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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
05 janvier 2023 (05.01.2023)

WIPO | PCT

(10) Numéro de publication internationale
WO 2023/274979 A1

(51) Classification internationale des brevets :
G06Q 20/32 (2012.01) *G06Q 20/38* (2012.01)
G06Q 20/42 (2012.01) *G06Q 20/40* (2012.01)

(21) Numéro de la demande internationale :
PCT/EP2022/067612

(22) Date de dépôt international :
27 juin 2022 (27.06.2022)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2106947 28 juin 2021 (28.06.2021) FR

(71) Déposant : **BANKS AND ACQUIRERS INTERNATIONAL HOLDING** [FR/FR] ; 28/32 boulevard de Grenelle, 75015 Paris (FR).

(72) Inventeurs : **LEGER, Michel** ; 5 rue Lalo, 75116 PARIS (FR). **BEUNARDEAU, Marc** ; 37 avenue de Lowendal, 75015 PARIS (FR). **CONNOLLY, Aisling** ; 34 rue Blomet, 75015 PARIS (FR). **GERAUD, Rémi** ; 135 rue du Mont Cenis, 75018 PARIS (FR). **NACCACHE, David** ; 92 boulevard Suchet, 75016 PARIS (FR). **TRICHINA, Elena** ; 33bis rue Célony, 13100 AIX EN PROVENCE (FR).

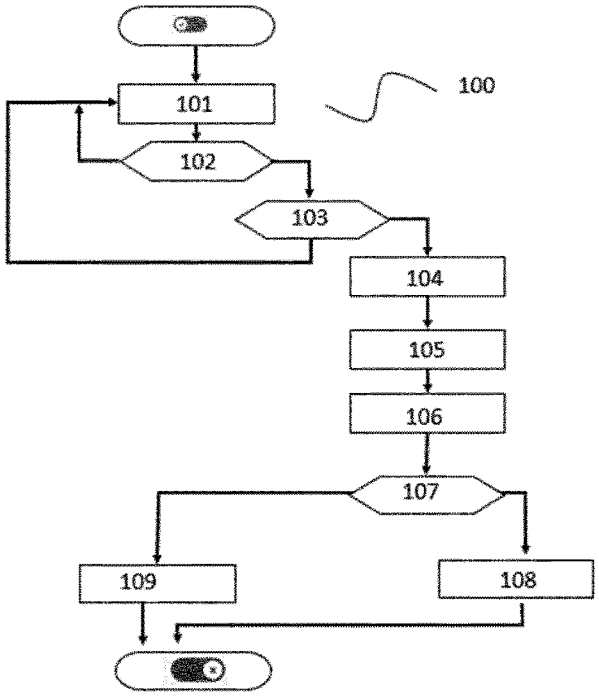
(74) Mandataire : **LLR** ; 11, boulevard de Sébastopol, 75001 PARIS (FR).

(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,

(54) Title: TRANSACTION AUTHENTICATION METHOD USING TWO COMMUNICATION CHANNELS

(54) Titre : PROCÉDÉ D'AUTHENTIFICATION DE TRANSACTION UTILISANT DEUX CANAUX DE COMMUNICATION

[Fig. 4]



(57) **Abstract:** The invention relates to a dual-factor authentication method (100). A terminal is connected to a bank transaction server via first and second communication channels that are logically separate from one another. It implements the following steps: - the server determines a verification code for the transaction and sends a message containing the code to the terminal via the second channel, - the server sends a request asking the terminal to return the code via the first channel to the terminal via the first channel, - the terminal receives the request over the first channel, - the terminal automatically detects (102) receipt of the message over the second channel and automatically identifies (104) the verification code for the transaction in the message, - the terminal returns (108) a response to the request, comprising the identified code, to the server via the first channel.

(57) **Abrégé :** L'invention concerne un procédé (100) d'authentification à deux facteurs. Un terminal est relié à un serveur de transaction bancaire via des premier et deuxième canaux de communication logiquement distincts l'un de l'autre. Il met en œuvre les étapes suivantes: - le serveur détermine un code de vérification de la transaction et envoie, au terminal et via le deuxième canal, un message contenant le code, - le serveur envoie, au terminal et via le premier canal, une requête demandant au terminal de renvoyer le code via le premier canal, - le terminal réceptionne la requête sur le premier canal, - le terminal détecte (102) automatiquement la réception du message sur le deuxième canal et identifie (104) automatiquement le code de vérification de la transaction dans le message, - le terminal renvoie (108), au serveur et via le premier canal, une réponse à la requête comprenant le code identifié.

WO 2023/274979 A1

[Suite sur la page suivante]

CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

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

— *en noir et blanc ; la demande internationale telle que déposée était en couleur ou en échelle de gris et est disponible sur PATENTSCOPE pour téléchargement.*

Description

Titre de l'invention : Procédé d'authentification de transaction utilisant deux canaux de communication

La présente invention se rapporte à un procédé d'authentification de transaction utilisant deux canaux de communication. Plus particulièrement, l'invention se rapporte à l'utilisation d'un deuxième canal de communication pour sécuriser une transaction réalisée à partir d'un premier canal de communication.

Les transactions de paiement électronique faisant l'objet de ce document concernent les opérations de paiement réalisées en ligne. Un paiement en ligne est réalisé lors de la vente ou l'achat de biens ou de services, aussi bien par des entreprises, des ménages, des particuliers, des gouvernements ou d'autres organisations, publiques ou privées, sur des réseaux interconnectés d'ordinateurs, tel que par exemple internet. Les biens et services sont commandés sur ces réseaux, mais le paiement et la livraison finale du bien ou du service peuvent être effectués en ligne ou hors ligne. De plus, les clients des banques effectuent régulièrement des opérations de paiement par virement en utilisant les services bancaires par Internet. De plus en plus de consommateurs utilisent le commerce électronique, pour rechercher et acheter des biens et des services sur des réseaux électroniques tels que, par exemple, Internet. Le paiement s'effectue généralement par la saisie d'un numéro de carte de débit et/ou de crédit, ou carte bancaire, ou à l'aide d'autres informations financières dans les champs respectifs d'un formulaire du site du commerçant en ligne. Les transactions peuvent également être effectuées à l'aide de fournisseurs de services de paiement en ligne ou mobiles, tels que ceux proposés par exemple par la société PayPal, Inc., de San Jose, en Californie. Pour assurer une meilleure sécurité, les systèmes de paiement électronique utilisent souvent des solutions de sécurité agglomérées telles que celle identifiées par les marques « 3Dsecure », « Verified by Visa », ou autre. De tels services de paiement et solutions de sécurité de paiement peuvent rendre les transactions plus faciles et/ou plus sûres pour les parties impliquées. Acheter avec l'aide d'un fournisseur de services de paiement depuis un terminal mobile portable est l'une des principales raisons pour lesquelles les achats en ligne et sur mobile se développent très rapidement.

Les systèmes de paiement en ligne traditionnels exposent les utilisateurs à des risques de sécurité. Par exemple, taper des numéros d'un identifiant de carte de crédit dans un champ d'un formulaire de paiement en ligne expose un utilisateur au vol de ce numéro par une tierce personne qui regarde son écran, par un virus informatique de journalisation de frappe, etc. Bien que le stockage des numéros de carte de crédit par

un détaillant en ligne puisse éviter d'obliger l'utilisateur à saisir manuellement à chaque achat les informations au cours de la transaction de paiement, il expose le détaillant en ligne à ses propres risques et responsabilités en matière de sécurité. Les informations sur les cartes de crédit peuvent également être capturées par des moyens simples, par exemple, en prenant une photo d'une carte exposée par inadvertance, sans oublier que des cartes de crédit peuvent être perdues ou volées, ce qui permet à une personne malintentionnée d'en faire un mauvais usage.

Afin d'améliorer la sécurité des transactions électroniques, les systèmes de paiement électroniques modernes utilisent souvent une procédure dite d'authentification à deux facteurs de sécurité, ci-après désigné 2FA. Les premières procédures 2FA ont utilisé des mots de passe supplémentaires. Sur les terminaux de paiement bancaire, cela s'est traduit par l'utilisation d'un code PIN (de l'anglais « *Personal Identification Number* ») vérifié sur la puce d'une carte bancaire. Pour les transactions bancaires par Internet, l'une des formes les plus anciennes d'authentification à deux facteurs de sécurité, une méthode consiste à émettre aux clients titulaires de carte, avec la carte bancaire, une liste numérotée de nombres d'authentification de transaction, communément nommée TAN (de l'anglais « *Transaction Authentication Numbers* »), afin que, lors d'une transaction, la banque puisse demander à l'utilisateur de saisir manuellement un nombre d'authentification correspondant à un numéro choisi aléatoirement parmi la liste TAN. Le développement des transactions sur internet et la prolifération des téléphones portables a conduit à la généralisation d'une procédure 2FA utilisant le téléphone mobile comme deuxième canal communication pour envoyer un code d'authentification, de type mot de passe à usage unique ou OTP (de l'anglais « *One-Time Password* »), par message court ou SMS (de l'anglais « *Short Message Service* »). En variante, le code d'authentification peut être transmis par courriel.

L'utilisation d'un message court présente cependant un inconvénient lorsque la transaction est réalisée intégralement sur un appareil de téléphonie intelligent de type smartphone ou ordiphone. En effet, l'utilisateur ne peut pas visualiser le message court lors de la saisie du code d'authentification sur le navigateur internet car il ne peut pas visualiser sur son écran simultanément ce message dans sa messagerie et la page web de transaction, il doit passer d'une application à l'autre. L'utilisateur doit donc mémoriser le code d'authentification, ce qui constitue une source d'une erreur de saisie qui peut entrainer l'utilisateur à abandonner la transaction. Pour éviter une erreur de mémorisation, l'utilisateur peut copier la chaine de caractères correspondant au code d'authentification depuis le message court pour ensuite la recopier (ou « coller ») dans le navigateur. Cependant l'utilisation des fonctions « copier-coller » sur un smartphone n'est pas maitrisée par tous les utilisateurs et peut parfois être déroutante.

L'utilisation d'un courriel présente les mêmes inconvénients lorsque le terminal est un téléphone ou une tablette qui ne permet pas de visualiser simultanément l'application de messagerie et de navigation sur internet. De plus, un utilisateur d'ordinateur personnel qui n'est pas familier avec les applications informatiques peut également se trouver en difficulté pour recopier le code à partir de sa messagerie vers un navigateur internet.

La présente invention vise à remédier aux désagréments évoqués précédemment lors de l'utilisation de code d'authentification dans une procédure à deux facteurs de sécurité lorsque la transaction est réalisée sur le terminal qui reçoit le message contenant le code d'authentification.

A cet effet, l'invention a pour objet un procédé d'authentification à deux facteurs d'une transaction bancaire, dans lequel, un terminal d'un utilisateur étant relié à au moins un serveur de transaction bancaire via des premier et deuxième canaux de communication, le deuxième canal étant un service de message court de téléphonie mobile les deux canaux étant logiquement distincts l'un de l'autre, le terminal comprenant en son sein une application mobile, on met en œuvre les étapes suivantes :

au préalable :

- l'application mobile demande au système d'exploitation du terminal à être alertée en cas de message reçu par le service de message court,
- l'application mobile demande au système d'exploitation du terminal la possibilité de lire les messages reçus par le service de message court,

ensuite :

- le serveur détermine un code de vérification de la transaction,
- le serveur envoie, à l'application mobile et via le deuxième canal, un message contenant le code de vérification,
- le serveur envoie, au terminal et via le premier canal, une requête demandant au terminal de renvoyer le code de vérification via le premier canal,
- le terminal réceptionne la requête sur le premier canal,
- l'application mobile détecte automatiquement la réception du message sur le deuxième canal,
- l'application mobile identifie automatiquement le code de vérification de la transaction dans le message, et pour identifier automatiquement le code de vérification dans le message, l'application mobile identifie d'abord automatiquement dans le message une chaine de caractère prédéterminée, distincte du code de vérification, attestant que le message comprend un code de vérification,
- le terminal renvoie, au serveur et via le premier canal, une réponse à la requête comprenant le code identifié.

Ainsi, en détectant automatiquement le code de vérification sur le deuxième canal et en le renvoyant via le premier canal, le terminal évite à l'utilisateur de devoir passer du premier canal au deuxième, par exemple de son navigateur web à son service de messagerie, et de devoir mémoriser ou copier-coller manuellement le code depuis son deuxième canal jusqu'au premier. L'authentification à deux facteurs est donc réalisée de manière aussi sûre que dans l'état de la technique, via les deux canaux, mais sans nécessiter de manipulation contraignante de la part de l'utilisateur. Les risques d'erreur et les probabilités d'abandon de la transaction sont donc diminués.

De plus, le message comprend un « flag », c'est-à-dire une chaine de caractères indiquant que le message comprend un code de vérification. Ce flag peut être propre à un protocole de transaction particulier (par exemple « 3D Secure »). Sa connaissance prédéterminée peut également permettre de connaître le format du code à identifier et sa position dans le message.

En outre, en particulier lors de l'installation de l'application mobile, celle-ci demande les accès nécessaires à son fonctionnement au système d'exploitation du terminal. Ces accès peuvent être acceptés automatiquement ou sur simple validation de l'utilisateur.

Par ailleurs, vis-à-vis des solutions de l'état de la technique, le seul changement concerne les étapes suivies par le terminal. Il n'est en particulier pas nécessaire de modifier la programmation ou les composants du serveur bancaire. Il n'est pas nécessaire non plus de modifier les composants matériels du terminal, tout terminal mobile de type smartphone ou ordiphone, disposant de deux canaux de communication logiquement distincts, pouvant implémenter ce procédé. Un ordinateur personnel comprenant deux canaux de communication logiquement distincts, par exemple la présence d'un navigateur Internet d'un côté et d'une messagerie de courriels de l'autre, est également un terminal apte à exécuter le procédé sans qu'il soit nécessaire de le modifier. L'invention est donc facilement mise en place au sein d'une architecture existante.

Avantageusement, le premier canal est un navigateur internet, et le deuxième canal est un service de message court de téléphonie mobile ou une messagerie de courriel.

Ainsi, tandis que la requête demandant le code est fournie sur une page web, par exemple dans un champ destiné à recevoir le code, le code de vérification est fourni par sms ou par e-mail. Son identification et copie automatique évite à l'utilisateur d'avoir à passer de son navigateur Internet à sa messagerie de téléphonie mobile ou de courriel et à retenir le code qui y a été envoyé pour le recopier dans le navigateur.

De préférence, après avoir identifié automatiquement le code de vérification dans le message et avant de renvoyer la réponse au serveur, le terminal copie automatiquement

le code, depuis le message reçu sur le premier canal, vers la réponse à la requête sur le deuxième canal.

Ainsi, c'est le terminal qui, sans intervention de l'utilisateur, reproduit le code dans la réponse à envoyer au serveur, par exemple dans un champ prévu à cet effet dans la page web de la requête.

Alternativement, après avoir identifié le code de vérification dans le message et avant de renvoyer la réponse au serveur :

- le terminal copie automatiquement le code, depuis le message reçu sur le premier canal, vers une mémoire tampon,
- l'utilisateur copie le code, depuis la mémoire tampon, vers la réponse à la requête sur le deuxième canal.

Ainsi, dans ce cas, le terminal copie automatiquement le code vers la mémoire, mais c'est l'utilisateur qui réalise l'opération de « collage », c'est-à-dire la manipulation consistant à copier depuis la mémoire tampon le code vers la réponse à la requête.

De préférence, la requête comportant un champ à remplir avec le code de vérification, la réponse à la requête comporte la requête avec le champ rempli.

Ainsi, la requête apparaît par exemple sur une page web succédant à la demande de transaction. Une fois le champ rempli avec le code et cette réponse validée, le serveur bancaire reçoit le code fourni dans le champ, via le premier canal qui est un navigateur Internet dans cet exemple, et le compare avec le code envoyé via le deuxième canal.

On prévoit également selon l'invention un procédé d'authentification à deux facteurs d'une transaction bancaire par un terminal mobile, dans lequel le terminal comprend en sein une application mobile mettant en œuvre les étapes suivantes :

au préalable :

- l'application mobile demande au système d'exploitation du terminal à être alertée en cas de message reçu par le service de message court,
- l'application mobile demande au système d'exploitation du terminal la possibilité de lire les messages reçus par le service de message court,

ensuite :

- réception d'une requête, sur un premier canal de communication du terminal, demandant le renvoi d'un code de vérification de la transaction,
- détection automatique de la réception d'un message, sur un deuxième canal de communication du terminal logiquement distinct du premier, le deuxième canal étant un service de message court de téléphonie mobile,
- identification automatique d'un code de vérification de la transaction dans le message, dans laquelle, pour identifier automatiquement le code de vérification dans le message, l'application mobile identifie d'abord automatiquement dans le message une chaine de

caractère prédéterminée, distincte du code de vérification, attestant que le message comprend un code de vérification,

- envoi, via le deuxième canal, d'une réponse à la requête comprenant le code identifié.

Ainsi, c'est l'application mobile installée sur le terminal qui met en œuvre les étapes de l'invention. Il n'est donc pas nécessaire de modifier le système d'exploitation du terminal ou d'autres éléments, il suffit d'installer et d'activer l'application, qui peut être implémentée avec tout type de terminal pourvu qu'il ait la capacité à communiquer sur deux canaux de communication logiquement distincts.

Avantageusement :

- l'application demande également au préalable au système d'exploitation du terminal la possibilité de supprimer les messages reçus par le service de message court,

- si un utilisateur du terminal invalide la transaction via le premier canal, l'application supprime le message, reçu par le service de message court, comprenant le code de vérification de la transaction.

Ainsi, si l'utilisateur annule la transaction, alors l'application supprime automatiquement le sms contenant le code de vérification, qui est donc retiré de la mémoire du terminal, ce code étant devenu inutile.

On prévoit également selon l'invention un programme d'ordinateur pour terminal mobile comprenant des instructions qui, lorsque le programme est exécuté par un terminal mobile, conduisent celui-ci à mettre en œuvre les étapes du procédé tel que décrit ci-avant. Ce programme correspond en particulier à l'application mobile elle-même.

Brève description des figures

L'invention sera mieux comprise et d'autres caractéristiques et avantages de celle-ci apparaîtront à la lecture de la description suivante de modes de réalisation particuliers de l'invention, donnés à titre d'exemples illustratifs et non limitatifs, et faisant référence aux dessins annexés, parmi lesquels :

[Fig. 1] montre un système de transaction commerciale à deux facteurs d'authentification selon l'état de la technique,

[Fig. 2] montre un système de transaction commerciale à deux facteurs d'authentification selon l'invention,

[Fig. 3] illustre un téléphone portable mettant en œuvre l'invention,

[Fig. 4] montre un logigramme de fonctionnement du procédé de l'invention.

Description détaillée

Les figures 1 et 2 montrent deux systèmes de transaction réalisée au travers d'un réseau ouvert, tel que par exemple internet, en utilisant une authentification à deux facteurs d'authentification. Sur ces deux figures, les mêmes références correspondent

aux mêmes éléments ou à des éléments similaires. Ces deux figures correspondent à des schémas de transaction à deux facteurs de sécurité tel qu'utilisés dans l'état de la technique et selon l'invention.

Par « réseau ouvert », il faut comprendre un réseau de communication permettant des interconnexions entre une ou plusieurs machines informatiques accessible à tout personne souhaitant le faire. Ce type de réseau peut être internet mais pourrait correspondre à d'autres types de réseaux dès lors que la connexion reste ouverte à tout le monde. Les réseaux ouverts ont l'avantage de faciliter une mise en relation des personnes permettant ainsi d'augmenter les possibilités de transactions commerciales entre personnes connectées audit réseau. Un inconvénient des réseaux ouverts est le risque d'interaction avec des machines appartenant à des personnes malveillantes.

La figure 1 correspond à un système de transaction bancaire permettant à un utilisateur de réaliser des opérations de transaction auprès de sa banque, tel que par exemple pour réaliser un virement bancaire ou pour réaliser un achat de titres en ligne ou tout autre type d'opération pour laquelle l'utilisateur réalise un transfert d'argent depuis son compte bancaire. Sur cette figure 1, l'utilisateur 1 interagit avec un premier terminal 2 connecté à un réseau ouvert 3, tel que par exemple internet, afin de communiquer avec un serveur de services bancaires 4 pour réaliser une opération correspondant à une transaction bancaire c'est-à-dire un transfert d'argent depuis un compte bancaire.

Le premier terminal 2 est par exemple un ordinateur personnel fixe ou portable, une tablette ou un smartphone disposant d'une unité de traitement, d'au moins une mémoire volatile et/ou non volatile, d'une interface de communication lui permettant de se connecter au réseau ouvert 3, d'une interface homme-machine permettant de visualiser et de rentrer des informations, tel que par exemple un écran de visualisation, un écran tactile, un clavier, une souris ou autre. Parmi les programmes stockés dans sa mémoire, le premier terminal dispose d'un programme de navigation sur le réseau ouvert 3, lui permettant de se connecter sur et d'interagir avec des sites web, notamment pour consulter des pages web ou pour remplir et envoyer des formulaires correspondant à des requêtes de transaction. De manière alternative, le premier terminal 2 peut disposer d'un programme spécifique lui permettant de se connecter au travers du réseau ouvert 3 au serveur de services bancaires 4.

Le serveur de services bancaires 4, qu'on appellera dans la suite également indifféremment « serveur bancaire » ou « serveur de transaction bancaire », est par exemple un ordinateur disposant d'une ou plusieurs unités de traitement, d'au moins une mémoire volatile et de masse, et d'au moins une interface de communication lui permettant de se connecter au réseau ouvert 3. La mémoire de masse mémorise entre

autres une base de données contenant toutes les informations relatives aux comptes bancaires des clients de la banque à laquelle il appartient. Le serveur de services bancaires 4 comporte des programmes stockés en mémoire lui permettant de mettre à disposition de terminaux connectés, au travers du réseau ouvert 3, des pages web consultables qui permettent d'interagir avec des utilisateurs via des formulaires contenus dans lesdites pages web. Les formulaires, une fois remplis et renvoyés par l'utilisateur, sont ensuite traités par l'unité de traitement pour validation.

Lorsqu'une transaction est souhaitée par un utilisateur 1, celui-ci utilise le premier terminal 2 pour se connecter au serveur de services bancaires 4. Une page web est alors transmise au premier terminal 2 par le serveur de services bancaires 4. La page web peut comporter des informations à visualiser sur le premier terminal 2, ainsi que des commandes à exécuter en fonction de choix fait par l'utilisateur par l'intermédiaire de l'interface homme-machine. Parmi les choix offerts à l'utilisateur 1, une transaction, par exemple un virement bancaire, peut être réalisée. En choisissant de réaliser un virement, un formulaire de transaction est présenté à l'utilisateur 1, le formulaire pouvant être inclus dans la page web ou transmis par le serveur de services bancaires 4 après réception d'un message indiquant le choix de l'utilisateur 1 provenant du premier terminal 2. L'utilisateur 1 remplit alors le formulaire avec les informations nécessaires à la transaction qui peuvent comprendre l'identification du compte bancaire à créditer, l'identification du compte bancaire à débiter, le montant de la transaction. De nombreuses autres informations peuvent également être requises, telles que des identifiants redondants de l'utilisateur et/ou du compte bancaire ou de son titulaire, un secret connu uniquement de la banque et du titulaire, un identifiant de transaction ou toute autre information qui soit en relation avec la transaction. Une fois le formulaire rempli, l'utilisateur 1 envoie le formulaire rempli au serveur de services bancaires 4 via le premier terminal 2. Le formulaire peut être accompagné de l'heure et de la date d'envoi et également d'identifiants propres au premier terminal 2.

Ayant reçu le formulaire de transaction rempli, le serveur de services bancaires 4 vérifie les informations contenues dans le formulaire et notamment si la transaction demandée peut être autorisée ou non. A cet effet, le serveur de services bancaires 4 interroge sa base de données pour vérifier si le compte à débiter est toujours en service et si le crédit du compte à débiter peut permettre d'autoriser la transaction. Eventuellement, le serveur peut vérifier la justesse d'identifiants redondants ou d'informations sur le titulaire du compte bancaire. Cette première vérification correspond à un premier facteur de sécurité. Cependant, la transaction a été transmise par le réseau ouvert 3 et, malgré cette première vérification, il est possible que cette transaction

provienne d'un détournement du formulaire et/ou des informations relatives au compte bancaire par un tiers malveillant.

En effet, les communications sur le réseau ouvert 3 peuvent être interceptées et rejouées éventuellement de manière modifiée. Afin de garantir un minimum de sécurité, il est connu d'encrypter les messages sensibles entre deux machines, tel que par exemple le terminal 2 et le serveur de services bancaires 4, à l'aide de clefs de sessions ou de clefs spécifiques. Cependant, tout message encrypté peut être décrypté au bout d'un certain temps, ce qui permet de récupérer un formulaire échangé et de réutiliser les informations qu'il contient. De plus, le fait que le réseau soit ouvert permet à des personnes malintentionnées de diffuser des virus sur les machines qui y sont connectées et notamment le premier terminal 2. Parmi les virus, certains peuvent intercepter les informations échangées sur l'interfaces homme-machine et les renvoyer vers une autre machine rendant également inopérante la confidentialité de messages encryptés.

Afin de rajouter un niveau de sécurité, un deuxième facteur de sécurité peut être rajouté en utilisant un deuxième canal de communication pour envoyer un code à usage unique. A cet effet, le serveur de services bancaires 4 dispose d'une deuxième interface de communication apte à communiquer via le deuxième canal de communication avec un deuxième terminal 5 qui appartient à un titulaire de compte bancaire. Le deuxième terminal 5 est identifié dans la base de données du serveur de services bancaires 4 en relation avec le compte bancaire à débiter. Le deuxième terminal 5 peut être, classiquement, un téléphone mobile du titulaire du compte bancaire, mais peut également être tout autre type de dispositif connecté à un réseau de communication, tel que, par exemple, un boitier connecté à un réseau de téléphonie mobile fourni par la banque ou encore une tablette ou un ordinateur relié à internet. L'important est que le deuxième canal de communication soit au moins logiquement distinct du premier canal de communication utilisé pour l'envoi du formulaire de transaction.

Après avoir fait la première vérification, le serveur de services bancaires 4 récupère, dans sa base de données, l'identifiant du deuxième terminal 5 pour lui envoyer un code de vérification à usage unique. L'identifiant du deuxième terminal 5 est, par exemple, un numéro de téléphone mobile et le message est, par exemple, envoyé par un message court de type SMS (de l'anglais Short Message Service). Le message peut également indiquer le montant de la transaction et/ou le bénéficiaire de la transaction, de sorte que le titulaire du compte puisse vérifier que la transaction en cours est conforme à une transaction désirée. Il est à noter que le service de messagerie court (messagerie SMS) est géré par le système d'exploitation de l'ordiphone 5.

En parallèle, le serveur de services bancaires 4 envoie au premier terminal 2 une requête de confirmation demandant le code à usage unique. L'utilisateur 1, s'il

correspond au titulaire du compte bancaire, peut alors lire le code à usage unique sur le deuxième terminal 5 et le recopier dans un formulaire de réponse joint à la requête de confirmation afin de le renvoyer au serveur de services bancaires 4.

A réception du formulaire de réponse, le serveur de services bancaires 4 compare le code présent dans le formulaire avec le code à usage unique envoyé au deuxième terminal 5. Si les deux codes sont identiques, alors le serveur de services bancaires 4 valide la transaction et envoie un message au premier terminal 2 pour l'informer de l'acceptation de la transaction. Si les deux codes sont différents, alors la transaction est refusée et le serveur de services bancaires 4 envoie un message au premier terminal indiquant que la transaction est refusée. De manière optionnelle, le serveur de services bancaires 4 peut réitérer l'envoi d'un nouveau code de vérification à usage unique au deuxième terminal 5 et d'une requête au premier terminal 2. Cette authentification à deux facteurs, dont le deuxième facteur est le code fourni à l'utilisateur par un deuxième canal et devant être renvoyé au serveur par le premier, permet d'améliorer la sécurité des transactions. L'inconvénient est que l'utilisateur doit disposer à la fois de son terminal 2 et de son ordiphone 5 pour valider la transaction. Il doit recopier, via l'interface du terminal 2, un code lu sur l'ordiphone 5, ce qui peut être source d'erreur. Ces contraintes peuvent pousser l'utilisateur à abandonner la transaction.

La figure 2 illustre des éléments d'une transaction selon l'invention qui sont similaires. Au lieu d'utiliser le terminal 2 et un l'ordiphone 5 de la figure 1, l'utilisateur réalise l'intégralité de la transaction sur un seul et même ordiphone 8, qui regroupe les étapes réalisées sur les terminaux 2 et 5 de la figure 1.

Le terminal 8, un smartphone, présente des composants classiques de tout ordiphone, comme illustré à la figure 3. Ainsi, il présente un microprocesseur 81 contrôlant un bus central 87 pour échanger des données avec une mémoire 84, de type EEPROM (de l'anglais « *Electrically-Erasable Programmable Read-Only Memory* ») flash, ou encore de type ROM (de l'anglais « *Read-Only Memory* ») ainsi qu'avec une mémoire 83 volatile de type RAM (de l'anglais « *Random Access Memory* »). Il communique également avec l'interface utilisateur 82 du terminal 8, comprenant en particulier un écran tactile, et éventuellement un ou plusieurs boutons, voire un clavier. Le terminal comprend également une carte SIM 86 et une antenne radioélectrique 85 pour communiquer sans contact avec l'extérieur, en particulier par Internet, par e-mail ou par sms. Un système d'exploitation, c'est-à-dire un programme d'ordinateur, est mis en œuvre par le microprocesseur 81 pour gérer l'ensemble des composants du terminal 8. En particulier, ce système d'exploitation peut autoriser l'accès en lecture ou en écriture de certaines zones de la mémoire à des commandes provenant d'applications mobiles installées sur le smartphone 8. Bien sûr, de nombreuses variantes d'architecture de

téléphone intelligent sont connues et l'homme du métier peut à loisir utiliser une architecture différente ou similaire de celle décrite sur la figure 3. Néanmoins, l'homme du métier prendra soin de n'utiliser que des architectures comprenant la possibilité de communiquer par au moins deux canaux de communications logiquement distincts.

Ainsi, cet ordiphone 8 est relié par deux canaux de communication logiquement distincts au serveur de services bancaires 4. Le premier canal est le navigateur Internet, qui permet à l'utilisateur de l'ordiphone 8 de requérir puis valider la transaction de la même manière que sur le terminal 2 de la figure 1. En d'autres termes, là où l'utilisateur 1 de la figure 1 réalisait la transaction sur un ordinateur 2, l'utilisateur 1 de la figure 2 la réalise sur son ordiphone 8, mais toujours par Internet. Le deuxième canal est, comme pour l'ordiphone 5 de la figure 1, le service de message court de type SMS géré par le système d'exploitation de cet ordiphone 8. Ce pourrait être alternativement une messagerie de courriels. Le serveur de services bancaires 4 lui réalise toujours les mêmes opérations : lorsque l'utilisateur commande une transaction et après la vérification d'un premier facteur d'authentification, le serveur 4 envoie au terminal 8 et par le premier canal, c'est-à-dire ici par Internet, une requête demandant de renvoyer un code de vérification. Il s'agit d'afficher à l'écran, via le navigateur web de l'ordiphone 8, la requête avec un champ à remplir destiné à ce code. Parallèlement, le serveur 4 produit un code de vérification à usage unique qu'il envoie à l'ordiphone 8 via le deuxième canal, c'est-à-dire ici par SMS. L'utilisateur 1 se voit donc présenter sur le smartphone 8, d'une part une page web où il lui est demandé de fournir un code de vérification pour valider la transaction qu'il a initié, et d'autre part, un sms sur sa messagerie SMS comprenant le code.

A ce stade, dans une transaction selon l'état de l'art, l'utilisateur, manipulant l'ordiphone 8, aurait alors à quitter son navigateur internet pour ouvrir son application de messagerie, à lire le code de vérification du sms reçu et à revenir au navigateur pour remplir, de mémoire, le champ destiné au code de vérification dans la page web où la requête correspondante apparaît. Alternativement, il pourrait tenter d'utiliser la fonction copier/coller de l'ordiphone à cet effet. Dans les deux cas, le processus est contraignant, source d'erreurs et peut conduire l'utilisateur à abandonner la transaction.

C'est pourquoi, à la différence de l'ordiphone 5 de la figure 1, l'ordiphone 8 comprend en son sein une application mobile 6 spécifique, illustrée schématiquement à la figure 2, enregistrée dans la mémoire 83 du terminal et installée via le système d'exploitation du terminal 8. Une fois activée, et sollicitée pour authentifier une transaction, cette application mobile 6 conduit le terminal 8 à mettre en œuvre les étapes du logigramme de la figure 4. Cette application mobile 6 se présente sous la forme d'un programme d'ordinateur prévu spécifiquement pour un terminal mobile. Elle peut être téléchargée et

installée sur tout terminal mobile de type ordiphone ou téléphone intelligent. Dans la suite, on décrira, au moyen de la figure 4, les étapes mises en œuvre par le terminal 8 grâce à cette application 6.

Rappelons que le contexte est le suivant : l'utilisateur 1 commande une transaction sur Internet via son terminal 8. Le premier facteur d'authentification est vérifié. Le deuxième est la production, par le serveur de services bancaires 4, du code de vérification, envoyé par sms au terminal 8. On considère que l'application 6 est activée. Alors, dans une première étape 101, l'application 6 est à l'écoute du service de messagerie géré par le système d'exploitation du terminal 8. Si et lorsqu'un sms est reçu sur le service de messagerie, une alerte est émise à l'étape 102 (un signal de type « INTERRUPT ») de manière à permettre à l'application 6 de lire le sms reçu, à l'étape 103. A cette étape, il est déterminé si le sms comprend une chaine de caractère prédéterminée attestant que le sms concerne une transaction bancaire. Si ce n'est pas le cas, rien n'est effectué et le procédé renvoie à l'étape 101, en attente du prochain sms. La chaîne de caractère, appelée « Flag », peut par exemple faire référence au service bancaire associé à la transaction, ou à un protocole d'authentification prédéterminé, par exemple avec la chaîne « 3D Secure » qui correspond au protocole du même nom décrit en 2017 (« *3DSecure2.0 Specification by EMVCo* »). Tout type de flag peut être reconnu par l'application mobile, à partir du moment où son identification a été prévue dans l'application mobile, avant son installation ou au cours d'une mise à jour. Si cette chaîne est identifiée, l'application mobile 6 identifie le code de vérification automatiquement à l'étape 104. En particulier, le format de ce type de sms étant connu, il est aisé d'identifier un code par exemple en calculant la position de son premier caractère vis-à-vis du Flag, position qui peut être toujours la même. Ce code est alors « copié », à l'étape 105, dans une mémoire tampon, par exemple la mémoire RAM 83 du terminal 8. L'application mobile 6 prévoit alors à l'étape 106 de « coller » le code, c'est-à-dire de reproduire ce code à partir de la mémoire tampon, pour le placer automatiquement dans le champ de la requête sur le navigateur web, réalisant ainsi une opération de copier-coller. En résumé, ces étapes 101 à 106 conduisent à produire automatiquement la réponse à la requête du service bancaire en détectant, identifiant et reproduisant automatiquement le code fourni par sms dans la page web de la transaction et particulièrement dans le champ correspondant. A l'étape 107, il est demandé à l'utilisateur de valider la fourniture du code. Il lui suffit d'appuyer sur le bouton correspondant à la validation. A l'inverse, il peut également annuler la transaction. En cas de validation et de manière classique, non propre à l'invention, le serveur de services bancaires 4 vérifiera à l'étape 108 la conformité du code reçu avec le code prévu, pour valider ou non la transaction.

Il est à noter que durant toutes les étapes 101 à 106, l'utilisateur n'a pas eu à manipuler l'ordiphone 8. Ainsi, la surveillance des sms, l'identification d'un sms pertinent, l'identification du code de vérification dans le sms, et sa copie dans le champ de la page web, ont été réalisées automatiquement par l'application mobile 6, l'utilisateur n'ayant qu'à valider la fourniture de ce code. A l'inverse, comme on l'a dit, il peut aussi l'annuler à l'étape 107. Dans ce cas, à l'étape 109, ou même si l'utilisateur annule la transaction plus tôt mais après avoir reçu le code de vérification par sms, l'application mobile 6 supprime automatiquement de la messagerie du terminal 8 le sms contenant le code. Ainsi, le code n'est plus stocké dans la mémoire du terminal.

Alternativement, on peut tout à fait prévoir de renvoyer le code sans même demander la validation à l'utilisateur. Dans ce cas, l'utilisateur ne réalise plus aucune action à partir du moment où il a commandé la transaction avant l'étape 101, tout le processus correspondant au second facteur étant réalisé automatiquement sans intervention de sa part.

Alternativement, on peut prévoir que le code est copié non pas directement dans le champ de la requête web, mais dans un champ distinct, par exemple au sein d'une fenêtre spécifique apparaissant à l'instant approprié (une « pop-up »). Cette « pop –up » affiche à l'utilisateur le code copié depuis la mémoire tampon (et donc avant cela depuis la messagerie), et un bouton permettant à l'utilisateur de valider ou non l'envoi de ce code. S'il valide, alors l'application 6 copie le code dans le champ approprié de la requête, et elle ajoute au code les caractères '\n', ce qui est interprété par le navigateur comme l'emploi de la touche « entrée » ou une validation. Ainsi, il n'est pas redemandé à l'utilisateur de valider ce code puisqu'il l'a déjà fait lorsqu'il a été affiché dans la « pop-up ».

Alternativement encore, on peut prévoir que le code est copié depuis la messagerie dans la mémoire tampon, mais qu'au lieu de le coller dans le champ de la page web ou dans une « pop-up » automatiquement, c'est à l'utilisateur de réaliser manuellement cette fonction de « collage » dans le champ de la page web.

Pour que l'application mobile 6 puisse réaliser les étapes décrites ci-avant, il est nécessaire qu'elle dispose des accès appropriés. C'est pourquoi, dans des étapes préalables non illustrées, lors de l'installation de l'application mobile 6 sur le terminal 8, celle-ci demande au système d'exploitation du terminal 8 l'accès à la lecture des sms (accès de type « READ ») du service de messagerie. Elle demande également la possibilité d'être alertée en cas de réception d'un sms, et enfin la possibilité de supprimer un sms. C'est une fois que ces accès ont été acceptés, par l'utilisateur ou automatiquement en fonction de la manière dont le terminal 8 est configuré, que l'activation peut fonctionner comme décrit plus haut.

Cette invention permet donc de copier-coller le code de vérification reçu par un deuxième canal, en l'espèce par sms, afin de l'envoyer via un premier canal, en l'espèce par Internet, en réponse à une requêtant demandant ce code pour valider l'authentification à deux facteurs. Elle permet de faire cela automatiquement, évitant à l'utilisateur de passer du navigateur à son service de messagerie et vice versa pour mémoriser ou copier-coller manuellement le code reçu par sms. Elle réduit le risque de voir l'utilisateur abandonner la transaction du fait des contraintes liées au second facteur d'authentification. L'un des autres avantages est qu'elle ne nécessite pas de modifier les systèmes en vigueur. Ainsi, le serveur bancaire reste identique. En outre, du côté du terminal, le système d'exploitation reste identique, il n'est pas nécessaire de l'adapter ou de le mettre à jour. L'unique élément modifié est la présence de l'application mobile installée sur le terminal. En outre, cette application mobile peut être compatible avec tout système d'exploitation et tout serveur bancaire, de même qu'avec tout protocole de paiement utilisant une authentification à deux facteurs.

L'invention n'est pas limitée aux modes de réalisation présentés et d'autres modes de réalisation apparaîtront clairement à l'homme du métier. En particulier, le procédé d'authentification à deux facteurs peut être réalisé dans le cadre du protocole de paiement « 3D Secure » mais n'est pas limité à un tel type de protocole. De même, les canaux de communication peuvent être différents de ceux mentionnés, l'invention pouvant s'appliquer à tout type de canaux accessible par une application mobile, si nécessaire après demande d'accès au système d'exploitation.

Revendications

[Revendication 1] Procédé (100) d'authentification à deux facteurs d'une transaction bancaire, dans lequel, un terminal (8) d'un utilisateur étant relié à au moins un serveur de transaction bancaire (4) via des premier et deuxième canaux de communication, le deuxième canal étant un service de message court de téléphonie mobile les deux canaux étant logiquement distincts l'un de l'autre, le terminal comprenant en son sein une application mobile, on met en œuvre les étapes suivantes :

au préalable :

- l'application mobile (6) demande au système d'exploitation du terminal (8) à être alertée en cas de message reçu par le service de message court,
- l'application mobile (6) demande au système d'exploitation du terminal (8) la possibilité de lire les messages reçus par le service de message court,

ensuite :

- le serveur (4) détermine un code de vérification de la transaction,
- le serveur (4) envoie, à l'application mobile et via le deuxième canal, un message contenant le code de vérification,
- le serveur (4) envoie, au terminal (8) et via le premier canal, une requête demandant au terminal (8) de renvoyer le code de vérification via le premier canal,
- le terminal réceptionne la requête sur le premier canal,
- l'application mobile (6) détecte (102) automatiquement la réception du message sur le deuxième canal,
- l'application mobile (6) identifie (104) automatiquement le code de vérification de la transaction dans le message, et pour identifier (104) automatiquement le code de vérification dans le message, l'application mobile (6) identifie d'abord (103) automatiquement dans le message une chaine de caractère prédéterminée, distincte du code de vérification, attestant que le message comprend un code de vérification,

- le terminal renvoie (108), au serveur et via le premier canal, une réponse à la requête comprenant le code identifié.

[Revendication 2] Procédé (100) selon la revendication précédente, dans lequel le premier canal est un navigateur internet, et le deuxième canal est un service de message court de téléphonie mobile ou une messagerie de courriel.

[Revendication 3] Procédé (100) selon l'une quelconque des revendications précédentes, dans lequel, après avoir identifié (104) automatiquement le code de vérification dans le message et avant de renvoyer (108) la réponse au serveur, le terminal (8) copie (105) automatiquement le code, depuis le message reçu sur le premier canal, vers (106) la réponse à la requête sur le deuxième canal.

[Revendication 4] Procédé (100) selon l'une quelconque des revendications 1 à 2, dans lequel, après avoir identifié (104) le code de vérification dans le message et avant de renvoyer (108) la réponse au serveur :

- le terminal (8) copie (105) automatiquement le code, depuis le message reçu sur le premier canal, vers une mémoire tampon,
- l'utilisateur copie le code, depuis la mémoire tampon, vers la réponse à la requête sur le deuxième canal.

[Revendication 5] Procédé (100) selon l'une des revendications précédentes, dans lequel, la requête comportant un champ à remplir avec le code de vérification, la réponse à la requête comporte la requête avec le champ rempli.

[Revendication 6] Procédé (100) d'authentification à deux facteurs d'une transaction bancaire par un terminal mobile (8), dans lequel le terminal (8) comprend en sein une application mobile (6) mettant en œuvre les étapes suivantes :

au préalable :

- l'application mobile (6) demande au système d'exploitation du terminal (8) à être alertée en cas de message reçu par le service de message court,
- l'application mobile (6) demande au système d'exploitation du terminal (8) la possibilité de lire les messages reçus par le service de message court,

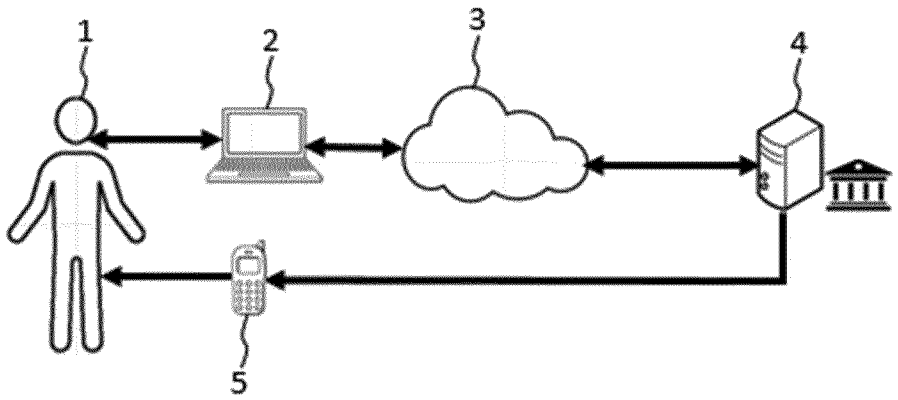
ensuite :

- réception d'une requête, sur un premier canal de communication du terminal (8), demandant le renvoi d'un code de vérification de la transaction,
- détection automatique (102) de la réception d'un message, sur un deuxième canal de communication du terminal (8) logiquement distinct du premier, le deuxième canal étant un service de message court de téléphonie mobile,
- identification automatique (104) d'un code de vérification de la transaction dans le message, dans laquelle, pour identifier (104) automatiquement le code de vérification dans le message, l'application mobile (6) identifie d'abord (103) automatiquement dans le message une chaine de caractère prédéterminée, distincte du code de vérification, attestant que le message comprend un code de vérification,
- envoi (108), via le deuxième canal, d'une réponse à la requête comprenant le code identifié.

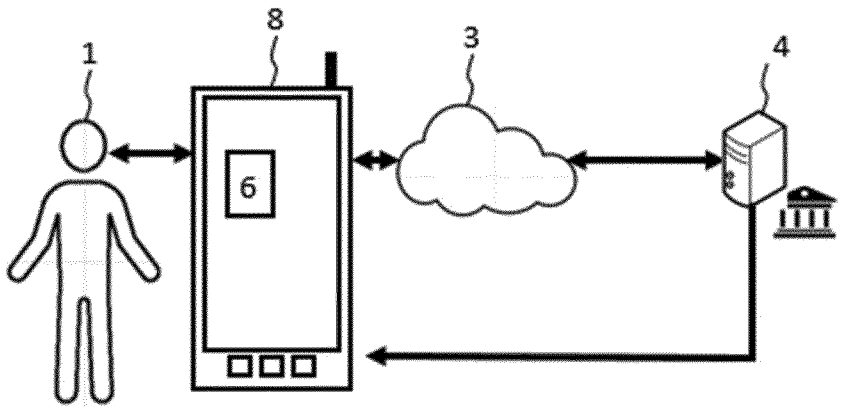
[Revendication 7] Procédé (100) selon la revendication précédente, dans lequel :
- l'application (6) demande également au préalable au système d'exploitation du terminal (8) la possibilité de supprimer les messages reçus par le service de message court,
- si un utilisateur du terminal (8) invalide la transaction via le premier canal, l'application (6) supprime (109) le message, reçu par le service de message court, comprenant le code de vérification de la transaction.

[Revendication 8] Programme d'ordinateur (6) pour terminal mobile comprenant des instructions qui, lorsque le programme est exécuté par un terminal mobile (8), conduisent celui-ci à mettre en œuvre les étapes des revendications 6 à 7.

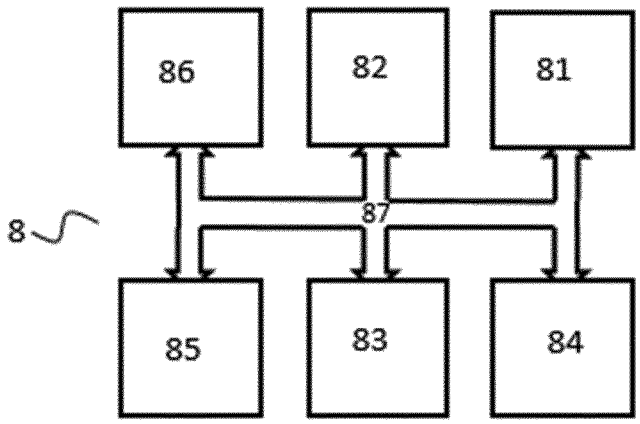
[Fig. 1]



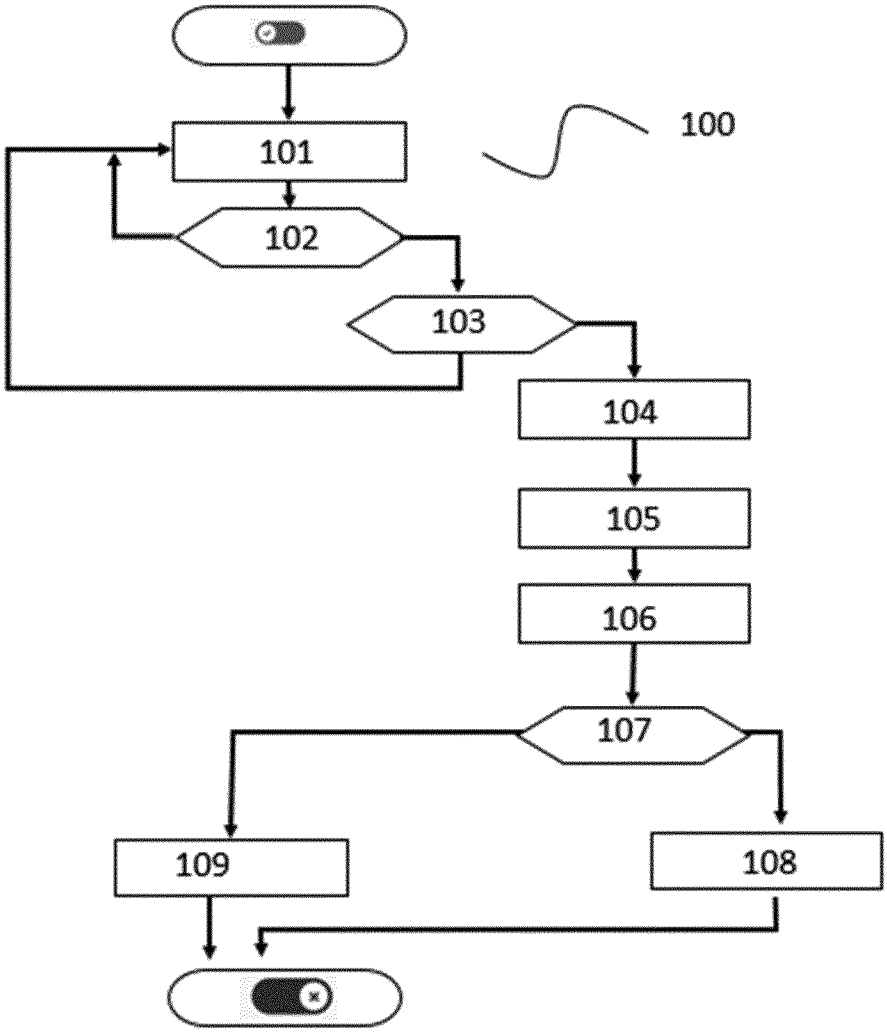
[Fig. 2]



[Fig. 3]



[Fig. 4]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2022/067612

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/32(2012.01)i; ***G06Q 20/42***(2012.01)i; ***G06Q 20/38***(2012.01)i; ***G06Q 20/40***(2012.01)i

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)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, 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	US 2007037591 A1 (CHOE JUN-YOUNG [KR] ET AL) 15 February 2007 (2007-02-15) figures 3, 4A-4C paragraph [0010] paragraph [0022] - paragraph [0027] paragraph [0031] paragraph [0033] - paragraph [0047]	1-8
X	EP 2405684 A2 (LG ELECTRONICS INC [KR]) 11 January 2012 (2012-01-11) figures 6, 8 paragraph [0070] - paragraph [0077]	1-8
X	US 2019385143 A1 (REISS DAVID [US]) 19 December 2019 (2019-12-19) figures 1, 4 paragraph [0019] paragraph [0027] - paragraph [0030]	1-8

☐ 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
21 September 2022	**29 September 2022**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Coquil, David** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2022/067612

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2007037591 A1	15 February 2007	KR 100651462 B1	29 November 2006
		US 2007037591 A1	15 February 2007
EP 2405684 A2	11 January 2012	EP 2405684 A2	11 January 2012
		KR 20120003731 A	11 January 2012
		US 2012005589 A1	05 January 2012
US 2019385143 A1	19 December 2019	US 2019385143 A1	19 December 2019
		WO 2019246303 A1	26 December 2019

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2022/067612

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. G06Q20/32 G06Q20/42 G06Q20/38 G06Q20/40
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06Q

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, 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	US 2007/037591 A1 (CHOE JUN-YOUNG [KR] ET AL) 15 février 2007 (2007-02-15) figures 3, 4A-4C alinéa [0010] alinéa [0022] - alinéa [0027] alinéa [0031] alinéa [0033] - alinéa [0047]	1-8
X	EP 2 405 684 A2 (LG ELECTRONICS INC [KR]) 11 janvier 2012 (2012-01-11) figures 6, 8 alinéa [0070] - alinéa [0077]	1-8
X	US 2019/385143 A1 (REISS DAVID [US]) 19 décembre 2019 (2019-12-19) figures 1, 4 alinéa [0019] alinéa [0027] - alinéa [0030]	1-8

☐ 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	Date d'expédition du présent rapport de recherche internationale
21 septembre 2022	29/09/2022

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Coquil, David

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2022/067612

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2007037591 A1	15-02-2007	KR 100651462 B1	29-11-2006
		US 2007037591 A1	15-02-2007
EP 2405684 A2	11-01-2012	EP 2405684 A2	11-01-2012
		KR 20120003731 A	11-01-2012
		US 2012005589 A1	05-01-2012
US 2019385143 A1	19-12-2019	US 2019385143 A1	19-12-2019
		WO 2019246303 A1	26-12-2019