

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

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(10) Numéro de publication internationale

WO 2014/001704 A1

(43) Date de la publication internationale
3 janvier 2014 (03.01.2014)

WIPO | PCT

(51) Classification internationale des brevets :
H04B 13/00 (2006.01) G06Q 20/04 (2012.01)
G06K 19/07 (2006.01) G06K 7/10 (2006.01)

(74) Mandataire : FRANCE
TELECOM/OLNC/OLPS/IPL/PAT; RENARD Béatrice,
38-40 rue du Général Leclerc, F-92794 Issy Moulineaux
Cedex 9 (FR).

(21) Numéro de la demande internationale :
PCT/FR2013/051475

(22) Date de dépôt international :
25 juin 2013 (25.06.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1255992 25 juin 2012 (25.06.2012) FR

(71) Déposant : ORANGE [FR/FR]; 78 rue Olivier de Serres,
F-75015 Paris (FR).

(72) Inventeurs : LEROY, Patrick; 5bis route de Verson, F-
14740 Saint Monvieux - Norrey (FR). MAYER, Emma-
nuel; 7 avenue des Clairières, F-14123 Ifs (FR).

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

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ,
TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

[Suite sur la page suivante]

(54) Title : METHOD OF AUTHENTICATION BETWEEN A MOBILE TERMINAL AND A PROCESSING TERMINAL

(54) Titre : PROCEDE D' AUTHENTIFICATION ENTRE UN TERMINAL MOBILE ET UN TERMINAL DE TRAITEMENT

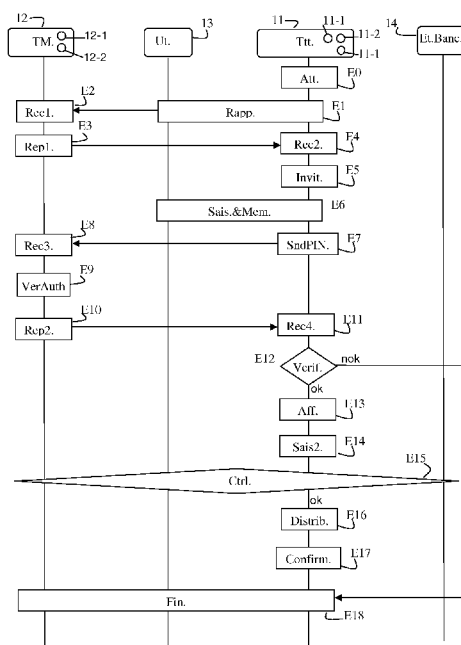


Figure 2

14 Bank Est.
E1 Approach
E6 Entry&Mem.
E13 Disp.
E14 Entry2
E18 End

(57) Abstract : The invention concerns a method of authentication between a mobile terminal (12), located at a distance less than a predefined distance from the body of a user (13), the mobile terminal comprising an antenna (12-1) constituting a radio interface suitable for transmitting and receiving radio signals through the body of the user, and a processing terminal suitable for transmitting and receiving radio signals through the body of the user, the method comprising: - a step (E1) of approaching a user interface (11-3) of the processing terminal with a portion of the body, said approach triggering an activation of the processing terminal and the establishment of communication between the processing terminal and the mobile terminal, - a step (E5) requesting the entering of a piece of personal authentication data, - a step (E6) of memorising the personal data entered, - a step (E7) of sending said personal authentication data through the body, - a step (E11) of receiving a piece of data representing the result of a check of the personal authentication data carried out by the terminal of the user, - a step (E12) of checking said piece of received data, authentication being successful when the check is positive. (Figure 2)

(57) Abrégé :

[Suite sur la page suivante]



EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, **Publiée :**

LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,

GW, KM, ML, MR, NE, SN, TD, TG).

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

L'invention concerne un procédé d'authentification entre un terminal mobile (12), situé à une distance inférieure à une distance prédéterminée du corps d'un utilisateur (13), le terminal mobile comprenant une antenne (12-1) constituant une interface radio adaptée pour émettre et recevoir des signaux radioélectriques à travers le corps de l'utilisateur, et un terminal de traitement adapté pour émettre et recevoir des signaux radioélectriques à travers le corps de l'utilisateur, le procédé comprenant : - une étape (E1) de rapprochement d'une partie du corps avec une interface utilisateur (11-3) du terminal de traitement, ledit rapprochement déclenchant un réveil du terminal de traitement et l'établissement d'une communication entre le terminal de traitement et le terminal mobile, - une étape (E5) d'invitation à saisir une donnée personnelle d'authentification, - une étape (E6) de mémorisation de la donnée personnelle saisie, - une étape (E7) d'envoi, à travers le corps de ladite donnée personnelle d'authentification, - une étape (E11) de réception d'une donnée représentant le résultat d'une vérification de la donnée personnelle d'authentification réalisée par le terminal de l'utilisateur, - une étape (E 12) de vérification de ladite donnée reçue, l'authentification étant réussie lorsque la vérification est positive. (Figure 2)

PROCEDE D' AUTHENTIFICATION ENTRE UN TERMINAL MOBILE ET UN TERMINAL DE TRAITEMENT

Procédé d'authentification

L'invention concerne un procédé d'authentification mis en œuvre au moyen d'un terminal mobile. Plus précisément, l'invention porte sur une authentification d'un utilisateur au cours d'une transaction entre un équipement mobile, porté par l'utilisateur et un terminal de traitement. L'équipement mobile n'est pas exposé lors de cette authentification et reste dans la poche, ou dans un sac proche du corps de l'utilisateur. En effet, l'authentification, réalisée par un élément de sécurité inséré dans le terminal mobile utilise les capacités conductrices du corps humain pour échanger des informations entre le terminal de traitement et le terminal mobile.

L'invention trouve une application particulièrement intéressante dans de nombreux services de communication en champ proche, mis en œuvre au moyen d'un terminal mobile, pour lesquels il n'est plus nécessaire d'exposer le terminal mobile au risque de se le faire voler. Ainsi, de tels services peuvent être utilisés en toute sécurité par les utilisateurs.

La technologie de communication en champ proche (on parle habituellement de « NFC », pour « Near Field Communication ») est une technologie de communication sans fil qui s'est largement développée ces dernières années. Ainsi de nombreuses expérimentations de services sur mobile basées sur cette technologie ont été lancées. On peut citer des services de micro-paiement, des services qui utilisent des tickets de transport dématérialisés ; on parle habituellement d'application de « ticketing » ou de « e-ticket ». Par exemple, dans le cas d'un service de ticketing pour transports en commun, un utilisateur équipé d'un terminal mobile NFC sur lequel est installée une application propre à ce service de transport, recharge dans un premier temps un compte dédié. A cette fin, il achète un nombre déterminé de tickets et recharge ce compte sur son terminal mobile auprès d'une borne NFC dédiée à cet usage. Lorsqu'ensuite, il souhaite emprunter le transport en commun, il approche son terminal mobile d'une borne NFC dédiée à ce service et située dans le véhicule de transport. Le compte propre au service est alors décrétement du nombre de ticket nécessaire pour effectuer un trajet et l'utilisateur est autorisé à effectuer le trajet. Cependant certains services nécessitent la saisie d'une donnée d'authentification de l'utilisateur destinée à prouver que l'utilisateur qui tente d'utiliser le terminal mobile pour un service donné est bien le détenteur légitime du terminal. Cette donnée est par exemple un code d'identification personnel, ou code « PIN » de service (pour « Personal Identification Number »). La saisie d'un code PIN correct et donc une authentification réussie de l'utilisateur permet en général de débloquent l'application installée sur le terminal mobile afin qu'elle s'exécute. Des services qui nécessitent la saisie d'un code PIN sont par exemple des services de paiement, pour lesquels un certain niveau de sécurité est requis. La sécurité est alors garantie par cette authentification préalable de l'utilisateur.

On connaît par ailleurs la technologie Body Area Network (ou Wireless Body Area Network) qui permet des communications sans fil entre des capteurs miniatures à même le corps et une unité de traitement portée par l'utilisateur. Cette technologie est décrite dans la thèse de Thomas Guthrie Zimmerman « Personal Area Networks (PAN) : Near-Field Intra-Body Communication ». La demande de brevet de la demanderesse publiée sous le numéro
5 WO2012/1314224 décrit un dispositif et un système de communication adaptés pour mettre en œuvre une communication à travers le corps de l'utilisateur entre un dispositif porté par l'utilisateur, ou dispositif portable, et une station de base équipée d'une surface sensitive sur laquelle l'utilisateur approche ou pose sa main pour assurer la communication entre la station de
10 base et le dispositif. La technique décrite dans cette demande de brevet est mise en œuvre dans le cadre d'un service de ticketing. Dans cette demande de brevet, la station de base est agencée pour fonctionner selon des cycles successifs d'émission/réception continus de durée respective prédéfinie. Ainsi, lors d'une première période d'émission de durée déterminée la station de base émet un premier signal électrique modulé associé à un message de recherche/d'interrogation. Le
15 dispositif portable qui était jusque-là en état d'attente, détecte et reçoit le premier signal électrique modulé véhiculé par le corps de l'utilisateur. Le signal modulé reçu est démodulé par le dispositif portable puis analysé. La détection et la réception du premier signal déclenche le passage du dispositif portable en mode émission pendant une deuxième période prédéfinie. Le dispositif portable répond alors au premier message reçu en calculant un nouveau solde de
20 tickets et en construisant un message numérique de réponse. Le message numérique de réponse est alors modulé par le dispositif portable en un deuxième signal électrique modulé qui est envoyé, via une interface radio du dispositif, à travers le corps de l'utilisateur. Dans une période suivante de réception, la station de base reçoit alors le deuxième signal électrique modulé via une antenne radio. Le deuxième message électrique modulé est démodulé et son contenu
25 analysé de manière à autoriser au non l'utilisateur à emprunter le transport en commun. Ainsi, la station de base est agencée pour être alternativement en mode émission pendant une première période donnée et en mode réception pendant une deuxième période donnée. Le dispositif porté par l'utilisateur est lui, dans un état d'attente jusqu'à recevoir un signal électrique modulé qui le fait passer en mode émission pendant une période donnée, puis en mode réception pendant une
30 autre période donnée.

Le dispositif portable et la station de base comprennent un modulateur, un démodulateur, une interface radio destinée à émettre et recevoir des signaux électriques modulés à travers le corps d'un utilisateur, et des moyens de commutation adaptés pour connecter alternativement l'interface radio au modulateur suite à la réception d'un signal électrique modulé puis au
35 démodulateur suite à l'émission d'un signal électrique modulé.

Dans un exemple particulier de réalisation, le dispositif portatif est un terminal mobile équipé d'une antenne NFC, ladite antenne constituant l'interface radio du dispositif, et l'utilisation de ce terminal est illustrée dans le cadre d'un service de ticketing. Ainsi, l'utilisateur peut utiliser son terminal mobile pour emprunter les transports en commun en exécutant une application NFC mémorisée sur son terminal mobile, sans sortir son terminal mobile de sa poche ou de son sac. Cependant, lorsque l'on souhaite utiliser le dispositif et le procédé dans un service NFC sécurisé, au cours duquel il est demandé à l'utilisateur de saisir une donnée qui lui est propre, tel un code PIN, l'utilisateur doit sortir son téléphone de son sac ou de sa poche pour saisir le code PIN sur le clavier de son terminal. Ceci expose le terminal de l'utilisateur dans un lieu public et augmente le risque de vol. Ainsi, une telle technologie sans contact perd de son intérêt à partir du moment où une authentification de l'utilisateur est requise.

Un des buts de l'invention est de remédier à des insuffisances/inconvénients de l'état de la technique et/ou d'y apporter des améliorations.

A cette fin, l'invention propose un procédé d'authentification entre un terminal mobile, situé à une distance inférieure à une première distance prédéterminée du corps d'un utilisateur, le terminal mobile comprenant une antenne constituant une interface radio adaptée pour émettre et recevoir des signaux radioélectriques, et un terminal de traitement adapté pour émettre et recevoir des signaux radioélectriques, les signaux radioélectriques étant transmis entre le terminal mobile et le terminal de traitement en utilisant une capacité de conductivité du corps de l'utilisateur, le procédé comprenant :

- une étape de détection qu'une partie du corps de l'utilisateur est située à une distance inférieure à une deuxième distance prédéterminée d'une interface utilisateur du terminal de traitement, ladite détection déclenchant un réveil du terminal de traitement et l'établissement d'une communication entre le terminal de traitement et le terminal mobile,

- une étape d'invitation de l'utilisateur par le terminal de traitement à saisir une donnée personnelle d'authentification,

- une étape d'envoi au terminal mobile d'un signal radioélectrique comprenant ladite donnée personnelle d'authentification,

- une étape de réception d'un signal radioélectrique émis par le terminal mobile comprenant une donnée représentant le résultat d'une vérification de la donnée personnelle d'authentification réalisée par le terminal mobile,

- une étape de vérification de ladite donnée reçue, l'authentification étant réussie lorsque la vérification est positive.

Avec le procédé de l'invention, l'authentification de l'utilisateur, nécessaire pour déclencher l'exécution d'une application mémorisée sur le terminal mobile de l'utilisateur se fait sans que l'utilisateur ait à sortir son terminal mobile pour saisir sa donnée personnelle d'authentification sur le clavier du terminal. En effet, la donnée personnelle d'authentification est saisie par l'utilisateur sur une interface utilisateur du terminal de traitement, puis transmise par celui-ci au terminal mobile qui effectue alors la vérification avec une donnée d'authentification de référence préalablement mémorisée sur le terminal en association avec l'application. Ainsi, le terminal mobile n'est pas exposé durant la transaction avec le terminal de traitement, puisque celui-ci reste dans le sac ou dans la poche de l'utilisateur. Le risque de vol du terminal mobile au moment de la saisie de la donnée personnelle d'authentification est donc limité.

Dans un mode de réalisation particulier, le procédé comprend en outre une étape de mémorisation de la donnée personnelle saisie.

Selon un exemple de réalisation, la vérification de la donnée personnelle d'authentification réalisée par le terminal mobile consiste à comparer la donnée saisie avec une donnée de référence, mémorisée dans un élément de sécurité du terminal mobile.

Avantageusement, l'antenne du terminal mobile constituant l'interface radio adaptée pour émettre et recevoir des signaux radioélectriques est une antenne NFC.

Dans ce mode de réalisation, le procédé propose une authentification de transactions dans le cadre de services NFC mis en œuvre sur le terminal mobile. La technologie NFC est actuellement en plein essor et de nombreux services sont envisagés ou déjà en expérimentation. L'utilisation du procédé de l'invention dans le cadre de tels services permet à l'utilisateur d'envisager de tels services en toute confiance puisque le risque non négligeable de vol de son terminal mobile est écarté. D'autre part, l'utilisation du service est pratique et facile puisque l'utilisateur interagit avec le terminal de traitement par le biais de son propre corps.

Selon un exemple de réalisation de l'invention, la donnée personnelle d'authentification saisie et la donnée représentant le résultat de la vérification sont transmises de manière sécurisée.

L'échange sécurisé de la donnée personnelle d'authentification saisie par l'utilisateur, et de la donnée de contrôle représentant le résultat de la vérification permet de renforcer la sécurité du service en limitant les risques de récupération de ces informations par écoute de la voie radio.

Dans un exemple de réalisation de l'invention, l'étape d'invitation consiste à afficher sur l'interface utilisateur du terminal de traitement un clavier numérique comprenant des chiffres dans lequel l'ordre d'affichage des chiffres est aléatoire.

La sécurité du service de retrait bancaire est renforcée puisque l'affichage des chiffres du clavier dans un ordre aléatoire évite à quelqu'un de malintentionné de repérer la donnée personnelle d'authentification par observation de l'utilisateur lors de la saisie de cette donnée.

Dans un autre exemple de réalisation, l'interface utilisateur du terminal de traitement est
5 équipée d'un filtre de confidentialité, rendant une observation par un tiers impossible lors de la saisie.

La sécurité d'un service, par exemple de retrait, est renforcée puisque le filtre ne permet pas à quelqu'un situé à proximité de l'utilisateur de lire l'écran du terminal de traitement lors de la saisie par l'utilisateur de la donnée personnelle d'authentification. En effet un tel filtre
10 nécessite d'être dans l'axe de l'écran pour voir effectivement ce qui apparaît sur l'écran.

L'invention concerne aussi une utilisation du procédé d'authentification tel que décrit précédemment dans un service de retrait bancaire, le procédé comprenant en outre, après une vérification positive :

- une étape d'invitation à saisir un montant,
- 15 - une étape de mémorisation d'un montant déterminé, choisi par l'utilisateur,
- une phase de dialogue avec un établissement bancaire pour obtenir une autorisation de débit,
- si le débit est autorisé, une étape de distribution dudit montant.

Le procédé de l'invention est utilisé dans le cadre d'un service de retrait bancaire. Le
20 terminal mobile a préalablement mémorisé l'application de retrait soumise à authentification. Le procédé de l'invention renforce la sécurité de ce type de service. En effet, l'utilisateur n'a pas à sortir une carte bancaire de sa poche ou de son sac, puisque l'application de retrait est mémorisée sur le terminal mobile. D'autre part, la saisie de la donnée personnelle d'authentification se fait sans que l'utilisateur ne sorte son terminal mobile de sa poche ou de
25 son sac. Ainsi, la sécurité de ce genre de service est renforcée.

Dans un exemple d'utilisation du procédé de l'invention dans un service de retrait bancaire, un message de confirmation de transaction est envoyé au terminal mobile de l'utilisateur.

La confirmation de la transaction de retrait est transmise directement au terminal mobile
30 au moyen par exemple d'un message SMS. Ainsi, l'utilisateur n'a pas à se soucier de récupérer et de stocker un ticket papier résumant la transaction. L'utilisateur peut par ailleurs traiter ce message comme il le souhaite. Notamment il peut facilement l'archiver sans risque de perte.

L'invention concerne aussi un terminal de traitement comprenant une interface radio agencée pour émettre et recevoir des signaux radioélectriques, les signaux radioélectriques étant
35 transmis entre un terminal mobile, situé à une distance inférieure à une première distance

prédéterminée du corps d'un utilisateur, et le terminal de traitement en utilisant une capacité de conductivité du corps de l'utilisateur, le terminal de traitement comprenant :

- une unité de traitement ;
- une interface utilisateur, couplée à l'interface radio, agencée pour détecter qu'une
- 5 partie du corps de l'utilisateur du terminal mobile est située à une distance inférieure à une deuxième distance prédéterminée, ladite détection déclenchant un réveil du terminal de traitement et l'établissement d'une communication entre le terminal de traitement et le terminal mobile,
- des moyens d'invitation, agencés pour inviter l'utilisateur à saisir une donnée
- 10 personnelle d'authentification,
- des moyens d'envoi, agencés pour envoyer un signal radioélectrique comprenant ladite donnée personnelle d'authentification au terminal mobile,
- des moyens de réception, agencés pour recevoir un signal radioélectrique émis par le terminal mobile comprenant une donnée représentant le résultat d'une vérification de la donnée
- 15 personnelle d'authentification réalisée par le terminal mobile,
- des moyens de vérification, agencés pour vérifier ladite donnée reçue.

Dans un mode particulier de réalisation, le terminal de traitement comprend en outre des moyens de mémorisation, agencés pour mémoriser la donnée personnelle d'authentification saisie.

- 20 Dans un exemple de réalisation, le terminal de traitement comprend en outre une plaque métallique posée au sol, destinée à maintenir la communication entre le terminal de traitement et le terminal mobile, lorsqu'un utilisateur pose ses pieds sur ladite plaque.

La plaque métallique permet de maintenir un contact entre le terminal de traitement et le terminal mobile de l'utilisateur et de prévenir toute rupture de communication entre les deux

25 entités. Cet élément rend plus fiable l'utilisation du service.

L'invention concerne aussi un système d'authentification comprenant :

- un terminal de traitement tel que décrit précédemment, et
- un terminal mobile adapté pour émettre et recevoir des signaux radioélectriques, situé
- à une distance inférieure à une distance prédéterminée du corps d'un utilisateur, les signaux
- 30 électriques étant transmis entre le terminal mobile et le terminal de traitement en utilisant une capacité de conductivité du corps de l'utilisateur.

L'invention porte également sur un programme sur un support de données et chargeable dans la mémoire interne d'un terminal de traitement, le programme comprenant des portions de code pour l'exécution des étapes du procédé d'authentification tel que décrit précédemment,

35 lorsque le programme est exécuté sur ledit terminal.

L'invention concerne aussi un support de données sur lequel est enregistré le programme d'ordinateur tel que décrit précédemment.

De nombreux détails et avantages de l'invention seront mieux compris à la lecture de la description d'un mode particulier de réalisation en référence aux dessins annexés donnés à titre non limitatif, et dans lesquels :

- la figure 1 est une représentation schématique d'un système d'authentification selon un premier exemple de réalisation de l'invention ;
- la figure 2 présente les étapes d'un procédé d'authentification, selon un premier exemple de réalisation ;
- la figure 3 est une représentation schématique d'un terminal de traitement selon un premier exemple de réalisation.

Un système d'authentification 10 va maintenant être décrit en relation avec la figure 1 dans un mode de réalisation particulier.

Le système 10 comprend un terminal de traitement 11 et un terminal mobile 12. Un utilisateur 13, détenteur du terminal mobile 12 joue un rôle actif dans le système 10. L'utilisation du système 10 est illustrée dans le cadre d'un service de retrait bancaire. Ainsi, dans l'exemple de réalisation décrit, le terminal de traitement 11 est un distributeur bancaire. Le terminal de traitement 11 et le terminal mobile 12 sont adaptés pour émettre et recevoir des signaux radioélectriques à travers le corps de l'utilisateur 13 via des antennes respectives 11-1, 12-1. Par la suite, une émission à travers le corps de l'utilisateur correspond à une émission d'un signal radioélectrique en utilisant une capacité de conductivité du corps de l'utilisateur. Une réception à travers le corps de l'utilisateur correspond alors à une réception d'un tel signal radioélectrique. Dans un mode de réalisation particulier, le terminal mobile 12 et le terminal de traitement 11 fonctionnent conformément aux dispositifs décrits dans la demande de la demanderesse publiée sous le numéro WO2012/1314224. Selon cette demande, un premier dispositif et un deuxième dispositif portatif, porté par l'utilisateur, sont agencés pour fonctionner selon des cycles successifs d'émission/réception continus de durée respective prédéfinie. Ainsi, lors d'une première période d'émission de durée déterminée, le premier dispositif émet un premier signal électrique modulé associé à un message de recherche/d'interrogation. Le deuxième dispositif qui était jusque-là en état d'attente, détecte et reçoit le premier signal électrique modulé véhiculé par le corps de l'utilisateur. Le signal modulé reçu est démodulé par le deuxième dispositif puis analysé. La détection et la réception du premier signal déclenche le passage du deuxième dispositif en mode émission pendant une

deuxième période prédéfinie. Le deuxième dispositif répond alors au premier message reçu en construisant un message numérique de réponse. Le message numérique de réponse est alors modulé par le deuxième dispositif en un deuxième signal électrique modulé qui est envoyé, via l'antenne du deuxième dispositif, à travers le corps de l'utilisateur. Dans une période suivante de réception, le premier dispositif reçoit alors le deuxième signal électrique modulé via son antenne radio. Le deuxième message électrique modulé est démodulé et son contenu analysé. Ainsi, le premier dispositif est agencé pour être alternativement en mode émission pendant une première période donnée et en mode réception pendant une deuxième période donnée. Le deuxième dispositif, porté par l'utilisateur, est lui, dans un état d'attente jusqu'à recevoir un signal électrique modulé qui le fait passer en mode émission pendant une période prédéfinie. Les deux dispositifs échangent ainsi au moyen de signaux radioélectriques modulés des informations qui permettent de mettre en œuvre des services. L'invention décrite dans la demande de brevet publiée sous le numéro WO2012/1314224 est illustrée dans le cadre d'un service qui utilise des tickets de transport dématérialisés (on parle habituellement de service de « ticketing »).

Dans le cadre de la présente invention, le terminal de traitement 11 comprend une première interface utilisateur 11-2, adaptée pour transmettre des informations à l'attention de l'utilisateur. La première interface utilisateur 11-2 est par exemple un écran sur lequel des messages sont affichés. Dans un autre exemple de réalisation, la première interface 11-2 est un haut-parleur adapté pour diffuser des messages vocaux. Le terminal de traitement 11 comprend également une deuxième interface utilisateur 11-3, adaptée pour recevoir des informations du terminal mobile 12 à travers le corps de l'utilisateur, et pour transmettre des informations au terminal mobile 12 à travers le corps de l'utilisateur 13. Dans un exemple de réalisation, la deuxième interface 11-3 est une surface sensitive adaptée pour réagir lorsque l'utilisateur l'effleure ou est en contact avec elle. Par exemple, l'utilisateur peut poser sa main sur la surface sensitive 11-3. La surface sensitive 11-3 est couplée à l'antenne 11-1 et reçoit et transmet des signaux radioélectriques à travers cette antenne. Le terminal de traitement 11 est décrit plus en détail en relation avec la figure 3. Dans l'exemple de réalisation du procédé qui va être décrit en relation avec la figure 2, le terminal de traitement 11 est un distributeur bancaire connecté à un établissement bancaire distant 14. Le distributeur et l'établissement bancaire 14 sont connectés au moyen d'une liaison spécialisée, ou à travers un réseau, par exemple le réseau Internet.

Le terminal mobile 12 est adapté pour établir des communications mobiles à travers un réseau de télécommunications mobile, par exemple un réseau « GSM » (de l'anglais « Global System for Mobile communications ») « UMTS » (de l'anglais « Universal Mobile Telecommunications System »), et pour fonctionner en mode NFC. Le fonctionnement en mode

NFC permet d'exécuter des applications dites NFC, préalablement installées dans une zone mémoire sécurisée d'un élément de sécurité 12-2 inséré dans le terminal 12 (une telle zone est habituellement appelée « container »). L'élément de sécurité est par exemple une carte « SIM » (pour « Subscriber Identity Module »). A cet effet, le terminal mobile 12 est équipé d'une

5 antenne NFC. Cette antenne NFC est adaptée pour émettre/recevoir une composante magnétique d'une onde électromagnétique et également une composante électrique de cette même onde. Cette antenne NFC constitue également l'interface radio 12-1 adaptée pour émettre et recevoir des signaux radioélectriques à travers le corps de l'utilisateur 13. On comprend qu'ainsi, le terminal mobile 12, équipé d'une seule antenne NFC, peut à la fois réaliser des

10 transactions NFC et également des transactions à travers le corps de l'utilisateur. Une application NFC sécurisée (non représentée sur la figure 1) est mémorisée dans l'élément de sécurité 12-2 du terminal mobile 12. Cette application est associée à une donnée personnelle d'authentification de référence (non représentée sur la figure 1) paramétrée par l'utilisateur 13. La donnée personnelle d'authentification de référence, mémorisée dans l'élément de sécurité

15 12-2 en association avec l'application NFC sécurisée est destinée à contrôler l'accès à ladite application. Ainsi, si l'utilisateur souhaite exécuter l'application NFC sécurisée, il lui est dans un premier temps demandé de saisir la donnée personnelle d'authentification associée à l'application. Si la donnée d'authentification saisie est identique à la donnée d'authentification de référence préalablement mémorisée dans l'élément de sécurité, alors l'application NFC est

20 exécutée. Dans l'exemple de réalisation du procédé qui va être décrit en relation avec la figure 2, l'application NFC sécurisée est une application de retrait bancaire.

Le terminal mobile 12 est situé à proximité de l'utilisateur 13, sans nécessairement être en contact direct avec celui-ci. Par exemple, le terminal mobile 12 est placé à l'intérieur d'une poche ou d'un sac porté contre l'utilisateur 13. Dans ces configurations, on estime que le

25 terminal mobile 12 n'est pas éloigné de plus de quelques centimètres du corps de l'utilisateur 13. La distance est par exemple inférieure à six centimètres. Un signal radioélectrique émis par l'antenne 12-1 du terminal mobile est alors transmis au travers du corps de l'utilisateur en utilisant la capacité de conductivité du corps humain et est reçu au moyen de la deuxième interface 11-3 du terminal de traitement. Réciproquement, un signal radioélectrique émis par

30 l'antenne 11-1 du terminal de traitement est transmis au moyen de la deuxième interface 11-3 à travers le corps de l'utilisateur en utilisant la capacité de conductivité du corps humain et est reçu par l'antenne 12-1 du terminal mobile.

Les étapes d'un procédé d'authentification, selon un exemple de réalisation, vont

35 maintenant être décrites en relation avec la figure 2.

Le procédé d'authentification d'une transaction est illustré dans le cadre d'un service de retrait bancaire. Le terminal de traitement 11 est un distributeur qui comprend comme première interface 11-2 un écran et comme deuxième interface 11-3 une surface sensitive que l'utilisateur peut effleurer ou sur laquelle il peut poser la main.

- 5 Pour effectuer une opération bancaire de type retrait, l'utilisateur doit préalablement s'authentifier. L'authentification a pour but d'identifier l'utilisateur et de prouver que l'utilisateur est bien la personne qu'il prétend être. Classiquement, lorsqu'un utilisateur souhaite effectuer un retrait bancaire au moyen d'une carte de crédit qui constitue l'élément de sécurité permettant une authentification de l'utilisateur, il insère sa carte de crédit dans un distributeur.
- 10 Le distributeur affiche alors un message invitant l'utilisateur à saisir un code confidentiel attaché à sa carte. Le code est censé n'être connu que de l'utilisateur, ce qui permet de valider l'identité de l'utilisateur. Le code saisi est alors vérifié localement, c'est-à-dire uniquement avec la carte, ce qui permet de mettre en œuvre l'opération financière entre l'utilisateur, plus précisément sa carte bancaire via le distributeur, et un établissement bancaire distant. Des
- 15 échanges sécurisés sont alors initiés entre la carte et l'établissement bancaire distant afin d'autoriser le retrait si les données bancaires de l'utilisateur en possession de l'établissement bancaire le permettent.

Dans le contexte de l'invention, l'utilisateur n'a pas à insérer sa carte bancaire dans le distributeur.

- 20 Dans une étape initiale E0 d'attente, il est affiché sur la première interface 11-2, en l'espèce l'écran du terminal de traitement 11 un message invitant l'utilisateur 13 à allumer son terminal mobile 12 ou à s'assurer que celui-ci est allumé, et à poser une partie de son corps, par exemple sa main sur la deuxième interface 11-3, en l'espèce la surface sensitive du terminal de traitement 11. Cet état E0 est un état de veille dans lequel le terminal de traitement 11 attend
- 25 d'être réveillé par une action de l'utilisateur. Dans cet état le terminal de traitement 11 est inactif, il n'émet ni ne reçoit aucune trame de données. La partie du message affichée sur l'écran 11-1 et relative au terminal mobile 12 est destinée à s'assurer qu'une communication peut être établie entre le terminal mobile 12 et le terminal de traitement 11. En effet, on comprend que si le terminal mobile 12 est éteint, alors aucune communication ne peut être établie entre le
- 30 terminal de traitement 11 et le terminal 12 et le procédé d'authentification ne peut s'exécuter. On suppose ici que le terminal mobile 12 de l'utilisateur est allumé.

- Dans une étape suivante E1 de rapprochement, l'utilisateur 13 pose sa main sur la surface sensitive 11-3 du terminal de traitement 11. Cette étape E1 de rapprochement est destinée à déclencher le réveil du terminal de traitement 11 et à établir une communication entre
- 35 le terminal de traitement 11 et le terminal mobile 12, à travers le corps de l'utilisateur 13. Le

contact de l'utilisateur 13 avec la surface sensitive 11-3 du terminal de traitement 11 est détecté par le terminal de traitement 11 et déclenche le réveil du terminal de traitement 11 et l'envoi par ce terminal d'un premier signal électrique modulé transportant une première trame de données via l'antenne 11-1 vers le terminal mobile 12 à travers le corps de l'utilisateur. Cette trame est
5 destinée à établir un contact entre les deux entités. Avec ce premier signal, le terminal de traitement 11 signale sa présence au terminal mobile 12 et lui demande de s'identifier.

L'établissement d'une communication entre deux entités est réalisée de manière connue dans une phase appelée habituellement « handshake », ou poignée de main. La phase de handshake consiste à échanger plusieurs trames préalables entre deux entités permettant
10 d'échanger de premiers paramètres afin de rendre possible un dialogue entre les deux entités.

Dans une étape E2 de réception par le terminal mobile, le terminal mobile 12, jusque-là en état d'attente, reçoit le premier signal électrique modulé correspondant à la trame d'établissement d'un contact, via l'antenne 12-1 du terminal mobile. Cette étape est destinée à informer le terminal mobile 12 que la communication en cours est établie en NFC via le corps
15 de l'utilisateur entre le terminal mobile 12 et le terminal de traitement 11.

Dans une étape E3 de réponse, le terminal mobile 12 envoie un deuxième signal électrique modulé correspondant à une deuxième trame de données. Ce deuxième signal électrique modulé est destiné à répondre au terminal de traitement 11 qu'un terminal mobile est présent et que ce terminal sait dialoguer avec le terminal de traitement 11 à travers le corps de
20 l'utilisateur, dans le même langage que celui du terminal de traitement 12.

Dans une étape E4 de réception par le terminal de traitement, le terminal de traitement 11 reçoit le deuxième message électrique modulé à travers le corps de l'utilisateur via l'antenne 11-1 couplée à la surface sensitive 11-3. A ce stade, le terminal de traitement 11 est assuré qu'il peut dialoguer avec le terminal mobile 12.

25 Les étapes E1 à E4 constituent la phase de poignée de main, ou de handshake, préalable au dialogue entre le terminal mobile 12 et le terminal de traitement 11.

Dans une étape E5 d'invitation par le terminal de traitement, il est affiché sur l'écran 11-2 du terminal de traitement 11 un message invitant l'utilisateur 13 à saisir une donnée personnelle d'authentification. La donnée personnelle d'authentification est associée à
30 l'application NFC de retrait bancaire mémorisée dans le terminal mobile 12 et est destinée à débloquer cette application sur le terminal. Dans un premier exemple de réalisation, la donnée personnelle d'authentification demandée est un code « PIN » de service (de l'anglais « Personal Identification Number »). Dans cet exemple, il est affiché également sur la surface sensitive 11-2 du terminal de traitement 11 un clavier numérique (non représenté sur la figure 2).

Dans une étape E6 de saisie et de mémorisation, l'utilisateur 13 saisit sa donnée personnelle d'authentification. Dans le premier exemple décrit ici, il saisit le code PIN associé à l'application NFC de retrait bancaire au moyen du clavier numérique affiché sur la surface sensitive 11-3 du distributeur 11. Le code PIN est en général constitué de quatre chiffres. Chacun des chiffres saisis par l'utilisateur 13 est mémorisé par le terminal de traitement 11. Dans un exemple de réalisation, un caractère du clavier permet de corriger le ou les derniers chiffres saisis.

Une fois les quatre chiffres saisis, ou après saisie d'un caractère spécifique marquant la fin de la saisie, la donnée d'authentification saisie et mémorisée par le terminal de traitement 11 est transmise au terminal mobile 12 au cours d'une étape E7 d'envoi de la donnée d'authentification. La donnée d'authentification saisie est transmise à l'intérieur d'un troisième signal électrique modulé.

Dans une étape E8 de réception de la donnée personnelle d'authentification, le terminal mobile 12 reçoit le signal modulé électrique qui transporte la donnée personnelle d'authentification saisie par l'utilisateur. Le signal est démodulé, ce qui permet au terminal mobile 12 d'obtenir la donnée d'authentification telle qu'elle a été mémorisée par le terminal de traitement 11.

Dans une étape E9 de vérification de l'authentification, la donnée d'authentification reçue au cours de l'étape précédente E8 est comparée à la donnée personnelle d'authentification de référence préalablement mémorisée dans le terminal mobile 12 en association avec le service de retrait bancaire. La donnée d'authentification de référence est stockée de manière sécurisée, dans un container de sécurité de l'élément de sécurité 12-2. La vérification de l'authentification est positive lorsque la donnée saisie est identique à la donnée de référence. Elle est négative dans le cas contraire.

Dans une étape E10 de réponse, le terminal mobile 12 envoie dans un quatrième signal électrique modulé une trame comprenant une donnée de contrôle destinée à indiquer le résultat de l'authentification réalisée par l'élément de sécurité 12-2. Par exemple, la donnée de contrôle correspond au message « ok », lorsque la vérification de l'authentification effectuée au cours de l'étape E9 est positive, et « nok » lorsque la vérification est négative. La donnée de contrôle représente ainsi le résultat de la vérification de la donnée personnelle d'authentification effectuée par le l'élément de sécurité 12-2.

Dans une étape E11 de réception, le terminal de traitement reçoit la donnée de contrôle envoyée par le terminal mobile 12 au cours de l'étape E10.

Dans une étape suivante E12 de vérification, le terminal de traitement 11 vérifie la donnée de contrôle reçue.

Si la vérification est positive (branche ok sur la figure 2), c'est-à-dire si la donnée de contrôle correspond à une authentification positive de l'utilisateur 13, alors dans une étape suivante E13 d'affichage d'un message d'invitation à saisir un montant, il est affiché sur l'écran 11-2 du terminal de traitement 11 un message invitant l'utilisateur 13 à saisir un montant. Il est également affiché sur la surface sensitive 11-3 du terminal de traitement 11 différents montants possibles, ou un clavier numérique adapté pour permettre à l'utilisateur de saisir le montant souhaité.

Dans une étape E14 de saisie d'un montant, l'utilisateur 13 saisit le montant qu'il souhaite retirer de son compte bancaire. Soit il sélectionne un montant proposé sur la surface sensitive 11-3, soit il saisit le montant à partir du clavier affiché sur la surface sensitive 11-3.

Dans une étape E15 de contrôle, il est vérifié que le montant saisi est cohérent avec des données bancaires propres à l'utilisateur. A cette fin un dialogue sécurisé est établi entre l'élément de sécurité 12-2 inséré dans le terminal mobile, plus précisément le container dédié à l'application NFC de retrait bancaire et l'établissement bancaire distant 14. Dans cette étape, l'établissement bancaire 14 vérifie que le compte associé à l'utilisateur 13 est créditeur d'un montant au moins supérieur au montant demandé.

Dans ce cas, dans une étape suivante E16 de distribution, le terminal de traitement 11 distribue à l'utilisateur 13 le montant demandé.

Dans une étape E17 de confirmation, l'établissement bancaire 14 émet un message de confirmation vers le terminal mobile 12 de l'utilisateur. Il s'agit par exemple d'un message « SMS » (de l'anglais « Short Message Service ») de confirmation à destination du terminal mobile 12 de l'utilisateur 13. Ce message de confirmation comprend des informations sur la transaction qui vient d'avoir lieu. Par exemple, le message SMS comprend l'heure du retrait, le nom de la banque associée au distributeur, et le montant du retrait.

Dans une étape suivante E18 de fin de transaction, il est procédé à la terminaison de la transaction. Le terminal de traitement 11 envoie un message de fin de communication au terminal mobile 12, à l'attention de l'utilisateur 13. Il est ensuite affiché sur l'écran 11-2 du terminal de traitement 11 un message informant l'utilisateur que la transaction est terminée et qu'il peut retirer sa main de la surface sensitive 11-2. On comprend que durant les étapes E1 à E17 l'utilisateur 13 maintient sa main sur la surface sensitive 11-3 du terminal de traitement 11 ou la maintient toujours très proche de cette surface de manière à maintenir un contact permanent entre le terminal mobile 12 et le terminal de traitement 11.

Au terme de l'étape E18 de fin de transaction, le terminal de traitement 11 retourne dans l'étape initiale E0 d'attente.

Si la vérification de la donnée de contrôle reçue effectuée au cours de l'étape E12 est négative (branche « nok » sur la figure), c'est-à-dire si l'authentification de l'utilisateur effectuée par le terminal mobile durant l'étape E9 a échoué, le terminal de traitement 11 peut mettre fin prématurément à la transaction en passant directement à l'étape E18 de fin de transaction.

Dans un exemple de réalisation correspondant au cas où la donnée personnelle d'authentification est un code PIN et dans un but de rendre le service encore plus sûr, au cours de l'étape E5 d'invitation à saisir une donnée personnelle d'authentification, les chiffres sont affichés sur le clavier numérique dans un ordre aléatoire. Ainsi, quelqu'un qui observerait l'utilisateur 13 en train de saisir son code aurait du mal à reconstituer la séquence à partir de la position des doigts de l'utilisateur. Dans un autre exemple de réalisation, un filtre de confidentialité est positionné sur la surface sensitive 11-3 sur laquelle est affiché le clavier. Un tel filtre de confidentialité est une protection qui se place devant la surface sensitive 11-3 et qui restreint la vision des données affichées de part et d'autre de l'axe de vision, rendant ainsi impossible l'observation du clavier par un tiers lors de la saisie. Le filtre de confidentialité est destiné à sécuriser la saisie de l'utilisateur 13. Bien sûr dans un autre exemple de réalisation, le filtre est combiné avec un clavier dont les touches sont affichées dans un ordre aléatoire.

Dans un autre exemple de réalisation de l'invention, le terminal de traitement 11 comprend également une plaque métallique, posée au niveau du sol, et sur laquelle l'utilisateur pose les pieds pour effectuer la transaction de retrait. Cette plaque métallique est destinée à maintenir un canal de communication permanent entre le terminal mobile 12 et le terminal de traitement 11 par le biais des pieds de l'utilisateur. Ainsi, la communication entre ces deux entités n'est pas rompue même si l'utilisateur éloigne ponctuellement sa main de la surface sensitive 11-3.

Avec le procédé de l'invention, l'utilisation classique de la carte bancaire est transposée sur le terminal mobile 12. Ainsi, la sécurité inhérente à l'utilisation d'une carte bancaire avec donnée personnelle d'authentification est renforcée d'une part par le fait que l'utilisateur 13 n'a pas à sortir sa carte bancaire de sa poche ou de son sac, et d'autre part par le fait que la saisie de la donnée personnelle d'authentification peut se faire sans que l'utilisateur ne sorte son terminal mobile. Ainsi, le terminal mobile 12 de l'utilisateur n'est pas exposé, ce qui diminue le risque de vol.

La donnée d'authentification saisie ici par l'utilisateur est un code PIN. L'invention n'est bien sûr pas limitée à cet exemple. Ainsi, dans un deuxième exemple de réalisation, la donnée personnelle d'authentification demandée est une empreinte digitale. Dans ce cas, au

cours de l'étape E5 d'invitation, il est affiché sur la surface sensitive 11-2 du terminal de traitement 11 une zone déterminée sur laquelle l'utilisateur est invité à poser son doigt.

Dans un autre exemple de réalisation, la donnée d'authentification saisie est envoyée au cours de l'étape E5 d'envoi de manière sécurisée au terminal mobile 12. Par exemple, la
5 donnée est chiffrée au moyen d'un algorithme de chiffrement préalablement à sa transmission. Les techniques de chiffrement sont supposées connues de l'homme du métier et ne sont pas décrites ici.

De même, dans un autre exemple de réalisation, la donnée de contrôle envoyée au terminal de traitement 11 au cours de l'étape E10 de réponse est transmise de manière sécurisée.
10 Dans ce cas, elle est chiffrée préalablement à son envoi.

Dans l'exemple décrit ici, l'utilisateur 13 pose sa main sur la surface sensitive 11-3. Dans une variante de réalisation, l'utilisateur 13 approche sa main de la surface sensitive 11-3 d'une distance inférieure à une distance déterminée. Cette distance déterminée n'excède pas quelques centimètres. Ainsi, l'interface utilisateur 11-3 détecte qu'une partie du corps, par
15 exemple la main, se situe à une distance inférieure à cette distance déterminée.

Le procédé d'authentification est décrit ici dans le cadre d'un service de retrait bancaire. L'invention n'est bien sûr pas limitée à ce service. Ainsi, le procédé s'applique aussi à tout service qui repose sur une application mémorisée dans l'élément de sécurité 12-2 du terminal mobile 12 et qui nécessite une authentification de l'utilisateur. Ainsi, l'invention s'applique par
20 exemple aussi à des services de paiement au moyen du terminal mobile. L'invention s'applique également à des services liés au domaine de la santé et qui nécessitent une authentification préalable à un accès à des données personnelles de santé. L'invention peut s'appliquer également à des services de contrôle d'accès à des bâtiments, etc.

25 Un terminal de traitement 11 va maintenant être décrit en relation avec la figure 3 dans un mode particulier de réalisation.

Dans l'exemple de réalisation décrit en relation avec la figure 2, le terminal de traitement 11 est un terminal de retrait bancaire. Plus généralement, le terminal de traitement 11 est un équipement informatique, adapté pour émettre et recevoir des informations à travers le
30 corps de l'utilisateur. A cette fin, il comprend :

- une interface radio 11-1, agencée pour émettre et recevoir des signaux électriques modulés transmis à travers le corps de l'utilisateur situé à une distance inférieure à une distance prédéterminée,

- une première interface utilisateur 11-2, agencée pour transmettre des informations à
35 l'utilisateur. Dans un premier exemple de réalisation, la première interface utilisateur est un

écran sur lequel des messages sont affichés à l'attention de l'utilisateur. Dans un autre exemple de réalisation, la première interface 11-2 est un haut-parleur adapté pour diffuser des messages vocaux. La première interface 11-2 constitue des moyens d'invitation agencés pour inviter l'utilisateur à saisir une donnée personnelle d'authentification,

5 - une deuxième interface utilisateur 11-3, agencée pour échanger des informations avec le terminal mobile 12 (non représenté sur le figure 3) à travers le corps de l'utilisateur. Par exemple, la deuxième interface utilisateur 11-3 est une surface sensitive que l'utilisateur peut effleurer ou sur laquelle il peut poser sa main. La deuxième interface 11-3 est couplée à l'interface radio 11-1,

10 - une unité de traitement de signaux 11-4, qui comprend un modulateur agencé pour moduler un premier signal numérique en un premier signal électrique modulé, un démodulateur agencé pour démoduler un deuxième signal électrique modulé reçu en un deuxième signal numérique, et des moyens de commutation pour connecter de façon alternative l'interface radio 11-1 au modulateur suite à la réception du deuxième signal électrique modulé, et l'interface
15 radio au démodulateur suite à l'émission du premier signal modulé,

 - une unité de traitement ou processeur 11-5, ou "CPU" (de l'anglais "Central Processing Unit"), destiné à charger des instructions en mémoire, à les exécuter, à effectuer des opérations ;

 - un ensemble de mémoires, dont une mémoire volatile 11-6, ou "RAM" (pour "Random Access Memory") utilisée pour exécuter des instructions de code, stocker des variables, etc., et
20 une mémoire de stockage 11-7 de type « EEPROM » (de l'anglais « Electrically Erasable Programmable Read Only Memory »). La mémoire de stockage 11-7 est en particulier agencée pour mémoriser la donnée personnelle d'authentification saisie par l'utilisateur,

 - des moyens d'envoi 11-8, agencés pour envoyer la donnée personnelle d'authentification saisie par l'utilisateur au moyen de la deuxième interface utilisateur 11-3 au
25 terminal mobile, à travers le corps de l'utilisateur,

 - des moyens de réception 11-9, agencés pour recevoir du terminal mobile, à travers le corps de l'utilisateur une donnée représentant le résultat d'une vérification de la donnée personnelle d'authentification réalisée par le terminal de l'utilisateur,

 - des moyens de vérification 11-10, agencés pour vérifier ladite donnée reçue.

30 Les interfaces utilisateur 11-2, 11-3, l'unité de traitement 11-4, les moyens d'envoi 11-8, de réception 11-9, et de vérification 11-10 sont de préférence des modules logiciels comprenant des instructions logicielles pour faire exécuter les étapes du procédé d'authentification précédemment décrit.

L'invention concerne donc aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé d'authentification tel que décrit précédemment lorsque ce programme est exécuté par un processeur du terminal de traitement ;

5 - un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur décrit ci-dessus.

Les modules logiciels peuvent être stockés dans, ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un CD-ROM, une disquette magnétique ou un disque dur, ou bien un support de transmission tel qu'un signal ou un réseau de télécommunication.

10 L'invention concerne également un système d'authentification qui comprend un terminal de traitement tel que décrit précédemment et un terminal mobile comprenant une interface radio, adaptée pour émettre et recevoir des signaux radioélectriques à travers le corps de l'utilisateur.

15 Le terminal mobile est également agencé pour recevoir une donnée personnelle d'authentification, pour la vérifier et pour transmettre une donnée représentant le résultat de cette vérification. Dans un mode de réalisation particulier, le terminal mobile comprend un élément de sécurité 12.2 et est agencé pour vérifier la donnée personnelle d'authentification en la comparant avec une donnée personnelle d'authentification de référence, mémorisée dans l'élément de sécurité.

20

REVENDICATIONS

1. Procédé d'authentification entre un terminal mobile (12), situé à une distance inférieure à une première distance prédéterminée du corps d'un utilisateur (13), le terminal mobile comprenant une antenne (12-1) constituant une interface radio adaptée pour émettre et recevoir des signaux radioélectriques, et un terminal de traitement adapté pour émettre et recevoir des signaux radioélectriques, les signaux radioélectriques étant transmis entre le terminal mobile et le terminal de traitement en utilisant une capacité de conductivité du corps de l'utilisateur, le procédé comprenant :
- une étape (E1) de détection qu'une partie du corps de l'utilisateur est située à une distance inférieure à une deuxième distance prédéterminée d'une interface utilisateur (11-3) du terminal de traitement, ladite détection déclenchant un réveil du terminal de traitement et l'établissement d'une communication entre le terminal de traitement et le terminal mobile,
 - une étape (E5) d'invitation de l'utilisateur par le terminal de traitement à saisir une donnée personnelle d'authentification,
 - une étape (E7) d'envoi au terminal mobile d'un signal radioélectrique comprenant ladite donnée personnelle d'authentification,
 - une étape (E11) de réception d'un signal radioélectrique émis par le terminal mobile comprenant une donnée représentant le résultat d'une vérification de la donnée personnelle d'authentification réalisée par le terminal mobile,
 - une étape (E 12) de vérification de ladite donnée reçue, l'authentification étant réussie lorsque la vérification est positive.
2. Procédé d'authentification selon la revendication 1, dans lequel la vérification de la donnée personnelle d'authentification réalisée par le terminal mobile consiste à comparer la donnée saisie avec une donnée de référence, mémorisée dans un élément de sécurité (12-2) du terminal mobile.
3. Procédé d'authentification selon la revendication 1, dans lequel l'antenne du terminal mobile constituant l'interface radio adaptée pour émettre et recevoir des signaux radioélectriques est une antenne NFC.
4. Procédé selon la revendication 1, dans lequel la donnée personnelle d'authentification saisie et la donnée représentant le résultat de la vérification sont transmises de manière sécurisée.

5. Procédé d'authentification selon la revendication 1, dans lequel l'étape d'invitation consiste à afficher sur l'interface utilisateur du terminal de traitement un clavier numérique comprenant des chiffres dans lequel l'ordre d'affichage des chiffres est aléatoire.

5

6. Procédé selon la revendication 5, dans lequel l'interface utilisateur du terminal de traitement est équipée d'un filtre de confidentialité, rendant une observation par un tiers impossible lors de la saisie.

10

7. Utilisation du procédé d'authentification selon la revendication 1 dans un service de retrait bancaire, le procédé comprenant en outre, après une vérification positive :

- une étape d'invitation à saisir un montant,
 - une étape de mémorisation d'un montant déterminé, choisi par l'utilisateur,
 - une phase de dialogue avec un établissement bancaire (14) pour obtenir une
- 15 autorisation de débit,
- si le débit est autorisé, une étape de distribution dudit montant.

20

8. Utilisation du procédé d'authentification selon la revendication précédente, comprenant en outre l'envoi d'un message de confirmation de transaction au terminal mobile.

9. Terminal de traitement (11) comprenant une interface radio (11-1) agencée pour émettre et recevoir des signaux radioélectriques, les signaux radioélectriques étant transmis entre un terminal mobile, situé à une distance inférieure à une première distance prédéterminée du corps d'un utilisateur, et le terminal de traitement en utilisant une capacité de conductivité du

25 corps de l'utilisateur, le terminal de traitement comprenant :

- une unité de traitement (11-5) ;
 - une interface utilisateur (11-3), couplée à l'interface radio, agencée pour détecter qu'une partie du corps d'un utilisateur du terminal mobile est située à une distance inférieure à une deuxième distance prédéterminée, ladite détection déclenchant un réveil du terminal de
- 30 traitement et l'établissement d'une communication entre le terminal de traitement et le terminal mobile,
- des moyens d'invitation (11-2), agencés pour inviter l'utilisateur à saisir une donnée personnelle d'authentification,
 - des moyens d'envoi (11-8), agencés pour envoyer un signal radioélectrique
- 35 comprenant ladite donnée personnelle d'authentification au terminal mobile,

- des moyens de réception (11-9), agencés pour recevoir un signal radioélectrique émis par le terminal mobile comprenant une donnée représentant le résultat d'une vérification de la donnée personnelle d'authentification réalisée par le terminal mobile,

- des moyens de vérification (11-10), agencés pour vérifier ladite donnée reçue.

5

10. Terminal de traitement selon la revendication 9, comprenant en outre une plaque métallique posée au sol, destinée à maintenir la communication entre le terminal de traitement et le terminal mobile, lorsque l'utilisateur pose ses pieds sur ladite plaque.

10

11. Système d'authentification comprenant :

- un terminal de traitement selon la revendication 9, et

- un terminal mobile adapté pour émettre et recevoir des signaux radioélectriques, situé à une distance inférieure à une distance prédéterminée du corps d'un utilisateur, les signaux radioélectriques étant transmis entre le terminal mobile et le terminal de traitement en utilisant une capacité de conductivité du corps de l'utilisateur.

15

12. Programme sur un support de données et chargeable dans une mémoire interne d'un terminal de traitement, le programme comprenant des portions de code pour l'exécution des étapes du procédé d'authentification selon la revendication 1, lorsque le programme est exécuté sur ledit terminal.

20

13. Support de données sur lequel est enregistré le programme d'ordinateur selon la revendication 12.

25

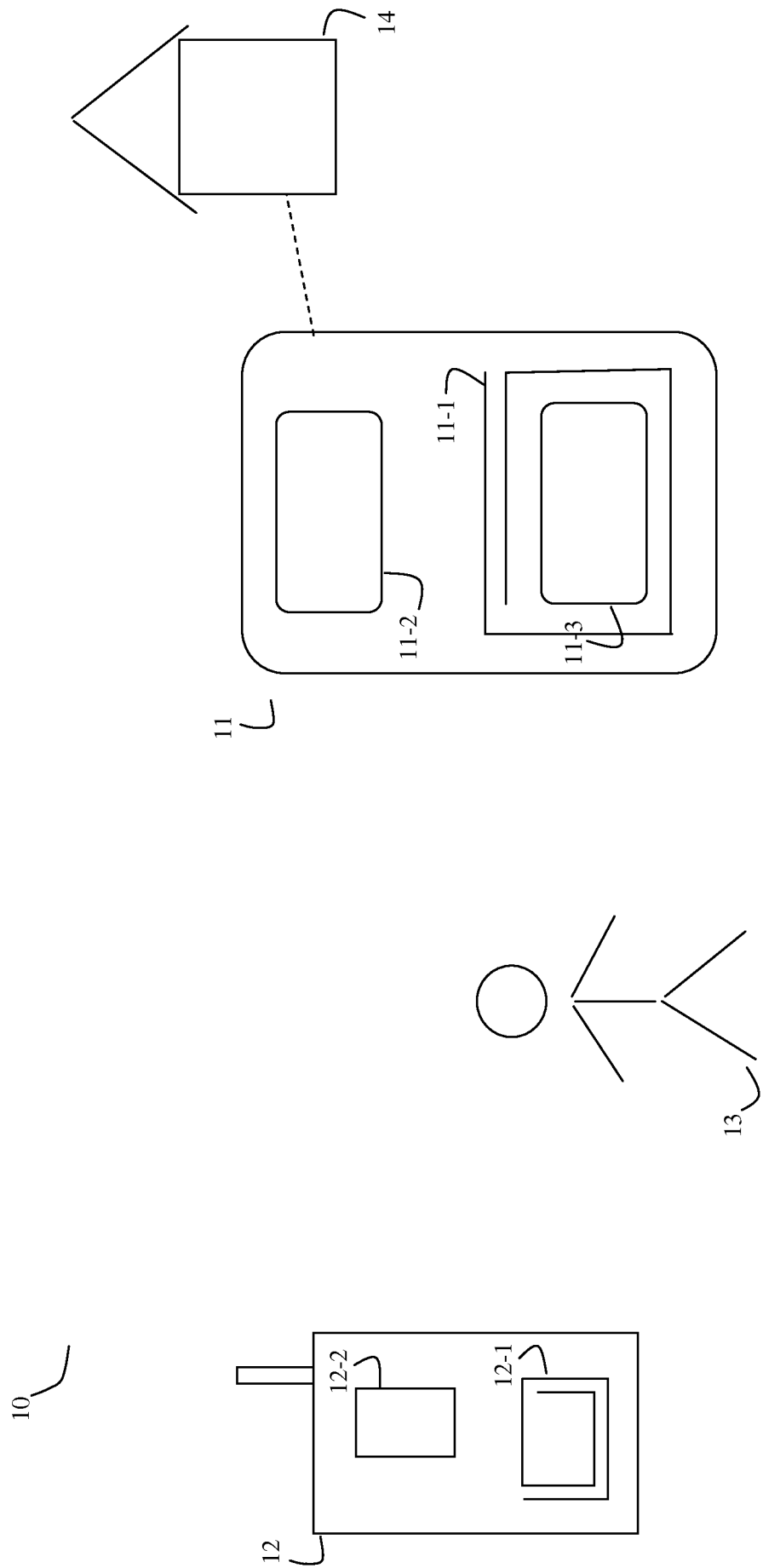


Figure 1

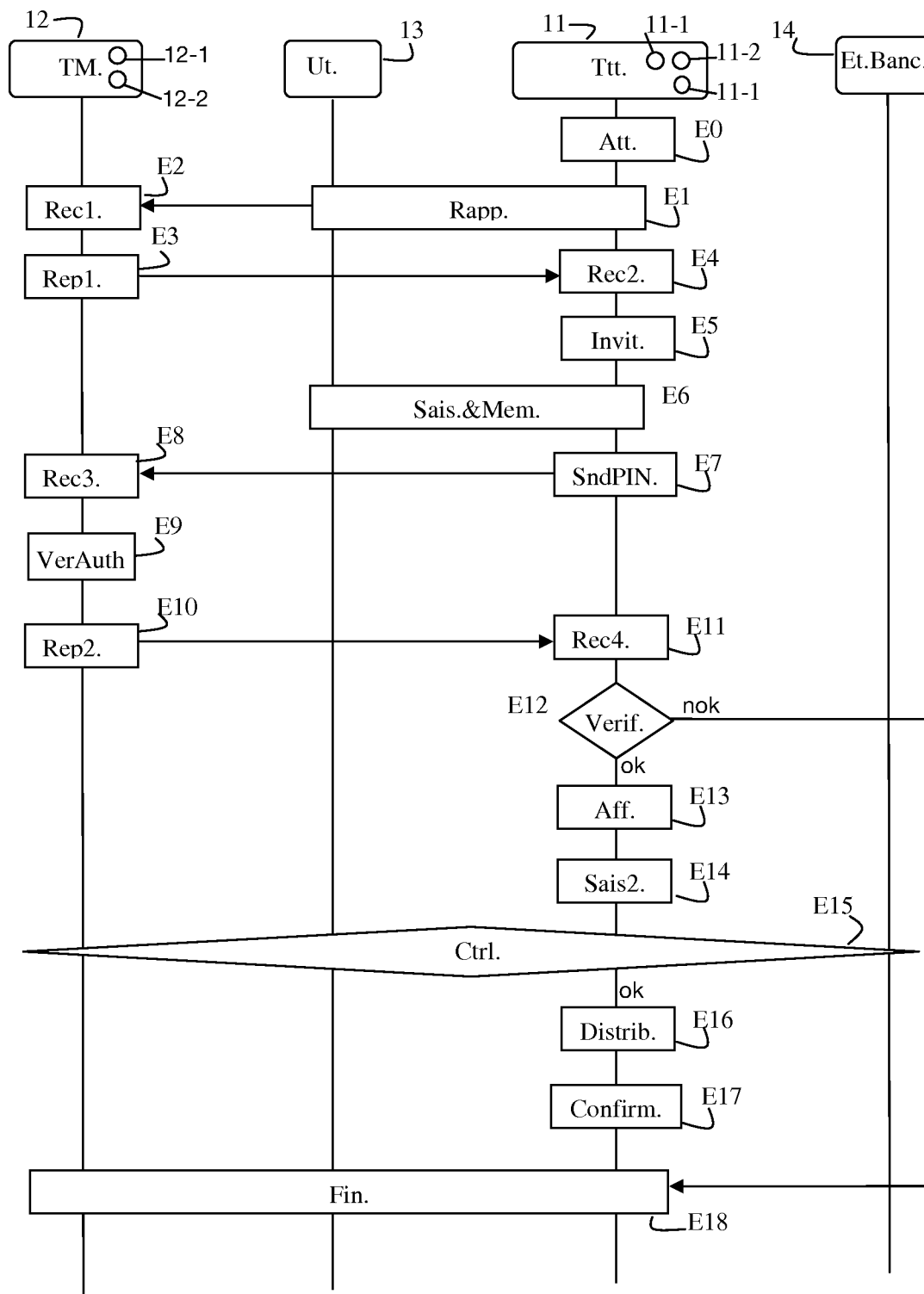


Figure 2

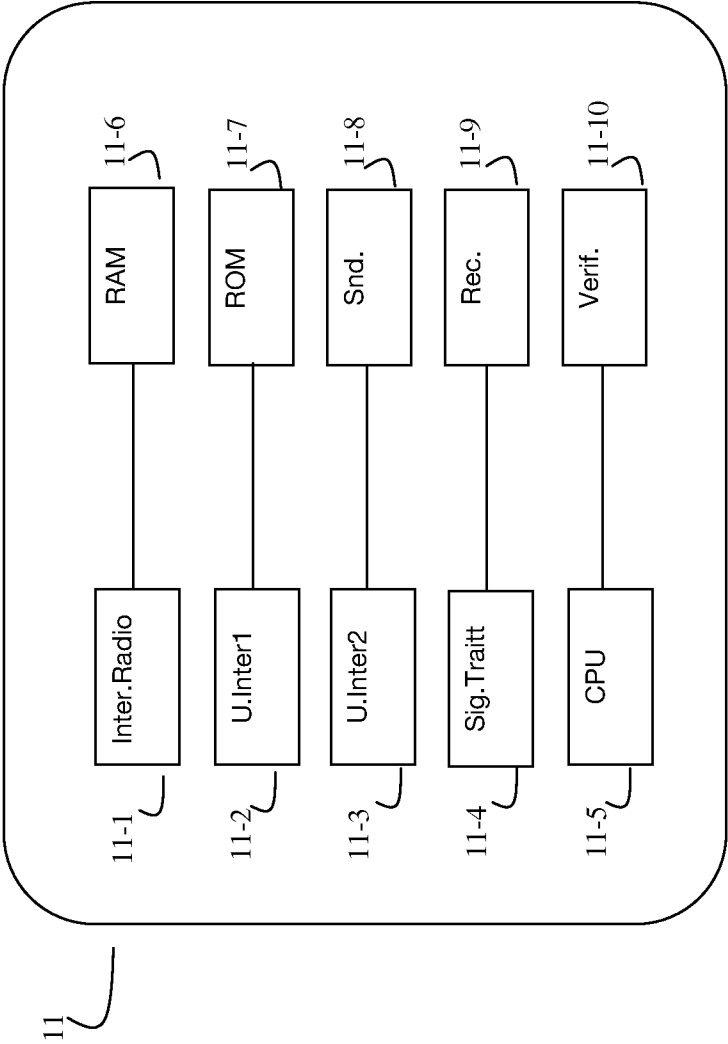


Figure 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2013/051475

A. CLASSIFICATION OF SUBJECT MATTER INV. H04B13/00 G06K19/07 G06Q20/04 G06K7/10 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04B G06K G06Q G07F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 843 425 A2 (IBM [US]) 20 May 1998 (1998-05-20) column 1, line 3 - column 2, line 6 column 7, line 42 - column 7, line 50 column 8, line 28 - column 9, line 15 column 9, line 50 - column 10, line 34 column 11, line 4 - line 9 column 18, line 29 - line 42 figures 1-3, 10, 13 ----- -/--	1-13
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search	Date of mailing of the international search report	
29 August 2013	09/09/2013	
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Glaser, Norbert	

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2013/051475

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 096 722 A2 (SONY CORP [JP]) 2 May 2001 (2001-05-02) paragraph [0059] - paragraph [0061] paragraph [0062] - paragraph [0063] paragraph [0071] paragraph [0072] paragraph [0074] - paragraph [0075] paragraph [0095] paragraph [0098] paragraph [0104] -----	1-13
A	EP 1 598 965 A1 (SONY CORP [JP] TAKICUCHI KIYOAKI [JP]) 23 November 2005 (2005-11-23) paragraph [0044] - paragraph [0048] paragraph [0081] - paragraph [0083]; figure 10 -----	3,10
A	WO 2009/081337 A1 (PHILIPS INTELLECTUAL PROPERTY [DE]; KONINKL PHILIPS ELECTRONICS NV [NL] 2 July 2009 (2009-07-02) page 1, paragraph 3 - paragraph 4; figure 1 page 5, last paragraph - page 7, paragraph 2 page 10, last paragraph - page 11, paragraph 1 page 3; figure 3 -----	3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2013/051475

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0843425	A2	20-05-1998	AT 235125 T 15-04-2003
		CN 1185065 A 17-06-1998	
		DE 69719919 D1 24-04-2003	
		DE 69719919 T2 18-12-2003	
		EP 0843425 A2 20-05-1998	
		ES 2189926 T3 16-07-2003	
		JP H10228524 A 25-08-1998	
		MY 117650 A 31-07-2004	
		US 5796827 A 18-08-1998	
EP 1096722	A2	02-05-2001	EP 1096722 A2 02-05-2001
		JP 2001195368 A 19-07-2001	
		US 7202773 B1 10-04-2007	
EP 1598965	A1	23-11-2005	BR PI0407434 A 24-01-2006
		CN 1754330 A 29-03-2006	
		CN 101667870 A 10-03-2010	
		EP 1598965 A1 23-11-2005	
		KR 20050104404 A 02-11-2005	
		RU 2302699 C2 10-07-2007	
		US 2006077616 A1 13-04-2006	
		WO 2004077704 A1 10-09-2004	
WO 2009081337	A1	02-07-2009	CN 101904117 A 01-12-2010
		EP 2241031 A1 20-10-2010	
		JP 2011509006 A 17-03-2011	
		US 2010311326 A1 09-12-2010	
		WO 2009081337 A1 02-07-2009	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2013/051475

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04B13/00 G06K19/07 G06Q20/04 G06K7/10 ADD.		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) H04B G06K G06Q G07F		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 843 425 A2 (IBM [US]) 20 mai 1998 (1998-05-20) colonne 1, ligne 3 - colonne 2, ligne 6 colonne 7, ligne 42 - colonne 7, ligne 50 colonne 8, ligne 28 - colonne 9, ligne 15 colonne 9, ligne 50 - colonne 10, ligne 34 colonne 11, ligne 4 - ligne 9 colonne 18, ligne 29 - ligne 42 figures 1-3, 10, 13 ----- -/--	1-13
☒ Voir la suite du cadre C pour la fin de la liste des documents ☒ Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités: "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets		
Date à laquelle la recherche internationale a été effectivement achevée 29 août 2013	Date d'expédition du présent rapport de recherche internationale 09/09/2013	
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Glaser, Norbert	

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 096 722 A2 (SONY CORP [JP]) 2 mai 2001 (2001-05-02) alinéa [0059] - alinéa [0061] alinéa [0062] - alinéa [0063] alinéa [0071] alinéa [0072] alinéa [0074] - alinéa [0075] alinéa [0095] alinéa [0098] alinéa [0104] -----	1-13
A	EP 1 598 965 A1 (SONY CORP [JP] TAKICUCHI KIYOAKI [JP]) 23 novembre 2005 (2005-11-23) alinéa [0044] - alinéa [0048] alinéa [0081] - alinéa [0083]; figure 10 -----	3,10
A	WO 2009/081337 A1 (PHILIPS INTELLECTUAL PROPERTY [DE]; KONINKL PHILIPS ELECTRONICS NV [NL]) 2 juillet 2009 (2009-07-02) page 1, alinéa 3 - alinéa 4; figure 1 page 5, dernier alinéa - page 7, alinéa 2 page 10, dernier alinéa - page 11, alinéa 1 page 3; figure 3 -----	3

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2013/051475

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0843425	A2	20-05-1998	AT	235125 T	15-04-2003
			CN	1185065 A	17-06-1998
			DE	69719919 D1	24-04-2003
			DE	69719919 T2	18-12-2003
			EP	0843425 A2	20-05-1998
			ES	2189926 T3	16-07-2003
			JP	H10228524 A	25-08-1998
			MY	117650 A	31-07-2004
			US	5796827 A	18-08-1998

EP 1096722	A2	02-05-2001	EP	1096722 A2	02-05-2001
			JP	2001195368 A	19-07-2001
			US	7202773 B1	10-04-2007

EP 1598965	A1	23-11-2005	BR	PI0407434 A	24-01-2006
			CN	1754330 A	29-03-2006
			CN	101667870 A	10-03-2010
			EP	1598965 A1	23-11-2005
			KR	20050104404 A	02-11-2005
			RU	2302699 C2	10-07-2007
			US	2006077616 A1	13-04-2006
			WO	2004077704 A1	10-09-2004

WO 2009081337	A1	02-07-2009	CN	101904117 A	01-12-2010
			EP	2241031 A1	20-10-2010
			JP	2011509006 A	17-03-2011
			US	2010311326 A1	09-12-2010
			WO	2009081337 A1	02-07-2009
