généré dans le serveur SP du fournisseur de services sur lequel les fonctionnalités d'authentification décrites précédemment ont été installées.

Sur cette figure 4C, les différents flux de données décrits sont similaires que ceux décrits en référence à la figure 4B, à la seule différence près que le serveur d'authentification AS et le serveur SP du fournisseur de services forment une seule et même entité gérée par le fournisseur de services.

Ce mode de réalisation est particulièrement adapté aux applications demandant un niveau de sécurisation accru, et en particulier au domaine bancaire où des critères stricts de confidentialité des données s'appliquent,

notamment au niveau des échanges de données entre le module de transaction et le module d'authentification.

Dans ce mode de réalisation particulier, une fois réalisée, cette transaction peut être horodatée aussi bien par le module d'authentification que par le serveur SP proprement dit, afin de servir de preuve à la disposition du fournisseur de services s'il y a lieu. L'historique des transactions horodatées est ainsi conservé au sein du serveur SP du fournisseur de services.

Le serveur SP peut également conserver en mémoire d'autres données de traçabilité comme le contenu de la transaction ou l'identifiant de l'utilisateur.

Le procédé d'authentification décrit ci-avant permet de résister à la plupart, voire à toutes, des attaques connues et répertoriées dans un contexte de transaction d'authentification et/ou de signature sur internet, et qui visent à compromettre l'établissement d'une communication entre un client et un serveur et/ou en altérer le fonctionnement, dont la liste est donnée ci-dessous :

Attaque de type « Malware »

Il s'agit d'un nom générique pour les virus informatiques, les chevaux de Troyes, les logiciels espions, les keyloggers, etc... Les logiciels malveillants sont des applications utilisées à des fins frauduleuses. Ils peuvent accéder à un ordinateur par des vulnérabilités de sa protection par l'ingénierie sociale. Quand le logiciel malveillant est en cours d'exécution, il peut généralement prendre le contrôle complet de l'ordinateur et par exemple dérober les informations et les données personnelles de l'utilisateur, activer le contrôle à distance de l'ordinateur ou exécuter des actions au nom de l'utilisateur.

Avec la présente invention, les seules données personnelles sensibles sont stockées en espace sécurisé, auprès du serveur du fournisseur de services, elles sont hors de portée des malwares.

Par ailleurs, la copie de l'application personnalisée sur un autre terminal mobile que celui de l'utilisateur Ui est inutile sans les données confidentielles générées par le serveur AS. De même, la copie des données

confidentielles sur un autre terminal mobile rend ces données confidentielles non interprétables.

Attaque de type « Keylogging »

Les attaques de type « Keylogging » sont réalisées à l'aide de programmes parasites appelés « keyloggers » qui se propagent souvent grâce à des virus, des vers ou des spywares. Un « keylogger » a pour principale fonction d'espionner toutes les actions effectuées sur l'ordinateur de l'utilisateur (saisie au clavier, ouverture d'applications, déplacement de fichiers...). Les traces de ces actions sont stockées dans un emplacement précis, puis envoyées vers une boîte aux lettres ou sur un site web. Certaines des données les plus confidentielles peuvent ainsi être soutirées à l'insu de l'utilisateur.

Certains « keyloggers » sont excessivement perfectionnés et sont en mesure de sélectionner les informations les plus importantes. Ils parviennent, lorsque l'utilisateur est sur son site de banque en ligne par exemple, à identifier et récupérer ses codes bancaires. Ils peuvent aussi connaître le contenu saisi dans ses messages ou savoir précisément quels sont les programmes sollicités par l'utilisateur.

Avec la présente invention, encore une fois, les données personnelles de l'utilisateur Ui ne sont ni stockées ni utilisées par l'application personnalisée et les données permettant l'authentification de celui-ci sont à usage unique. Le « Keylogging » est donc inefficace.

Attaque de type « Phishing »

Lors d'une attaque de type « Phishing », autrement appelée hameçonnage, l'attaquant utilise un e-mail ou une messagerie instantanée pour mener l'utilisateur à un site web paraissant digne de confiance mais qui est en réalité une copie conforme du site original et sous son contrôle. Le message e-mail comme le site web pouvant être par exemple une réplique exacte d'un site de banque en ligne couramment visité par l'utilisateur. Celui-ci croit alors qu'il est sur un site digne de confiance (par exemple, celui de sa

banque) et saisit ses données personnelles d'identification telles que sont mot de passe, un mot de passe à usage unique, voire son numéro de carte bancaire.

L'attaquant peut ensuite utiliser ses informations pour accéder au compte de l'utilisateur ou effectuer des transactions frauduleuses à son insu (par exemple un virement bancaire ou un paiement en ligne s'il y a récupération du numéro de carte bancaire).

Avec la présente invention, une attaque de type « phishing » permet éventuellement de connaître la réponse unique à une donnée d'authentification donnée. Cependant, une telle réponse ne pourrait pas être réutilisée puisque la donnée d'authentification transmise par le fournisseur de services est générée et change à chaque fois.

Par ailleurs, en mode de sécurité renforcée, la donnée d'authentification permet une authentification mutuelle, ce qui entraîne le dévoilement du site de « fishing ».

Attaque de type « Pharming » ou « Whaling »

Ces sous-catégories d'attaques de type « phishing » (hameçonnage) permet de voler des informations après avoir attiré la victime sur un site web maquillé, même si le nom de domaine est correctement saisi.

Une attaque de type « pharming » (ou dévoiement en français) est une technique de piratage informatique exploitant des vulnérabilités au niveau du serveur DNS. Cette technique opère de manière à ce que, pour une requête DNS visant un nom de domaine particulier, ce ne soit pas la véritable adresse IP du nom de domaine qui soit donnée mais celle d'un site frauduleux.

Il existe deux types d'attaques de type « pharming ».

Le premier est type est réalisé par la modification d'un server DNS local. Les internautes demandant un nom de domaine se font diriger vers l'adresse IP d'un serveur frauduleux.

Le second type est réalisé au moyen d'un malware reconfigurant les paramètres réseaux du matériel informatique infecté, que ce soit un poste de travail ou un routeur. Cette reconfiguration agit de manière à ce que l'internaute

soit redirigé, pour des noms de domaines prédéterminés, vers l'adresse IP d'un serveur frauduleux.

Quant au « whaling », il s'agit d'une autre sous-catégorie d'attaque de type « phishing » (hameçonnage) ciblée sur des individus de haut niveau, pouvant être des cadres d'une entreprise ou des individus haut placés dans la hiérarchie d'un réseau dans l'attaque d'institutions financières. L'attaque visant un seul individu, est elle plus personnalisée et devient par conséquent plus convaincante mais aussi plus difficile à détecter.

Avec la présente invention, tout comme pour les attaque de type « phishing », des attaques de type « pharming » ou « whaling » permettent éventuellement de connaître la réponse unique à une donnée d'authentification donnée. Cependant, une telle réponse ne pourrait pas être réutilisée puisque la donnée d'authentification transmise par le fournisseur de services est générée et change à chaque fois.

Attaque de type "Man-in-the-Middle (MiTM)"

L'attaque de type « man in the middle » (littéralement « attaque de l'homme au milieu » ou « attaque de l'intercepteur » en français), parfois notée MiTM, est un scénario d'attaque dans lequel un pirate (l'attaquant) écoute une communication entre deux interlocuteurs et falsifie les échanges entre le client et l'hôte afin de se faire passer pour l'une des parties.

Cette attaque fait donc intervenir trois protagonistes : le client, le serveur et l'attaquant. Le but de l'attaquant est de se faire passer pour le client auprès du serveur et se faire passer pour le serveur auprès du client. Il devient ainsi l'homme du milieu. Cela permet de surveiller tout le trafic réseau entre le client et le serveur, et de le modifier à sa guise pour l'obtention d'informations telles que des mots de passe, un accès système, etc.

La plupart du temps, de telles attaques reposent sur l'utilisation les techniques de détournement de flux qui consistent à écouter le réseau à l'aide d'outils appelés « sniffer ».

Avec la présente invention, entre l'utilisateur Ui et le serveur d'authentification AS, toutes les transactions sont chiffrées, rendant inopérante une interception de type MiTM.

Une attaque de type MiTM entre l'utilisateur Ui et le serveur SP du fournisseur de services peut permettre d'intercepter le code d'autorisation, mais celui-ci est à usage unique donc non réutilisable

Une attaque de type « Man in the Middle » est donc sans effet avec la présente invention.

Man-in-the-Browser (MiTB)

Des outils, ainsi que la vigilance des utilisateurs, permettent désormais d'identifier les faux sites de type « Man-in-the-Middle », puisque leur adresse peut être incorrecte. Tandis que certains sont cryptés, l'inspection attentive de la certification de site Web peut prouver que le site n'appartient pas vraiment à qui il prétend. En outre, alors que les fraudeurs peuvent essayer de se relier au site Web (cible de l'attaque) à partir d'un ordinateur dans le même pays que le client, les systèmes de détection de fraude pourraient relever des caractéristiques soupçonneuses.

Pour ces raisons, les fraudeurs ont maintenant développé une variante plus sophistiquée de MitM – l'attaque de type « man in the browser » ou MitB.

Dans cette variante, au lieu d'intervenir entre l'ordinateur du client et le site Web de la banque, les interceptions de MitB agissent entre le client et son navigateur.

Une attaque de MitB est conçue en installant un logiciel malveillant (i.e. un malware) sur l'ordinateur du client. L'objectif est de permettre à l'attaquant de contrôler toutes les applications et tous les appareils non sécurisés connectés à l'ordinateur de l'utilisateur.

Ceci peut se produire lorsqu'un client ouvre un attachement d'email ou télécharge un dossier d'un site Web. Visiter un site Web, ou lire un email, peut être suffisant pour qu'un fraudeur puisse installer le malware sans permission du client. Dans certains cas les cybers criminels ont trifouillé des sites Web

légitimes existants, de sorte qu'ils infectent leurs visiteurs. Le client est peu susceptible de noter que quelque chose est différent.

Les technologies d'authentification forte classiques, tels que l'e-Banking par exemple, ne peuvent pas protéger contre une attaque de type « Man-in-the-Browser ». En effet, qu'il s'agisse de "tokens" classique de type OTP (Securid, Vasco, Aladdin, etc.) ou la technologie PKI (Certificat numérique) utilisée sur des supports comme une SmartCard, un Token USB (eToken, etc.), ces technologies n'offrent pas un niveau de sécurité suffisant pour prévenir les attaques de type « Man in the Browser ».

Avec la présente invention, tout comme pour les attaques MiTM, toutes les transactions sont chiffrées entre l'utilisateur Ui et le serveur d'authentification AS, ce qui rend inopérante une interception de type MiTB. Par ailleurs, une attaque de type MiTB entre l'utilisateur Ui et le serveur SP du fournisseur de services peut certes permettre d'intercepter le code d'autorisation, mais celui-ci est à usage unique donc non réutilisable

Une attaque de type « Man in the Browser » est donc sans effet avec la présente invention.

Attaque de type « ID Theft »

Dans ce type d'attaque, l'attaquant prétend être quelqu'un d'autre pour accéder par exemple à un système ou effectuer des transactions financières frauduleuses. Cette technique repose donc sur le principe de l'usurpation d'identité. Celle-ci débute toujours par la collecte de renseignements personnels sur l'individu fraudé. Les renseignements personnels peuvent être le nom, le numéro de téléphone, la date de naissance, l'adresse, le numéro d'assurance sociale, le numéro de carte de crédit, le mot de passe de carte de crédit ou de débit ou toute autre information permettant d'identifier la personne.

A cet effet, la prolifération des réseaux sociaux tels que FaceBook, MySpace, Linked-in, Twitter, Xing, Viadeo, etc., et leur utilisation massive rend facile cette collecte des informations mais aussi problématique leur sécurisation.

Les usurpateurs utilisent ensuite ces informations pour effectuer une ou des transactions en simulant l'identité de la personne fraudée. Par exemple, un fraudeur peut effectuer des appels téléphoniques ou faire des achats importants et diriger les frais vers la personne fraudée, il peut aussi retirer de l'argent du compte de banque de cette personne.

Avec la présente invention, les données personnelles de l'utilisateur ne sont pas utilisées lors du processus d'authentification. Une attaque de type « ID Theft » est donc inopérante.

Attaque de type « Social Engineering »

Ce type d'attaque n'est autre que le fait de faire réaliser à une personne une action dont elle n'aurait pas pris l'initiative seule. Le « social engineering » est une technique qui fonctionne, car elle fait appel à des caractéristiques humaines telles l'entraide ou la confiance. Pour arriver à ses fins, l'attaquant soulève différents leviers d'attaque tels que :

- L'amitié et la coopération : l'empathie, la sympathie, la détresse, la culpabilité. Il faut pour cela connaître le contexte de la cible, ainsi que certains aspects personnels du sujet. Cette méthode est relativement discrète mais nécessite souvent plusieurs tentatives.

- L'usurpation d'identité et l'intimidation : pouvoir et soumission, diffusion de responsabilités. Cette méthode est un peu plus risquée que la précédente. Il faut disposer d'un annuaire bien renseigné sur la société, de son organigramme. Cette méthode est plus rapide puisque dans la mesure où cette méthode est agressive, un seul essai est possible.

- Le sabotage : vise les administrateurs. Il s'agit de se faire connaître comme l'interlocuteur adéquat en cas de problème du SI. L'attaquant profite alors de la confiance instaurée. Cette méthode est peu discrète mais efficace.

- Diverses techniques associées : le « trash recovering » qui n'est autre que de la récupération de poubelles, le « shoulder surfing », qui pourrait se traduire par de la navigation au-dessus de l'épaule de la cible.

Le seul moyen de lutte reste ici la sensibilisation des utilisateurs. Elle est coûteuse en temps et en ressources mais peut cependant se réaliser. La

meilleure parade consiste à retirer l'information à l'utilisateur, la classifier et la chiffrer à travers un système d'authentification physique et/ou logique (token, biométrie, code 2D).

Avec la présente invention, tout comme pour une attaque de type « ID Theft », une attaque de type « Social engineering » est inopérante car les données personnelles de l'utilisateur ne sont pas utilisées lors du processus d'authentification.

Attaque de type « Cross-Channel »

Dans ces attaques, une brèche ouverte dans la sécurité d'un canal est utilisée pour accéder à d'autres canaux. Les contraintes de sécurité différentes d'un canal à un autre expliquent qu'il est plus facile d'attaquer un canal et de procéder à la fraude sur un autre.

Par exemple, l'attaquant pourrait utiliser des données personnelles obtenues sur le canal de commerce en ligne pour se connecter à la banque en ligne. Dès lors, il devient nécessaire de procéder à une séparation des domaines pour se prémunir contre ce type d'attaque.

Avec la présente invention, les données confidentielles sont spécifiques au fournisseur de service, ce qui réduit drastiquement les possibilités d'attaque de type « cross-channel ».

En cas de faiblesse due à une trop forte mutualisation de services dans un groupe de fournisseurs donné, une attaque de type « cross-channel » reste sans effet, car elle ne permet d'intercepter que des données confidentielles à usage unique, donc non réutilisables.

Attaque de type « Card-Not-Present »

Dans des environnements où une carte est requise (par exemple, une carte de paiement), cette attaque consiste en une transaction pendant laquelle la carte n'est pas présente sur le site du commerçant. Ceci comprend les commandes dite sur internet, le téléphone et le courrier électronique, plus communément appelées MoTo (Mail Order / Telephone Order).

Contrairement à une transaction où la carte est présente et généralement assortie de la saisie d'un code personnel (Code PIN) dont l'utilisateur à seule la connaissance, la carte n'étant pas présente, le marchand ne peut pas vérifier que la transaction est réellement effectuée par le propriétaire de la carte. En effet un attaquant peut copier les informations de la carte auprès de son propriétaire et les utiliser ensuite pour procéder à des transactions de type « card-not-present ».Avec la présente invention dans le mode de réalisation « on-line », l'identification de l'utilisateur, l'authentification de la transaction et l'horodatage sont réalisés. L'ensemble de ces éléments est dont traçable. L'utilisation de règlementations éventuelles pour une répudiation technique ne permet que la répudiation du moyen et non de l'acte et permet un recours judiciaire indiscutable.

La présente invention concerne aussi un serveur d'authentification AS comprenant un module de réception arrangé pour recevoir la donnée d'authentification d_{auth} ainsi qu'au moins une donnée interne d'identification d_{int} provenant du serveur SP du fournisseur de service, des moyens de calcul arrangés pour générer un code d'autorisation cod_i en fonction de la donnée d'authentification reçue et d'au moins une des donnée internes d'identification reçues, ainsi qu'un module d'émission arrangé pour émettre le code d'autorisation cod_i généré vers le terminal mobile TEL.

Un tel serveur d'authentification AS peut être utilisé dans le mode de réalisation « on-line » tel que décrit à la figure 4B, dans lequel la fonctionnalité d'authentification de la transaction, au moyen de la donnée d'authentification $d_{auth,}$ est effectuée dans un serveur distinct du fournisseur de service.

La présente invention concerne également un système d'authentification d'un utilisateur requérant une transaction auprès d'un fournisseur de service comprenant un écran SCN arrangé pour afficher une donnée d'authentification reçue du fournisseur de service, un terminal mobile TEL disposant de moyens de saisie de la donnée d'authentification affichée sur l'écran et arrangé pour retourner un code d'autorisation spécifique à l'utilisateur et à la transaction requise, et des moyens de saisie PC permettant l'envoi du code d'autorisation au fournisseur de service afin d'authentifier l'utilisateur. Ce système est par

exemple décrit à la figure 1B. Dans un mode particulier de réalisation, ce système implique un serveur d'authentification tel que décrit précédemment.

Dans un autre mode particulier de réalisation, le système comprend en outre le serveur SP du fournisseur de service, ce serveur étant arrangé pour fournir le service requis par l'utilisateur, et comprenant un module de réception arrangé pour recevoir au moins une donnée personnelle de l'utilisateur et le code d'autorisation émis par l'utilisateur, des moyens de calcul arrangé pour générer au moins une donnée interne d'identification à partir d'au moins une des données personnelles reçues, et un module d'émission arrangé pour envoyer la donnée interne d'identification générée au serveur d'authentification AS.

Un tel serveur SP de fourniture de service peut être utilisé dans le mode de réalisation « on-line » tel que décrit à la figure 4B, dans lequel la fonctionnalité de fourniture de service est effectuée dans un serveur distinct de celui effectuant l'authentification de la transaction.

Bien entendu, l'invention n'est pas limitée aux exemples de réalisation ci-dessus décrits et représentés, à partir desquels on pourra prévoir d'autres modes et d'autres formes de réalisation, sans pour autant sortir du cadre de l'invention.

Ainsi, toutes ou partie des étapes mises en œuvre par le terminal mobile TEL sont effectuées dans un mode de réalisation suite à l'exécution d'instructions de programmes d'ordinateur sur des moyens de calcul du terminal mobile TEL. Similairement, tout ou partie des étapes mises en œuvre par le serveur d'authentification AS sont effectuées dans un mode de réalisation suite à l'exécution d'instructions de programmes d'ordinateur sur des moyens de calcul de ce serveur AS.

Par ailleurs, le terme de fournisseur de services utilisé précédemment recouvre tout opérateur apte à fournir un service dans lequel une transaction est effectuée. Un tel fournisseur peut être par exemple, à titre purement illustratif, un opérateur bancaire, un opérateur de jeux en ligne, un opérateur de télécommunications, un loueur de véhicules ou de vélos, etc.

REVENDICATIONS

1. Procédé d'authentification d'un utilisateur (Ui) requérant une transaction auprès d'un fournisseur de service (SP), le procédé comportant la génération (E) d'un code d'autorisation (cod_i) spécifique à l'utilisateur et à la transaction requise à partir d'une donnée d'authentification (d_{auth}) lue sur un écran au moyen d'un terminal mobile (TEL) et l'envoi (F) du code d'autorisation généré au fournisseur de service afin d'authentifier l'utilisateur.

2. Procédé d'authentification selon la revendication 1, caractérisé en ce que la donnée d'authentification lue est interprétée dans le terminal mobile au moyen d'une application personnalisée (APP_i) spécifique à l'utilisateur et téléchargée (B1) à partir d'un serveur d'authentification (AS).

3. Procédé d'authentification selon la revendication 2, caractérisé en ce que l'application personnalisée (APP_i) téléchargée dans le terminal mobile génère (E) le code d'autorisation à partir de la donnée d'authentification lue.

4. Procédé d'authentification selon la revendication 1 ou 2, caractérisé par la transmission (E1) de la donnée d'authentification lue du terminal mobile au serveur d'authentification (AS), la génération (E4) du code d'autorisation à partir de la donnée d'authentification dans le serveur d'authentification (AS), et la transmission (E5) du code d'autorisation généré au terminal mobile.

5. Procédé d'authentification selon l'un des revendications 2 à 4, dans lequel un lien de téléchargement pointant vers l'application personnalisée générée est envoyé à l'utilisateur, le procédé comprenant en outre une étape d'activation (B) au cours de laquelle le terminal mobile télécharge l'application personnalisée au moyen du lien de téléchargement.

6. Procédé d'authentification selon la revendication 5, caractérisé en ce que l'étape d'activation comprend la transmission d'au moins une donnée confidentielle ($scrt_i$) spécifique à l'utilisateur au terminal mobile, ladite donnée confidentielle servant à chiffrer la donnée d'authentification dans le terminal mobile avant sa transmission au serveur d'authentification et/ou à déchiffrer le code d'autorisation reçu par le terminal mobile.

7. Procédé d'authentification selon l'une des revendications 2 à 6, caractérisé par une étape préalable d'enrôlement (A) au cours de laquelle l'application personnalisée (APP_i) et/ou la donnée confidentielle ($scrt_i$) est générée en fonction d'au moins une donnée interne d'identification (d_{int}) générée à partir d'au moins une donnée personnelle d'identification (d_{id}) envoyée par l'utilisateur au fournisseur de service.

8. Procédé d'authentification selon la revendication 7, caractérisé en ce que l'étape d'enrôlement comprend la transmission d'un code d'activation (PIN) au terminal mobile, ledit code d'activation étant utilisé lors de l'étape d'activation pour activer l'application personnalisée téléchargée.

9. Procédé d'authentification selon la revendication 8, caractérisé en ce que l'étape d'enrôlement comprend une étape de vérification de l'identité de l'utilisateur avant la transmission du code d'activation, ladite transmission n'étant effectuée que si ladite vérification est effectuée de façon positive.

10. Procédé d'authentification selon l'une des revendications 1 à 9, caractérisé en ce que la donnée d'authentification est générée par le fournisseur de service de façon spécifique à l'utilisateur et à la transaction requise.

11. Procédé d'authentification selon l'une des revendications 1 à 10, caractérisé en ce que l'étape d'envoi du code d'autorisation comprend la lecture du code d'autorisation affiché par le terminal mobile par des moyens de

lecture d'un ordinateur et l'envoi du code d'autorisation lu vers le fournisseur de service.

12. Serveur d'authentification (AS) caractérisé en ce qu'il comprend :

- un module de réception arrangé pour recevoir une donnée d'authentification et au moins une donnée interne d'identification ;

- des moyens de calcul arrangés pour générer un code d'autorisation en fonction de la donnée d'authentification reçue et d'au moins une des donnée internes d'identification reçues, ledit code d'autorisation étant spécifique à un utilisateur, identifié au moyen de la donnée interne d'identification, et à une transaction requise par ledit utilisateur, authentifiée au moyen de la donnée d'authentification; et

- un module d'émission arrangé pour émettre le code d'autorisation généré vers un terminal mobile.

13. Système d'authentification d'un utilisateur (Ui) requérant une transaction auprès d'un fournisseur de service (SP), le système comprenant un écran (SCN) arrangé pour afficher une donnée d'authentification reçue du fournisseur de service, un terminal mobile (TEL) disposant de moyens de saisie de la donnée d'authentification affichée sur l'écran et arrangé pour retourner un code d'autorisation spécifique à l'utilisateur et à la transaction requise, et des moyens de saisie (PC) permettant l'envoi du code d'autorisation au fournisseur de service afin d'authentifier l'utilisateur.

14. Système d'authentification selon la revendication 13, caractérisé en ce qu'il comprend en outre un serveur d'authentification selon la revendication 12.

15. Système d'authentification selon la revendication 14, caractérisé en ce qu'il comprend un serveur (SP) arrangé pour fournir un service requis par l'utilisateur, ledit serveur de service comprenant un module de réception arrangé pour recevoir au moins une donnée personnelle de l'utilisateur et le

code d'autorisation émis par l'utilisateur, des moyens de calcul arrangé pour générer au moins une donnée interne d'identification à partir d'au moins une des données personnelles reçues, et un module d'émission arrangé pour envoyer la donnée interne d'identification générée au serveur d'authentification (AS) .

FIG.1A.

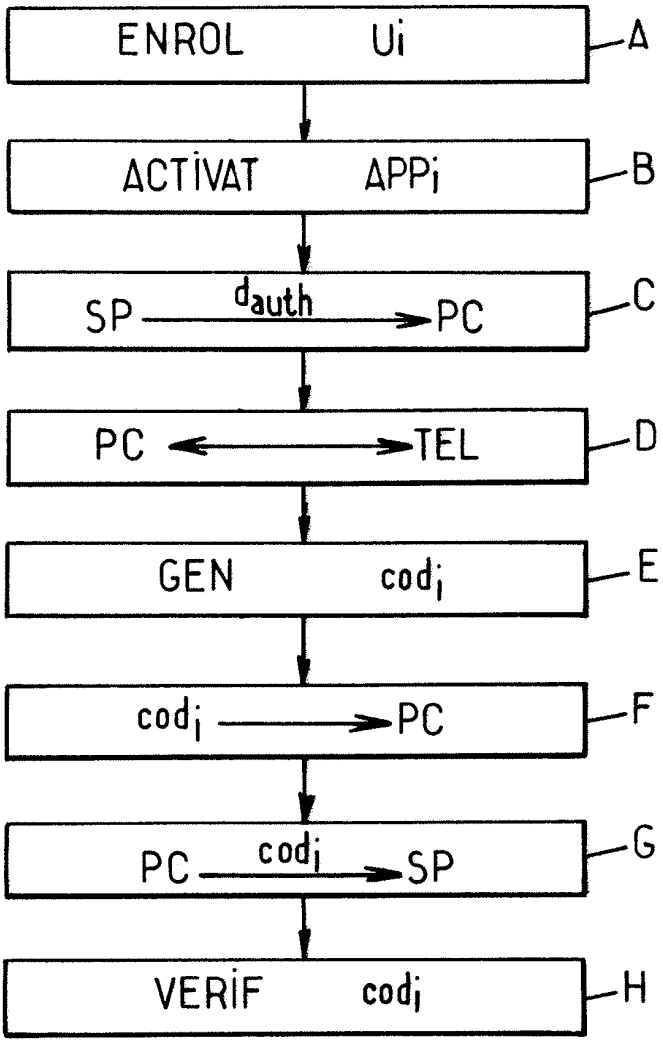
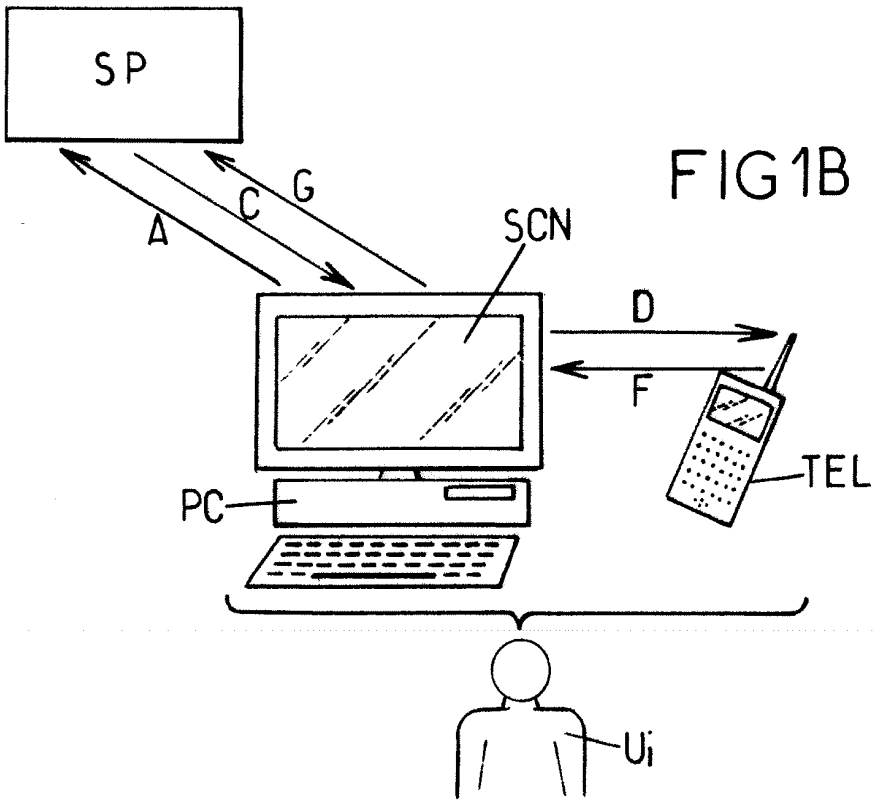

ENROL Ui
A
ACTIVAT APPi
B
SP dauth PC
C
PC TEL
D
GEN codi
E
codi PC
F
PC codi SP
G
VERIF codi
H

FIG1B


SP
A
C
G
SCN
D
F
TEL
PC
Ui

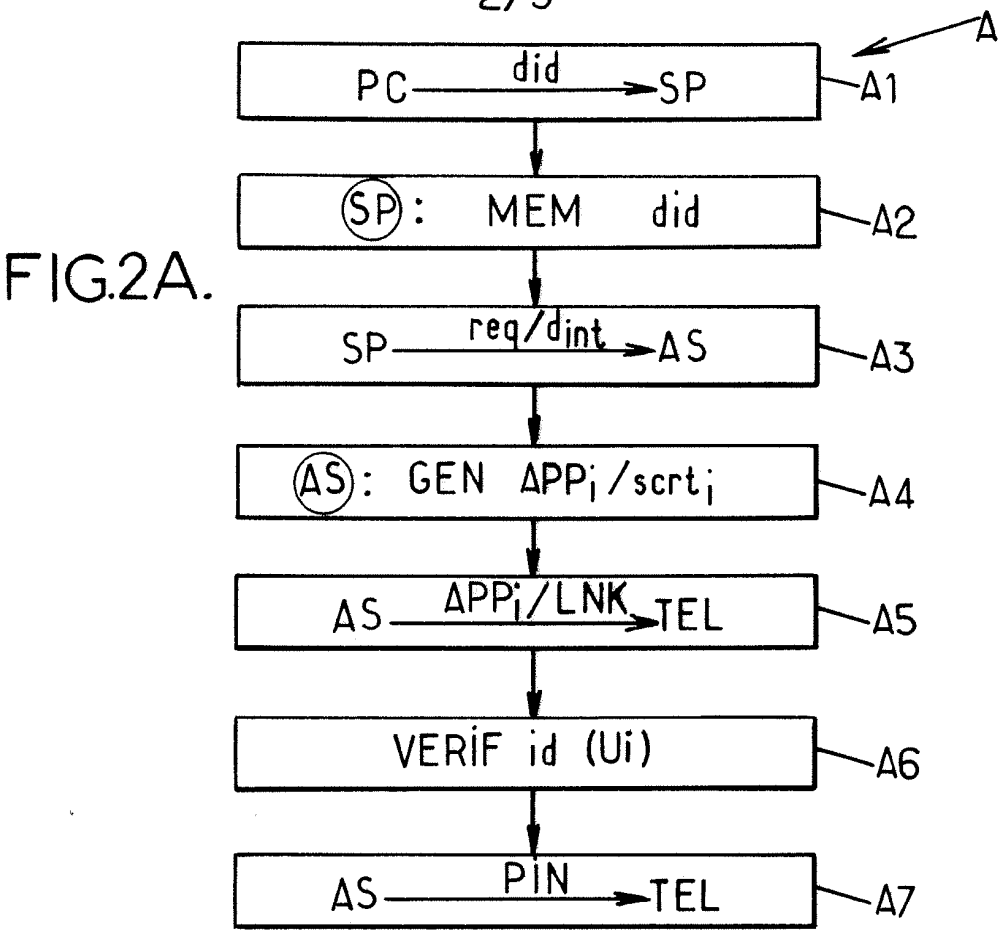

A
PC
did
SP
A1
SP : MEM did
A2
SP
req/dint
AS
A3
AS : GEN APPi/scrti
A4
AS
APPi/LNK
TEL
A5
VERIF id (Ui)
A6
AS
PIN
TEL
A7

FIG.2A.

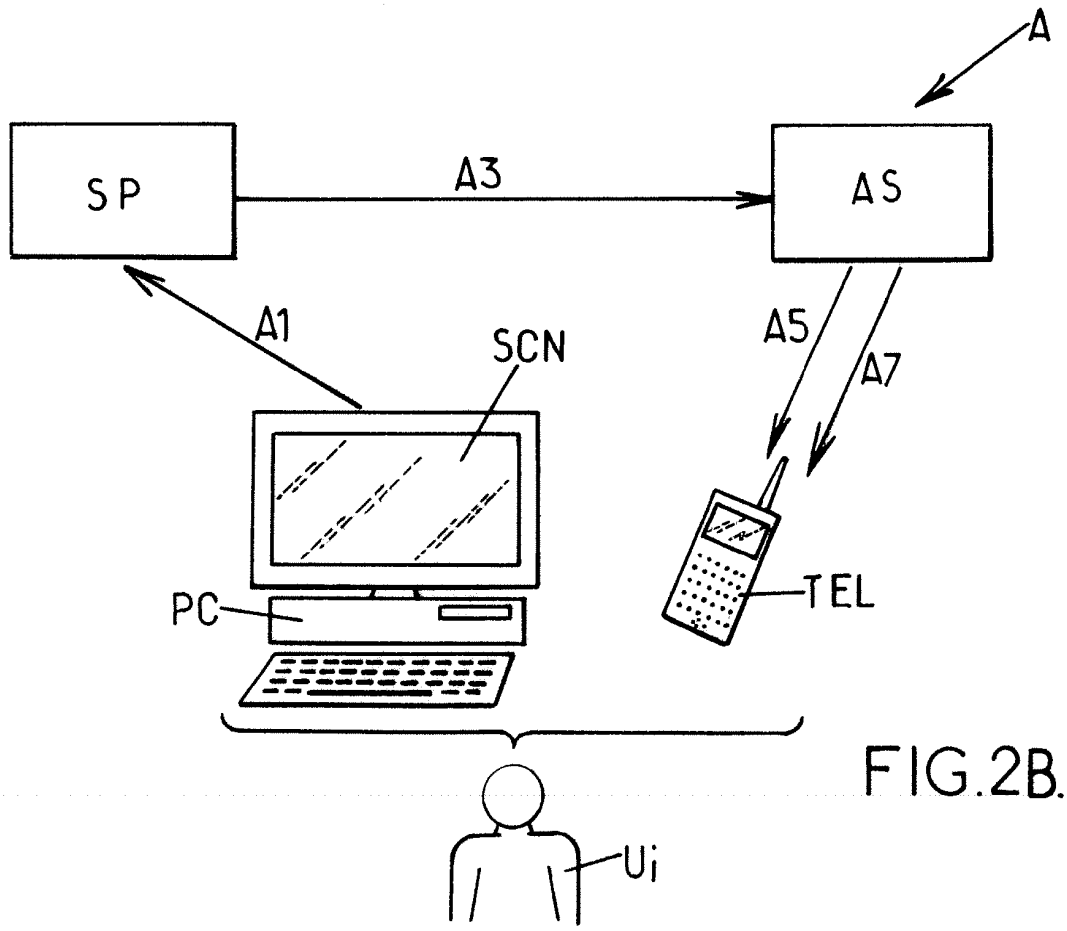
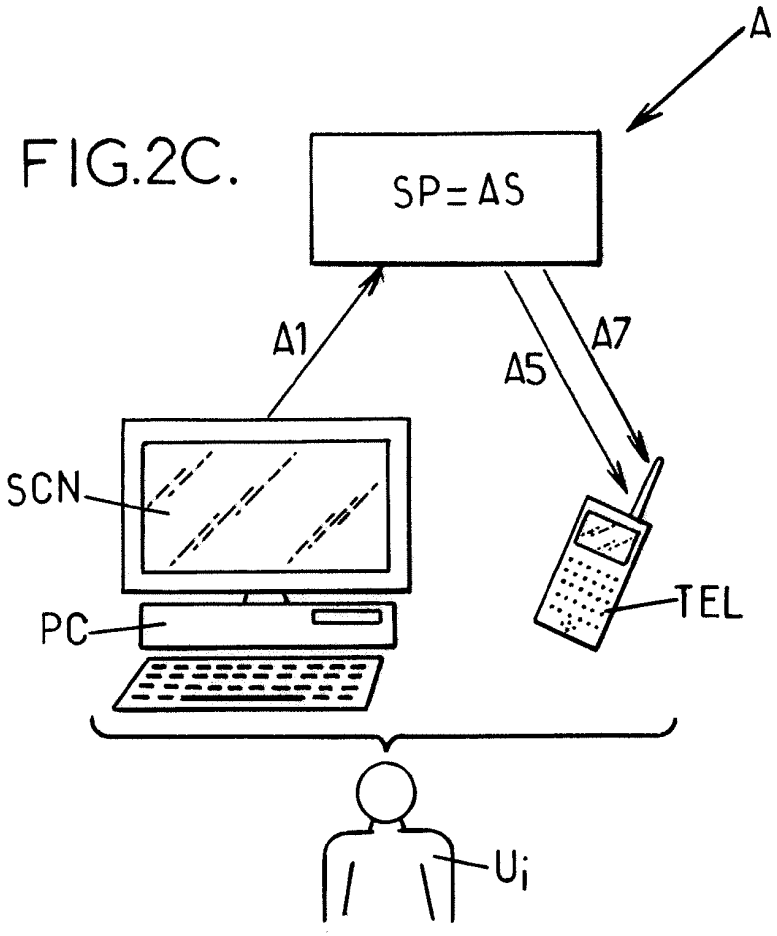

A
SP
A3
AS
A1
SCN
A5
A7
PC
TEL
Ui

FIG.2B.

FIG.2C.


A
SP=AS
A1
A5
A7
SCN
PC
TEL
Ui

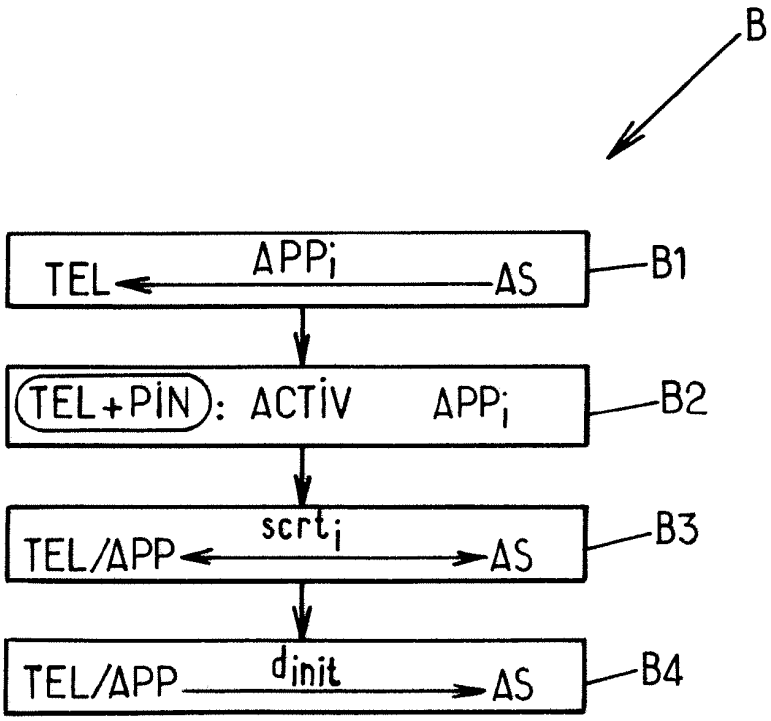

B
TEL
APPi
AS
B1
TEL+PIN
: ACTIV
APPi
B2
TEL/APP
scrti
AS
B3
TEL/APP
dinit
AS
B4

FIG.3A.

FIG.3B.

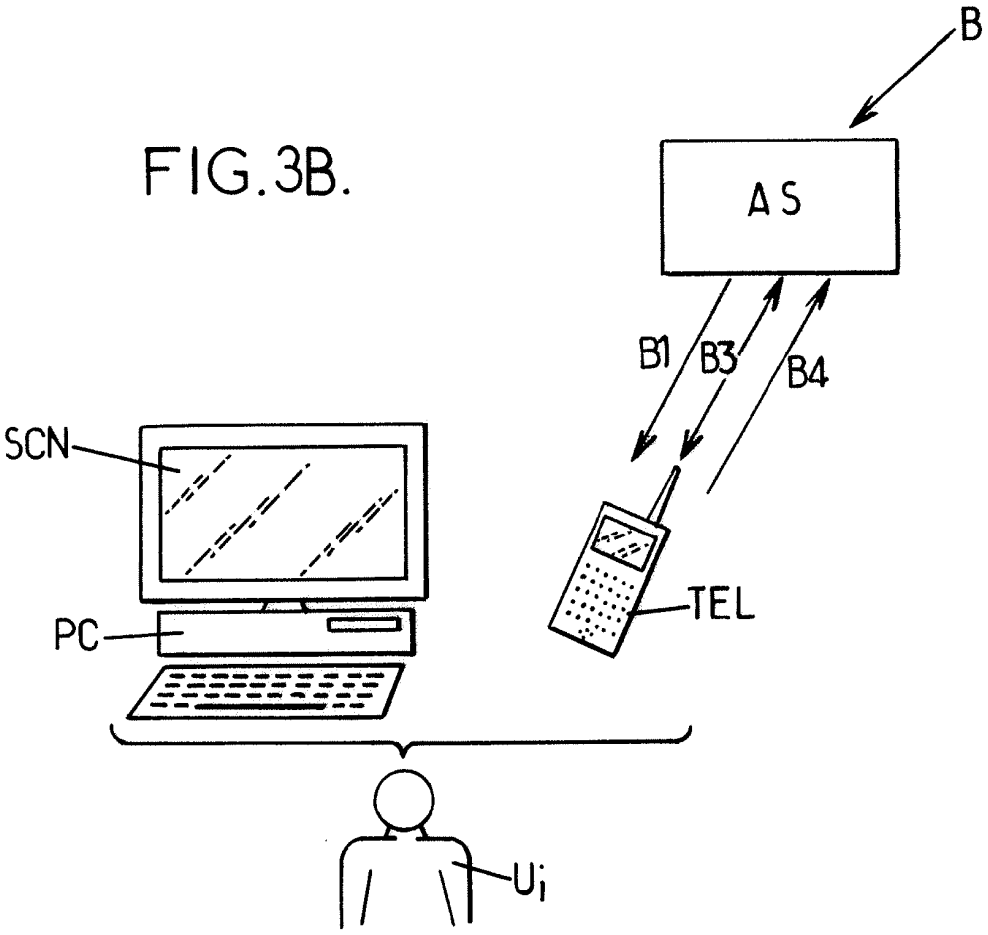

B
AS
B1
B3
B4
SCN
PC
TEL
Ui

FIG.4A.

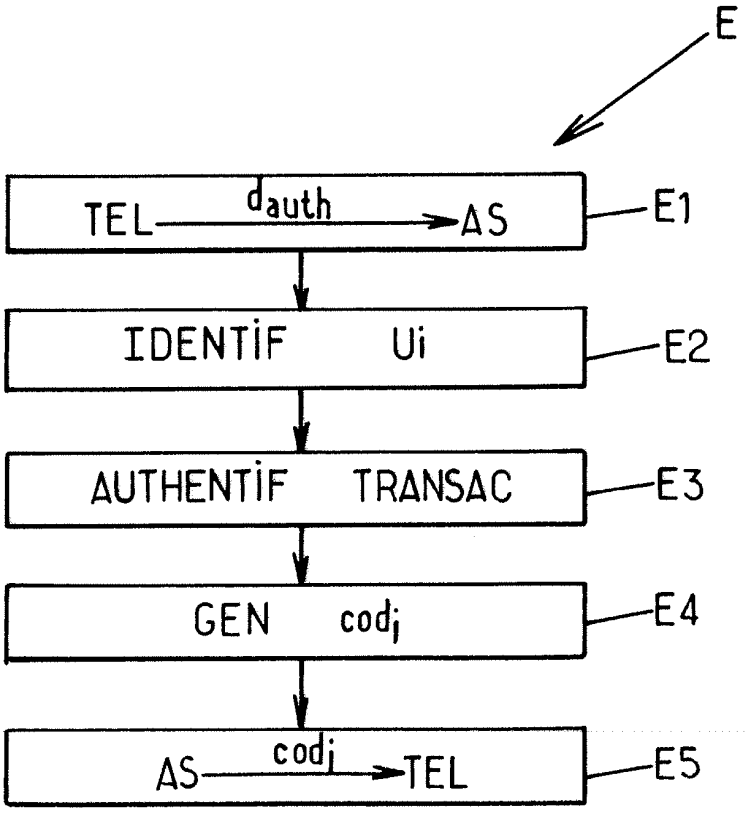

E
TEL
dauth
AS
E1
IDENTIF Ui
E2
AUTHENTIF TRANSAC
E3
GEN codi
E4
AS
codi
TEL
E5

FIG.4B.

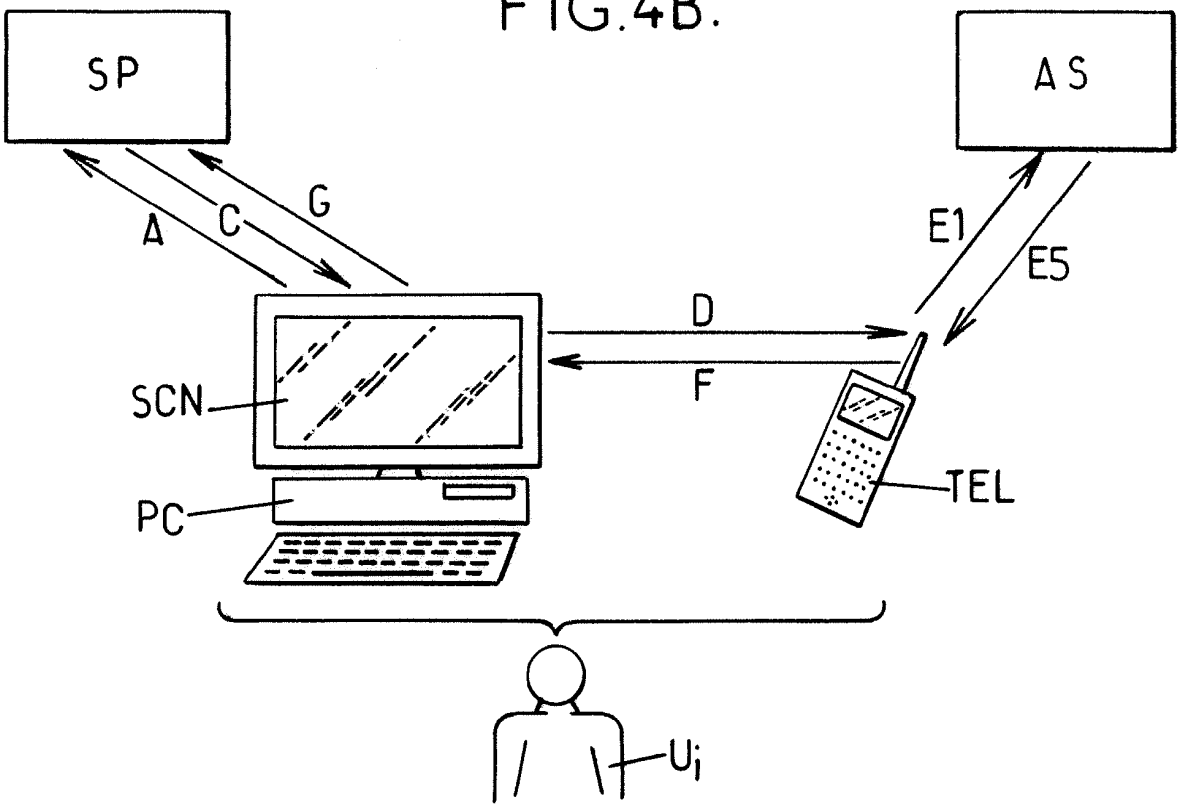
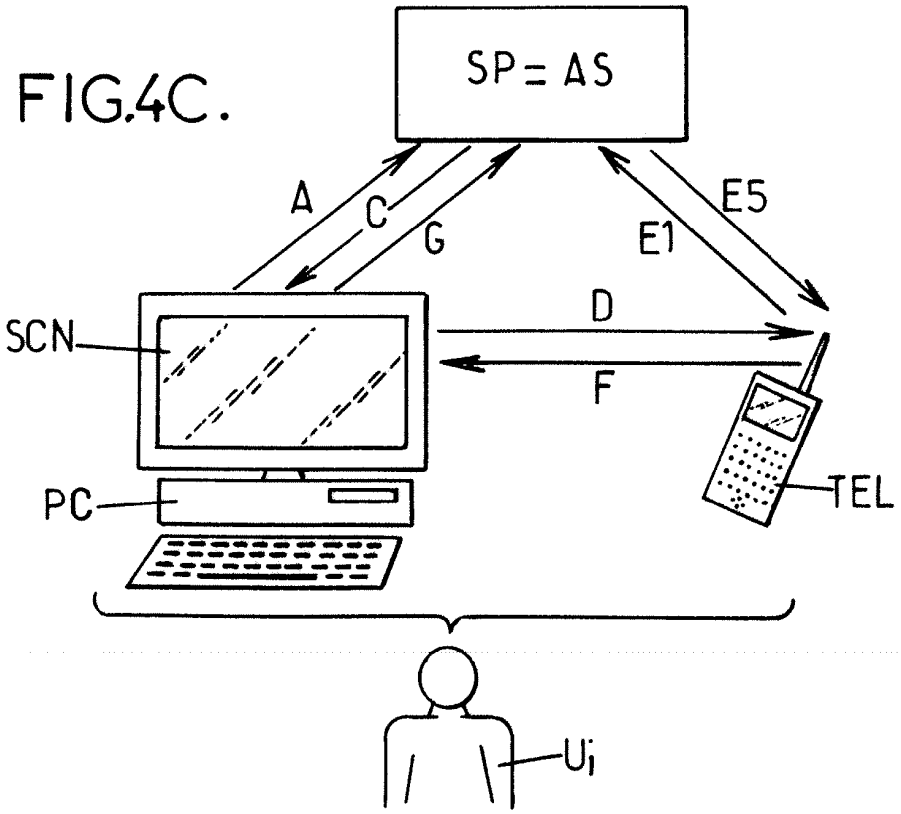


FIG.4C.



RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 741390
FR 1053523

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
X Y	FR 2 852 471 A1 (FRANCE TELECOM [FR]) 17 septembre 2004 (2004-09-17) * abrégé * * page 3, ligne 9 - page 4, ligne 8 * * page 5, ligne 30 - page 7, ligne 15 * -----	1-4,7-15 5,6	H04L 9/32 G06F 21/22
X Y	EP 1 840 814 A1 (HITACHI SOFTWARE ENG [JP]) 3 octobre 2007 (2007-10-03) * abrégé * * alinéa [0008] - alinéa [0016] * * alinéa [0048] - alinéa [0095] * * alinéa [0109] - alinéa [0169] * * figures 1-3,6,12,17 * -----	1-4,7-15 5,6	
X A	WO 2009/134213 A2 (RADIANTRUST PTE LTD [SG]; TANG WENG SING [SG]; LEE PERN CHERN [SG]; NU) 5 novembre 2009 (2009-11-05) * page 3, ligne 1 - page 7, ligne 15 * * page 12, ligne 7 - page 15, dernière ligne * -----	1,4, 10-15 2,3,5-9	
Y A	WO 01/56352 A2 (MAGICAXESS [FR]; KREMER GILLES [FR] MAGICAXESS [FR]; KREMER GILLES [FR]) 9 août 2001 (2001-08-09) * abrégé * * page 16, ligne 20 - page 20, ligne 3 * * page 32, ligne 5 - ligne 8 * -----	5,6 1-4,7-15	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L G09C
E	WO 2010/116109 A1 (LYNKWARE [FR]; PANZA MAURO [FR]) 14 octobre 2010 (2010-10-14) * le document en entier * -----	1-5, 13-15	

Date d'achèvement de la recherche	Examinateur
22 février 2011	Bec, Thierry

CATÉGORIE DES DOCUMENTS CITÉS

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 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1053523 FA 741390

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 22-02-2011
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
FR 2852471 A1	17-09-2004	WO 2004082354 A2	30-09-2004
EP 1840814 A1	03-10-2007	CN 101038653 A	19-09-2007
		JP 2007249726 A	27-09-2007
		US 2007220597 A1	20-09-2007
WO 2009134213 A2	05-11-2009	US 2011026716 A1	03-02-2011
WO 0156352 A2	09-08-2001	AU 5488301 A	14-08-2001
		CA 2377626 A1	09-08-2001
		EP 1192608 A2	03-04-2002
		EP 1253564 A2	30-10-2002
		US 2002138450 A1	26-09-2002
WO 2010116109 A1	14-10-2010	FR 2944400 A1	15-10-2010

EPO FORM P0465