(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
24 août 2017 (24.08.2017)

WIPO | PCT

(10) Numéro de publication internationale
WO 2017/140993 A1

(51) Classification internationale des brevets : *H04L 29/06* (2006.01)

(21) Numéro de la demande internationale : PCT/FR2017/050362

(22) Date de dépôt international : 17 février 2017 (17.02.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1651392 19 février 2016 (19.02.2016) FR

(71) Déposant : **OBERTHUR TECHNOLOGIES** [FR/FR]; 420 rue d'Estienne d'Orves, 92700 Colombes (FR).

(72) Inventeurs : **JOLETTE, Martin**; c/o OBERTHUR TECHNOLOGIES, 420 rue d'Estienne d'Orves, 92700 COLOMBES (FR). **COHEN-HADRIA, Igal**; c/o OBERTHUR TECHNOLOGIE, 420 rue d'Estienne d'Orves, 92700 COLOMBES (FR).

(74) Mandataires : **UNDERWOOD, Nicolas** et al.; CABINET BEAU DE LOMENIE, 158, Rue de l'Université, 75340 PARIS CEDEX 07 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, 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, 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))*

(54) **Title** : SYSTEM FOR AUTHENTICATING A USER WITH A SERVER

(54) **Titre** : SYSTÈME D'AUTHENTIFICATION D'UN UTILISATEUR AUPRÈS D'UN SERVEUR

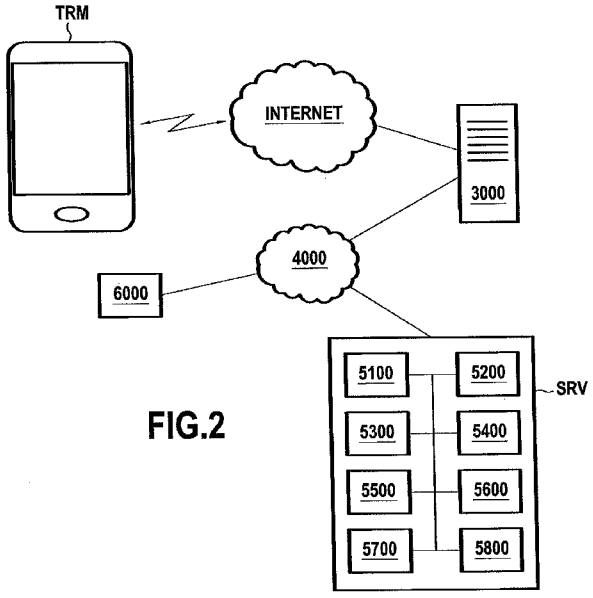

FIG.2

(57) **Abstract** : This system for authenticating a user comprises a microcircuit card (1000) comprising means for generating a dynamic security code (DCCVi) and a terminal (TRM) comprising: - means (MS) for obtaining the dynamic security code (DCCVi) generated by the microcircuit card (1000); - means (MOTP) for generating an authentication code on the basis of said dynamic security code (DCCVi), of a secret shared with said authentication server (SRV) and of a temporal datum obtained by said terminal. The authentication code can be dispatched to the authentication server by the terminal or by another device.

(57) **Abrégé** : Ce système d'authentification d'un utilisateur comporte une carte à microcircuit (1000) comportant des moyens de génération d'un code dynamique de sécurité (DCCVi) et un terminal (TRM) comportant : - des moyens (MS) d'obtention du code dynamique de sécurité (DCCVi) généré par la carte à microcircuit (1000); - des moyens (MOTP) de génération d'un code d'authentification à partir dudit code dynamique de sécurité (DCCVi), d'un secret partagé avec ledit serveur d'authentification (SRV) et d'une donnée temporelle obtenue par ledit terminal. Le code d'authentification peut être envoyé au serveur d'authentification par le terminal ou par un autre équipement.

WO 2017/140993 A1

Système d'authentification d'un utilisateur auprès d'un serveur.

Arrière-plan de l'invention

L'invention se situe dans le domaine de l'authentification d'un terminal utilisateur auprès d'un serveur d'authentification.

Dans l'état actuel de la technique, on connaît, par exemple pour sécuriser l'accès à un site bancaire, l'utilisation d'un petit boitier sécurisé (en anglais « token ») au format d'une petite calculatrice, permettant à un utilisateur d'obtenir un code d'authentification, par exemple sur saisie des derniers chiffres de son numéro de compte.

Cette solution présente l'inconvénient de reposer sur l'utilisation d'un tel boîtier dédié et du coût associé pour l'établissement bancaire.

Afin de supprimer ces coûts, une solution alternative a été proposée dans laquelle le boîtier sécurisé est remplacé par une application mobile s'exécutant sur un terminal mobile. Cette deuxième solution présente l'inconvénient d'être vulnérable aux attaques logicielles (par exemple par un malware).

L'invention vise à une solution d'authentification qui ne présente pas les inconvénients mentionnés ci-dessus.

Objet et résumé de l'invention

A cet effet, et selon un premier aspect, l'invention concerne un procédé d'authentification mis en œuvre par un serveur d'authentification pour authentifier un terminal, ce procédé comportant :

- une étape de réception d'une requête pour vérifier un code d'authentification ;
- une étape d'obtention, par une fonction cryptographique secrète, d'un code dynamique de sécurité en utilisant un numéro de compte bancaire associé audit terminal, et une donnée temporelle obtenue par ledit serveur ;
- une étape d'obtention d'un code de vérification à partir dudit code dynamique de sécurité, d'une clef secrète partagée entre ledit terminal et ledit serveur et d'une donnée temporelle obtenue par ledit serveur ;

- une étape de vérification de la validité dudit code d'authentification en le comparant avec ledit code de vérification.

Selon un deuxième aspect, l'invention concerne aussi un procédé d'authentification d'un terminal auprès d'un serveur d'authentification, ledit procédé comportant :

- une étape, mise en œuvre par le terminal, d'obtention d'un code dynamique de sécurité généré par une carte à microcircuit ;
- une étape, mise en œuvre par le terminal, de génération d'un code d'authentification à partir dudit code dynamique de sécurité, d'un secret partagé avec ledit serveur d'authentification et d'une donnée temporelle obtenue par le terminal ; et
- une étape d'envoi du code d'authentification au serveur pour authentifier ledit terminal auprès dudit serveur.

Ainsi, et d'une façon générale, l'invention propose de sécuriser une transaction en générant un code d'authentification à partir d'un code dynamique de sécurité généré par une carte à microcircuit, d'une clef secrète partagée entre le terminal et le serveur et de données temporelles synchronisées mais calculées indépendamment par le serveur et par le terminal chacun avec ses propres moyens , par exemple avec sa propre horloge.

On rappelle en effet que depuis peu, on connaît des cartes à microcircuit, aussi connues sous le nom de cartes « motion code » (voir [REFMC]), de telles cartes étant notamment décrites dans le document US2014/0279555, dans lesquelles un code dynamique de sécurité (aussi connu sous le nom de « motion code ») est changé régulièrement, par exemple toutes les 45 mn environ et affiché sur un écran de la carte à microcircuit sans intervention de l'utilisateur.

Cette solution présente l'intérêt de ne pas nécessiter de boîtier dédié comme dans la première solution de l'art antérieure présentée en préambule et de ne pas être vulnérable aux attaques logicielles, notamment de type malware.

Les données temporelles utilisées par le terminal et le serveur d'authentification peuvent être des compteurs. Ces compteurs sont préférentiellement mis à jour plus souvent que le code dynamique de sécurité généré par la carte à microcircuit.

Dans un mode particulier de réalisation de l'invention, ledit code d'authentification constitue un mot de passe temporaire à durée de vie limitée.

Dans un mode particulier de réalisation de l'invention, les codes dynamiques de sécurité générés par le terminal et par le serveur sont des codes à 3 ou 4 chiffres.

Dans un mode particulier de réalisation de l'invention, le code d'authentification est un code dont la longueur est supérieure à celle dudit code dynamique de sécurité, par exemple un code à 6 chiffres.

Dans un mode particulier de réalisation, le terminal effectue l'étape d'envoi du code d'authentification au serveur.

En variante, cet envoi est réalisé par un autre équipement, par exemple un ordinateur personnel utilisé par l'utilisateur pour effectuer une transaction.

Cette variante renforce encore la sécurité du procédé d'authentification selon l'invention, puisqu'une attaque malveillante nécessite dans ce cas d'attaquer simultanément, le terminal utilisateur et ce deuxième équipement.

La sécurité peur encore être renforcée en prévoyant un mécanisme d'authentification au niveau du deuxième équipement, par exemple par mot de passe ou mesure de données biométiques.

Dans un mode particulier de réalisation, le procédé d'authentification mis en œuvre par le serveur d'authentification comporte une étape de génération ou de renouvellement dudit secret partagé à partir d'un identifiant dudit terminal utilisateur et d'envoi d'une information obtenue à partir de ce secret audit terminal.

Dans un mode particulier de réalisation du procédé d'authentification mis en œuvre par le serveur d'authentification, au moins une sous-étape de ladite étape d'obtention dudit code dynamique de sécurité ou de ladite étape d'obtention dudit code de vérification est mise en œuvre par une entité matérielle sécurisée.

Dans un mode particulier de réalisation, le procédé d'authentification mis en œuvre par le terminal comporte une étape préalable d'authentification de l'utilisateur du terminal auprès du terminal.

Dans un mode particulier de réalisation du procédé d'authentification mis en œuvre par le terminal, l'étape de génération du

code d'authentification prend en compte des données d'entrée supplémentaires propres à une transaction.

Dans un mode particulier de réalisation du procédé d'authentification mis en œuvre par le terminal, le code d'authentification est généré par le terminal plus fréquemment que le code dynamique de sécurité n'est généré par la carte à microcircuit.

Corrélativement, l'invention concerne un serveur d'authentification pouvant être utilisé pour authentifier un terminal, ce serveur comportant :

- des moyens de réception d'une requête pour vérifier un code d'authentification ;
- des moyens d'obtention, par une fonction cryptographique secrète, d'un code dynamique de sécurité en utilisant un numéro de compte bancaire associé audit terminal et une donnée temporelle obtenue par le serveur ;
- des moyens cryptographiques d'obtention d'un code de vérification à partir dudit code dynamique de sécurité, d'une clef secrète partagée entre ledit terminal et ledit serveur et d'une donnée temporelle obtenue par ledit serveur ;
- des moyens de vérification de la validité dudit code d'authentification en le comparant avec ledit code de vérification.

L'invention vise aussi un terminal comportant :

- des moyens d'obtention d'un code dynamique de sécurité généré par une carte à microcircuit ;
- des moyens de génération d'un code d'authentification à partir dudit code dynamique de sécurité, d'un secret partagé avec le serveur d'authentification et d'une donnée temporelle obtenue par ledit terminal.

Dans un mode particulier de réalisation , le terminal comporte des moyens d'envoi dudit code d'authentification audit serveur pour authentifier ledit terminal auprès dudit serveur.

Le terminal est par exemple un terminal mobile, un téléphone mobile ou une tablette tactile.

Dans un mode particulier de réalisation de l'invention, les moyens du terminal pour obtenir le code dynamique de sécurité sont constitués par une zone de saisie dans laquelle l'utilisateur peut saisir ce code après l'avoir lu sur un écran de la carte à microcircuit.

L'invention vise également un système d'authentification d'un utilisateur comportant :

- une carte à microcircuit comportant des moyens de génération d'un code dynamique de sécurité; et
- un terminal tel que mentionné ci-dessus, ce terminal comportant des moyens d'obtention du code dynamique de sécurité généré par cette carte.

Dans un mode particulier de réalisation dy système selon l'invention, le code d'authentification est généré par le terminal plus fréquemment que le code dynamique de sécurité n'est généré par la carte à microcircuit.

Dans un mode particulier de réalisation de l'invention, la carte à microcircuit utilisée pour générer le code dynamique de sécurité prséente au moins une caractéristique suivante :

- la carte est conforme à la norme ISO7816 ;
- la carte est au format ID1 ;
- la carte est une carte de paiement ;
- la carte comporte en particulier une interface à contacts affleurant ;
- la carte comporte le nom du titulaire de la carte à microcircuit, un numéro de compte bancaire et une date d'expiration, le numéro de compte bancaire, la date d'expiration et le code dynamique de sécurité permettant de réaliser une transaction de paiement.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif et dans lesquels:

- la figure 1 représente une carte à microcircuit pouvant être utilise dans un mode de mise en œuvre de l'invention;
- la figure 2 représente, de façon schématique, un terminal et un serveur d'authentification conformes à un mode particulier de réalisation de l'invention, dans leur environnement ;
- la figure 3 représente un terminal conforme à un mode particulier de réalisation de l'invention ;

- la figure 4 représente sous forme d'organigramme les principales étapes d'un procédé d'authentification conforme à un mode particulier de réalisation de l'invention, mis en œuvre par le terminal de la figure 2 ;

- la figure 5 représente sous forme d'organigramme les principales étapes d'un procédé d'authentification conforme à un mode particulier de réalisation de l'invention, mis en œuvre par le serveur d'authentification de la figure 2 ; et

- la figure 6 représente des échanges de message entre les différents équipements de la figure 2 au cours d'un exemple de mise en œuvre de l'invention.

Description détaillée d'un premier mode de réalisation

La **figure 1** représente une carte à microcircuit (en anglais smartcard) de paiement. Dans le mode de réalisation décrit ici, la carte à microcircuit 1000 est conforme à la norme ISO7816. Elle comporte en particulier une interface à contacts affleurant 1300.

De façon connue, le nom NOM du titulaire de la carte à microcircuit, un numéro de compte bancaire PAN (par exemple à 16 chiffres), une date d'expiration EXP sont imprimés sur la carte à microcircuit 1000. La carte comporte en outre un code statique de sécurité CVV, celui-ci pouvant être ou ne pas être imprimé sur la carte. Pour plus de renseignements sur :

- le code statique de sécurité CVV, l'homme du métier peut consulter le document [REFCVV] ;

- le numéro de compte bancaire PAN, l'homme du métier peut consulter le document [REFPAN].

Cette carte à microcircuit 1000 comporte un contrôleur 1200 comportant un module apte à fournir la date courante, par exemple une horloge CLK, ce contrôleur 1200 étant apte à calculer un code dynamique de sécurité $DCCV_1$ en appliquant une fonction cryptographique secrète à des paramètres comportant le numéro de compte bancaire PAN et un paramètre temporel.

Dans le mode de réalisation décrit ici, le code dynamique de sécurité $DCCV_1$ est varié de façon périodique, selon une période prédéterminée.

Au contraire, le code statique de sécurité CVV est constant dans le temps.

La carte à microcircuit 1000 comporte un écran 1100 d'affichage de ce code dynamique de sécurité $DCCV_1$. Cet écran peut comporter par exemple 3 ou 4 zones élémentaires selon la taille de ce code dynamique.

Dans le mode de réalisation décrit ici, la carte à microcircuit 1000 comporte en outre une batterie non représentée permettant d'alimenter l'écran d'affichage 1100, notamment lorsque le code dynamique de sécurité $DCCV_1$ est modifié.

Afin de limiter la consommation de cette batterie, il peut être souhaitable de ne pas modifier le code dynamique de sécurité $DCCV_1$ trop souvent.

La **figure 2** représente un terminal TRM et un serveur d'authentification SRV conformes à un mode particulier de réalisation de l'invention, un serveur d'application 3000, le système bancaire 6000 de l'entité émettrice de la carte à microcircuit 1000, et un serveur d'authentification SRV conforme à l'invention.

Dans le mode de réalisation décrit ici, le terminal TRM accède au serveur d'application 3000 par le réseau Internet ; le serveur d'application 3000, le système bancaire 6000 et le serveur SRV d'authentification communiquent via un réseau interbancaire 4000.

En référence à la **figure 3**, le terminal utilisateur TRM est dans cet exemple constitué par un téléphone mobile. Il comporte notamment un écran tactile SCR, un clavier KB, un processeur CPU, une mémoire morte MM, une mémoire non volatile réinscriptible MF et une mémoire vive MV, un module de communication COM, ces éléments étant reliés entre eux par un système de bus non représenté.

Le terminal utilisateur comporte des moyens MS de saisie permettant à un utilisateur de saisir un code dynamique de sécurité $DCCV_1$ calculé par la carte à microcircuit 1000. Ces moyens de saisie MS peuvent être constitués par une fenêtre de saisie à 3 ou 4 zones élémentaires, en fonction de la taille du code $DCCV_1$.

Le module de communication 1000 est apte à envoyer ce code dynamique de sécurité $DCCV_1$ au serveur d'authentification SRV.

. Le terminal utilisateur comporte également un module cryptographique MOTP apte à générer un code d'authentification OTP_1, à

partir du code dynamique de sécurité $DCCV_1$ saisi par l'utilisateur et d'un secret KD partagé avec le serveur d'authentification SRV. Le secret partagé KD est dans cet exemple mémorisé dans la mémoire MF. Le module de communication COM est apte à envoyer le code d'authentification OTP1 au serveur d'authentification SRV.

Dans le mode de réalisation de l'invention décrit ici, le code d'authentification OTP1 est renouvelé plus fréquemment que le code dynamique de sécurité $DCCV_1$ par la carte à microcircuit.

La mémoire morte MM comporte un programme d'ordinateur (ou application) APP conforme à l'invention. Cette application APP comporte des instructions, qui lorsqu'elles sont exécutées par le processeur CPU, permettent de mettre en œuvre les étapes E20 à E40 du procédé d'authentification conforme à l'invention et dont les principales étapes seront décrites en référence à la figure 4.

L'architecture du serveur d'authentification SRV est représentée à la figure 1. Il comporte notamment :

- un module 5100 apte à obtenir à obtenir une donnée temporelle, soit en utilisant des moyens internes, soit par exemple à partir d'un autre équipement ou d'un autre réseau, par des moyens de communications sans fil ou filaires ;
- un module 5200 de communication apte notamment à recevoir simultanément ou séparément un premier code dynamique de sécurité $DCCV_1$ et un code d'authentification OTP_1 envoyés par le terminal utilisateur TRM ;
- un module 5300 de génération d'un deuxième code dynamique de sécurité $DCCV_2$ en utilisant un numéro de compte bancaire PAN, une fonction cryptographique secrète et une donnée temporelle obtenue par le module 5100 ; et
- un module 5400 de vérification de la validité d'un premier code dynamique de sécurité $DCCV_1$ généré par une carte bancaire 1000 en le comparant avec le deuxième code dynamique de sécurité $DCCV_2$.

On notera que dans un mode de réalisation, le serveur d'authentification coopère avec une entité matérielle sécurisée HSM pour générer le deuxième code dynamique de sécurité $DCCV_2$ et/ou vérifier la validité du premier code dynamique de sécurité $DCCV_1$ par comparaison

avec le deuxième code dynamique de sécurité $DCCV_2$ comme mentionné ci-dessus.

Pour plus de renseignements sur une telle entité matérielle sécurisée HSM, l'homme du métier peut se reporter au document [REFHSM].

Le serveur d'authentification SRV comporte également :

- des moyens 5500 d'obtention et de renouvellement, à partir d'un identifiant du terminal utilisateur TRM, d'un secret KD pouvant être partagé avec le terminal TRM ;
- un module 5600 d'obtention, à partir du secret partagé KD et du deuxième code dynamique de sécurité $DCCV_2$, d'un secret à durée de vie limitée KSL. Ce module 5600 utilise à cet effet une fonction de code d'authentification de message HMAC :

$$KSL = HMAC(KD, DCCV_2).$$

Pour plus de renseignements sur les fonctions de code d'authentification de message, l'homme du métier peut se reporter à la référence [REFHMAC].

Le serveur SRV est apte à envoyer le secret partagé KD et/ou le secret à durée de vie limitée KSL au terminal utilisateur TRM en utilisant son module de communication 5200.

Le serveur d'authentification SRV comporte également :

- un module cryptographique 5700 de génération d'un code de vérification OTP_2 à partir du code dynamique de sécurité $DCCV_2$ obtenu par ce serveur et du secret partagé KD, éventuellement en coopération avec l'entité HSM ; et
- un module 5800 de vérification de la validité du code d'authentification OTP_1 en le comparant avec le code de vérification OTP_2.

On notera là encore, que dans un mode de réalisation, le serveur d'authentification coopère avec l'entité HSM pour générer le code de vérification OTP_2 et/ou vérifier la validité du code d'authentification OTP_1 par comparaison avec le deuxième code de vérification OTP_2 comme mentionné ci-dessus.

Le serveur d'authentification SRV est apte à envoyer un message au serveur d'application 3000 ou système bancaire 6000 pour autoriser une transaction lorsque la validité du code d'authentification OTP_1 a été vérifiée.

Exemple de procédé d'authentification mis en œuvre par le terminal utilisateur

La **figure 4** représente les principales étapes d'un procédé d'authentification d'un utilisateur auprès d'un serveur d'authentification SRV conforme à l'invention, ce procédé étant mis en œuvre par le terminal utilisateur TRM.

Au cours d'une étape E10, l'utilisateur s'authentifie sur son terminal utilisateur TRM. Cette étape E10 d'authentification peut être réalisée en saisissant un code personnel d'identification (en anglais « PIN CODE »), constitué par exemple de 4 chiffres, en utilisant le clavier numérique KB du terminal TRM. Dans une variante, cette étape E10 d'authentification peut être réalisée par l'utilisateur en dessinant, sur l'écran tactile SCR du terminal TRM, un motif préalablement mémorisé dans la mémoire non volatile réinscriptible MF du terminal TRM. Dans une autre variante, cette étape E10 d'authentification peut par exemple être réalisée par des moyens biométriques aptes à identifier une caractéristique physique de l'utilisateur, par exemple une empreinte digitale, un iris, ...

En cas de succès de l'étape E10 d'authentification de l'utilisateur, l'application APP du terminal TRM invite l'utilisateur, au cours d'une étape E20 à saisir, dans la zone de saisie MS, un code dynamique de sécurité $DCCV_1$ affiché sur l'écran 1100 de la carte à microcircuit 1000.

Conformément, à l'invention, au cours d'une étape E30, l'application APP génère un code d'authentification OTP_1 à partir du premier code dynamique de sécurité $DCCV_1$ saisi à l'étape E20 et du secret KD partagé avec le serveur d'authentification SRV. Une façon dont ce secret partagé KD peut être renouvelé et transmis au terminal utilisateur TRM par le serveur d'authentification SRV sera décrite ultérieurement.

Le code d'authentification OTP_1 est utilisé par l'utilisateur pour s'authentifier auprès du serveur SRV au cours d'une étape E40.

Selon le scénario de mise en œuvre de l'invention, et comme décrit ultérieurement, le code d'authentification OTP_1 peut être généré à l'étape E30 sans donnée d'entrée ou avec données d'entrée saisies par exemple au moyen du clavier KB du terminal TRM.

Dans un mode particulier de réalisation, le code d'authentification OTP_1 est un cryptogramme à 6 chiffres.

Dans le mode de réalisation décrit ici, ce code d'authentification OTP_1 est calculé partir d'un secret à durée de vie limitée KSL et d'une donnée temporelle TC obtenue par le terminal utilisateur TRM. Ce secret à durée de vie limitée KSL peut être reçu directement du serveur SRV ou recalculé par le terminal TRM à partir du secret partagé KD reçu de ce serveur.

Par exemple, dans le mode de réalisation décrit ici, le secret à durée de vie limitée KSL est obtenu par le terminal utilisateur en appliquant une fonction de code d'authentification de message HMAC prenant en entrée le secret KD partagé avec le serveur d'authentification SRV et le premier code dynamique de sécurité $DCCV_1$ saisi par l'utilisateur :

$$KSL = HMAC(KD, DCCV_1).$$

Par exemple, OTP_1 = HOTP (KSL, TC), avec :

- HOTP(K, C) = Truncate(HMAC(K,C)) & 7FFFFFFF16

La durée temporelle TC peut par exemple être un compteur calculé à partir de l'instant courant et d'une période de temps. Par exemple :

$$TC= (unixtime(now) - unixtime(T0)) / TS,$$

où T0 et TS sont des paramètres temporels spécifiques connus de l'application APP et du serveur d'authentification SRV.

Exemple de procédé d'authentification mis en œuvre par le serveur d'authentification SRV

La **figure 5** représente les principales étapes d'un procédé d'authentification de l'utilisateur d'un terminal TRM, ce procédé étant mis en œuvre par un serveur d'authentification SRV conforme à l'invention.

On supposera qu'au cours d'une étape F10, le serveur d'authentification SRV a généré ou renouvelé, à partir d'un identifiant du terminal utilisateur TRM un secret KD et envoyé ce secret KD au terminal TRM. En ce sens le secret KD est partagé entre le serveur SRV et le terminal TRM.

Comme mentionné précédemment, le serveur SRV peut également ou de façon alternative envoyer au terminal utilisateur TRM un secret à durée de vie limitée KSL, le terminal TRM étant apte à recalculer le secret à durée de vie limitée KSL à partir du secret partagé KD et du premier code dynamique de sécurité $DCCV_1$.

Au cours d'une étape F20, le serveur d'authentification SRV reçoit, du serveur d'application 3000, une requête pour vérifier un code d'authentification OTP_1 envoyé à ce serveur 3000 par un terminal utilisateur TRM.

Au cours d'une étape F30, le serveur d'authentification génère, ou demande la génération, par exemple à une entité HSM, d'un code dynamique de sécurité $DCCV_2$ (deuxième code au sens de l'invention) en utilisant un numéro de compte bancaire PAN associé au terminal utilisateur TRM, une fonction cryptographique secrète et une donnée temporelle CTC obtenue par ce serveur.

Puis au cours d'une étape F40, le serveur d'authentification génère, ou demande la génération, par exemple à une entité HSM, d'un code de vérification OTP2, à partir du deuxième code dynamique de sécurité $DCCV_2$, de la clef secrète KD partagée avec le terminal TRM et d'une donnée temporelle ATC obtenue par le serveur. Par exemple :

$$KSL_2 = HMAC(KD, DCCV_2).$$

Par exemple, $OTP_2 = HOTP (KSL_2, ATC)$,

Le serveur SRV vérifie la validité du code d'authentification OTP_1 en le comparant avec le code de vérification OTP2 au cours d'une étape F50.

Dans le mode de réalisation, il renvoie le résultat de ce cette vérification (OK, NOK) au serveur d'application 3000 au cours d'une étape F60.

Description d'un premier scénario de mise en œuvre de l'invention

Dans un premier scénario, on suppose que l'utilisateur souhaite utiliser un ordinateur personnel pour s'authentifier auprès d'un serveur bancaire SRV, par exemple pour consulter l'état de son compte en banque ou imprimer un relevé d'identité bancaire.

Dans ce scénario, l'utilisateur demande la génération d'un code d'authentification OTP_1 comme décrit précédemment en référence aux étapes E10 à E30, et le code d'authentification OTP_1 s'affiche sur l'écran SCR du terminal comme représenté à la figure 4C.

Ce code d'authentification OTP_1 constitue un mot de passe temporaire (en anglais « one time password ») dont la durée de vie limitée TTL restante avant expiration de ce code s'affiche sur l'écran du terminal TRM.

Ce code d'authentification OTP_1 est alors saisi par l'utilisateur sur son ordinateur personnel pour s'authentifier auprès du serveur bancaire SRV.

Description d'un deuxième scénario de mise en œuvre de l'invention

Dans ce deuxième scénario, on suppose que l'utilisateur souhaite utiliser un ordinateur personnel pour effectuer un achat en ligne s'authentifier auprès d'un site marchand.

Dans ce scénario, au moment de payer, le serveur SRV de paiement du site marchand envoie une requête d'authentification à l'application APP, cette requête comportant avec le montant et des informations sur la transaction, par exemple les détails d'un titre de transport, ou d'un ticket de réservation de spectacle.

L'application APP invite ensuite l'utilisateur, comme décrit précédemment en référence à l'étape E20, à saisir le code dynamique de sécurité $DCCV_1$ affiché sur l'écran 1100 de la carte à microcircuit 1000.

Dans ce scénario d'utilisation, l'application APP génère, au cours de l'étape E30, le code d'authentification OTP_1 avec des données d'entrée constituées par exemple par le montant et/ou par au moins une partie des informations sur la transaction. Le code d'authentification OTP_1 peut s'afficher sur l'écran SCR du terminal TRM.

Ce code d'authentification OTP_1 est alors saisi par l'utilisateur sur son ordinateur personnel pour s'authentifier auprès du serveur de paiement SRV du site marchand.

Ce deuxième scénario de mise en œuvre de l'invention peut également et notamment être utilisé pour permettre à un utilisateur de

s'authentifier auprès d'un serveur bancaire SRV afin d'effectuer un virement vers un compte bénéficiaire dont le numéro est saisi par l'utilisateur au moyen du clavier KB du terminal TRM. Une partie de ce numéro de compte peut constituer une donnée d'entrée pour générer le code d'authentification OTP_1 à l'étape E30.

Description d'un troisième scénario de mise en œuvre de l'invention

Dans le deuxième scénario décrit ci-dessus, le code d'authentification OTP_1 calculé à l'étape E30 est saisi par l'utilisateur sur son ordinateur personnel pour s'authentifier auprès d'un serveur SRV (serveur de paiement du site marchand ou serveur bancaire).

Dans un troisième scénario de mise en œuvre de l'invention, le code d'authentification OTP_1 calculé par le terminal TRM à l'étape E30 est directement envoyé au serveur SRV par le terminal utilisateur TRM.

On notera que dans ce mode de réalisation, il n'est pas nécessaire que le code d'authentification OTP_1 s'affiche sur l'écran SCR du terminal TRM.

Description détaillée d'un autre mode de réalisation de l'invention

La **figure 6** représente un mode de réalisation de l'invention dans lequel on met régulièrement à jour le deuxième secret dans le téléphone.

Au cours d'une première étape G10, l'utilisateur se connecte avec son ordinateur personnel auprès d'un portail P, en saisissant l'URL de ce portail dans un navigateur Internet installé sur cet ordinateur.

Au cours d'une étape G20, le portail P envoie à l'ordinateur personnel une page Web permettant à l'utilisateur de saisir un code d'authentification OTP_1.

Au cours d'une étape G30, l'utilisateur lance l'application APP sur son terminal utilisateur TRM.

Au cours d'une étape G40, l'application APP demande à l'utilisateur de saisir un code dynamique de sécurité $DCCV_1$ dans une zone de saisie affichée sur l'écran SCR de ce terminal TRM.

Au cours d'une étape G50, l'utilisateur lit le code dynamique $DCCV_1$ affiché sur l'écran DISP de la carte à microcircuit 1000 et saisit ce code dynamique $DCCV_1$ dans cette zone de saisie.

Au cours d'une étape G60, l'application APP demande à l'utilisateur de s'authentifier sur le terminal TRM, par exemple en saisissant un code personnel, en dessinant un motif sur l'écran SCR ou par lecture de données biométriques.

Si le terminal TRM authentifie effectivement l'utilisateur (étape G70), l'application APP interroge au cours d'une étape G70, le serveur d'authentification SRV pour obtenir le secret partagé KD.

Dans le mode de réalisation décrit ici, ce secret KD est renouvelé au cours d'une étape G80 et renvoyé au terminal TRM au cours d'une étape G90.

Le terminal TRM génère le code d'authentification OTP_1 au cours d'une étape G100 en utilisant le code dynamique de sécurité $DCCV_1$ saisi à l'étape G50 et le secret partagé KD reçu à l'étape G90.

Au cours d'une étape G110, l'utilisateur saisit le code d'authentification OTP_1 dans la page Web reçue du portail P à l'étape F20.

Au cours d'une étape G120, le portail P transmet le code d'authentification OTP_1 au serveur d'authentification SRV pour demander sa vérification.

A cet effet, au cours d'une étape G130, le serveur d'authentification calcule, seul, ou en combinaison avec une entité HSM :

- un code dynamique de sécurité DCCV2 en utilisant un numéro de compte bancaire PAN associé au terminal utilisateur TRM, une fonction cryptographique secrète et une donnée temporelle obtenue par ce serveur ;
- un code de vérification OTP2, à partir du code dynamique de sécurité DCCV2, de la clef secrète KD partagée avec le terminal TRM et d'une donnée temporelle TC obtenue par le serveur.

Le serveur SRV vérifie la validité du code d'authentification OTP_1 en le comparant avec le code de vérification OTP_2.

Dans le mode de réalisation, le serveur renvoie le résultat de ce cette vérification (OK, NOK) au serveur d'application SRV au cours d'une étape G140.

Références :

[REFMC] : http://www.oberthur.com/fr/le-groupe-bpce-lance-avec-oberthur-technologies-une-innovation-mondiale-la-premiere-carte-bancaire-a-cryptogramme-dynamique/

[REFCVV] : en.wikipedia.org/wiki/card_security_code

[REFPAN] : en.wikipedia.org/wiki/Bank_card_number

[REFHSM] : HSM : https://fr.wikipedia.org/wiki/Hardware_Security_Module

[REFHMAC] :https://fr.wikipedia.org/wiki/Keyed-Hash_Message_Authentication_Code

REVENDICATIONS

1. Procédé d'authentification mis en œuvre par un serveur d'authentification pour authentifier un terminal (TRM), ce procédé comportant :
- une étape (F20) de réception d'une requête pour vérifier un code d'authentification (OTP_1) ;
- une étape (F30) d'obtention, par une fonction cryptographique secrète, d'un code dynamique de sécurité ($DCCV_2$) en utilisant un numéro de compte bancaire associé audit terminal (TRM), et une donnée temporelle (CTC) obtenue par ledit serveur (SRV)
- une étape (F40) d'obtention d'un code de vérification (OTP2) à partir dudit code dynamique de sécurité ($DCCV_2$), d'une clef secrète (KD) partagée entre ledit terminal (TRM) et ledit serveur (SRV) et d'une donnée temporelle (ATC) obtenue par ledit serveur ;
- une étape (F50) de vérification de la validité dudit code d'authentification (OTP_1) en le comparant avec ledit code de vérification (OTP2)

2. Procédé d'authentification selon la revendication 1, caractérisé en ce qu'il comporte une étape de génération ou de renouvellement dudit secret partagé (KD) à partir d'un identifiant dudit terminal utilisateur (TRM) et d'envoi (F10) d'une information (KD, KSL) obtenue à partir de ce secret audit terminal (TRM).

3. Procédé d'authentification selon la revendication 1 ou 2, caractérisé en ce que au moins une sous-étape de ladite étape (F30) d'obtention dudit code dynamique de sécurité ($DCCV_2$) ou de ladite étape (F40) d'obtention dudit code de vérification (OTP2) est mise en œuvre par une entité matérielle sécurisée (HSM).

4. Procédé d'authentification d'un terminal (TRM) auprès d'un serveur d'authentification (SRV), ledit procédé comportant :
- une étape (E20), mise en œuvre par ledit terminal, d'obtention un code dynamique de sécurité ($DCCV_1$) généré par une carte à microcircuit (1000) ;

- une étape (E30), mise en œuvre par ledit terminal ; de génération d'un code d'authentification (OTP_1) à partir dudit code dynamique de sécurité ($DCCV_1$), d'un secret (KD) partagé avec ledit serveur d'authentification (SRV) et d'une donnée temporelle (TC) obtenue par ledit terminal ; et
- une étape (E40) d'envoi dudit code d'authentification (OTP_1) audit serveur (SRV) pour authentifier ledit terminal (TRM) auprès dudit serveur (SRV).

5. Procédé d'authentification selon la revendication 4, caractérisé en ladite étape (E40) d'envoi un effectué par un autre équipement.

6. Procédé d'authentification selon la revendication 4 ou 5, caractérisé en ce qu'il comporte une étape préalable (E10) d'authentification de l'utilisateur du terminal auprès dudit terminal (TRM).

7. Procédé d'authentification selon l'une quelconque des revendications 4 à 6, caractérisé en ce que ladite étape (E30) de génération dudit code d'authentification (OTP_1) prend en compte des données d'entrée supplémentaires propres à une transaction.

8. Procédé d'authentification selon l'une quelconque des revendications 4 à 7, caractérisé en ce que ledit code d'authentification (OTP_1) constitue un mot de passe temporaire à durée de vie limitée.

9. Procédé d'authentification selon l'une quelconque des revendications 1 à 8 caractérisé en ce que ledit code d'authentification (OTP_1) est un code dont la longueur est supérieure à celle dudit code dynamique de sécurité ($DCCV_1$, $DCCV_2$), par exemple un code à 6 chiffres.

10. Procédé d'authentification selon l'une quelconque des revendications 1 à 9 caractérisé en ce que ledit code dynamique de sécurité ($DCCV_1$, $DCCV_2$) est un code à 3 ou 4 chiffres.

11. Serveur d'authentification pouvant être utilisé pour authentifier un terminal (TRM), ce serveur comportant :

- des moyens (5200) de réception d'une requête pour vérifier un code d'authentification (OTP_1) ;
- des moyens (5300) d'obtention, par une fonction cryptographique secrète, d'un code dynamique de sécurité ($DCCV_2$) en utilisant un numéro de compte bancaire associé audit terminal (TRM) et une donnée temporelle (CTC) obtenue par ledit serveur (SRV) ;
- des moyens cryptographiques (5700) d'obtention d'un code de vérification (OTP2) à partir dudit code dynamique de sécurité ($DCCV_2$), d'une clef secrète (KD) partagée entre ledit terminal (TRM) et ledit serveur (SRV) et d'une donnée temporelle (ATC) obtenue par ledit serveur ;
- des moyens (5800) de vérification de la validité dudit code d'authentification (OTP_1) en le comparant avec ledit code de vérification (OTP2).

12. Terminal (TRM) comportant :
- des moyens (MS) d'obtention d'un code dynamique de sécurité ($DCCV_1$) généré par une carte à microcircuit (1000) ;
- des moyens (MOTP) de génération d'un code d'authentification (OTP_1) à partir dudit code dynamique de sécurité ($DCCV_1$), d'un secret (KD) partagé avec ledit serveur d'authentification (SRV) et d'une donnée temporelle (TC) obtenue par ledit terminal.

13. Terminal selon la revendication 12 caractérisé en ce qu'il comporte des moyens (COM) d'envoi dudit code d'authentification (OTP_1) audit serveur (SRV) pour authentifier ledit terminal (TRM) auprès dudit serveur (SRV).

14. Système d'authentification d'un utilisateur comportant :
- une carte à microcircuit (1000) comportant des moyens de génération d'un code dynamique de sécurité ($DCCV_1$) ; et
- un terminal selon la revendication 12 ou 13, ce terminal comportant des moyens d'obtention dudit code dynamique de sécurité ($DCCV_1$).

15. Système d'authentification selon la revendication 14, caractérisé en ce que le code d'authentification (OTP_1) est généré (E30) par le

terminal (TRM) plus fréquemment que le code dynamique de sécurité ($DCCV_1$) n'est généré par ladite carte à microcircuit.

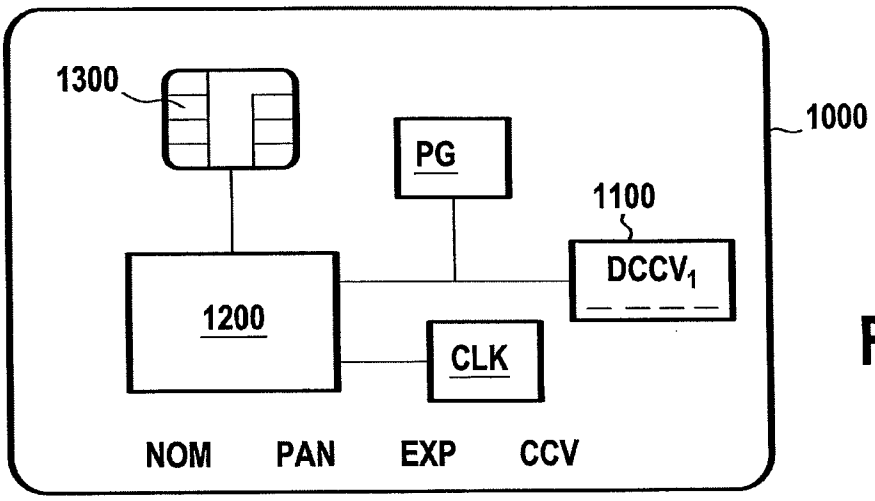
1300
PG
1000
1100
DCCV1
1200
CLK
NOM
PAN
EXP
CCV

FIG.1

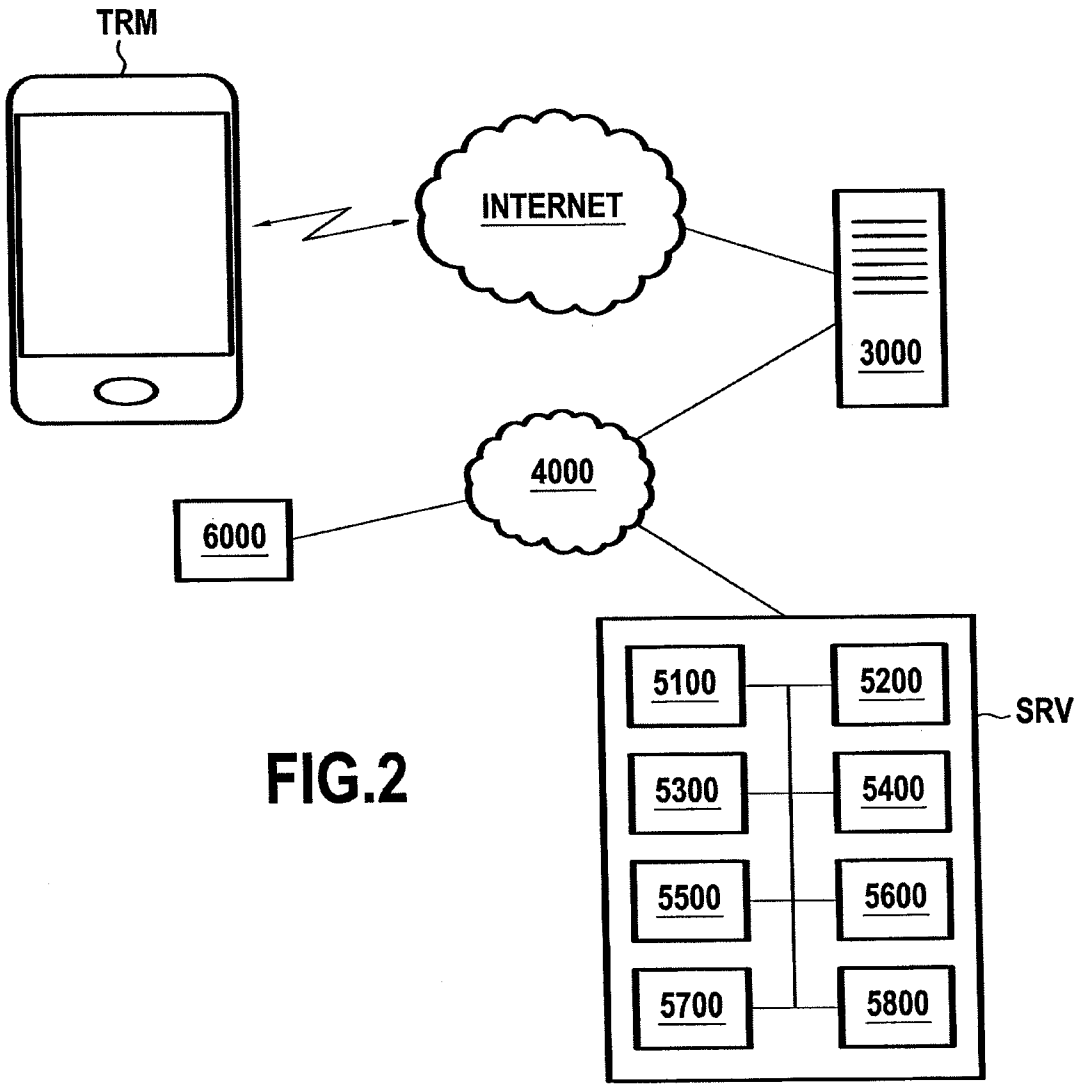
TRM
INTERNET
3000
4000
6000
5100
5200
SRV
5300
5400
5500
5600
5700
5800

FIG.2

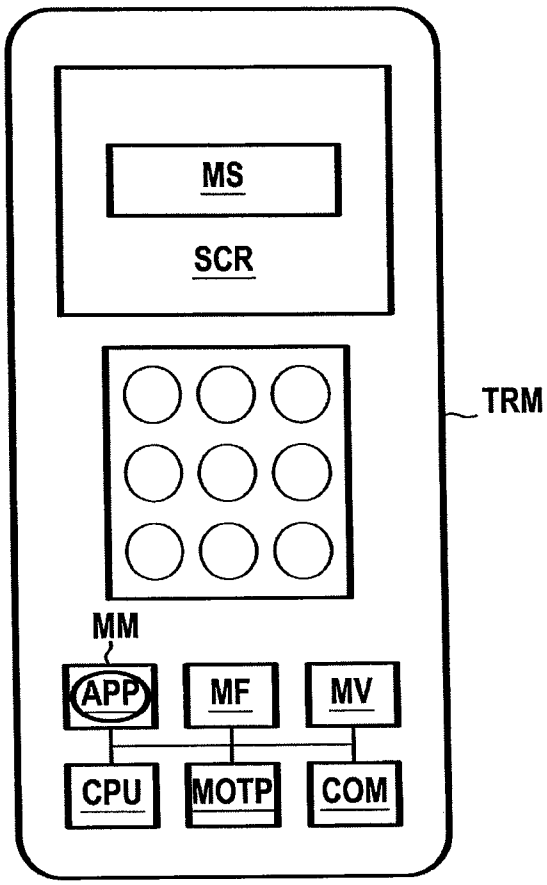

FIG.3

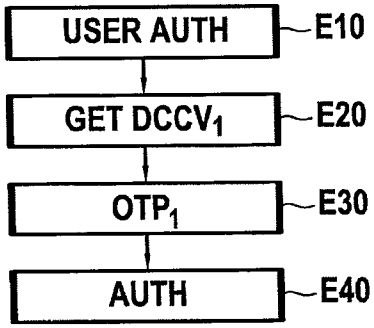

FIG.4

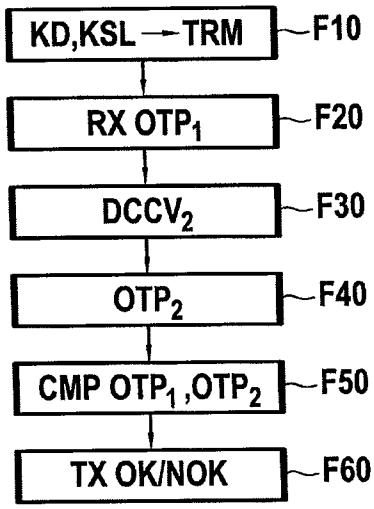

FIG.5

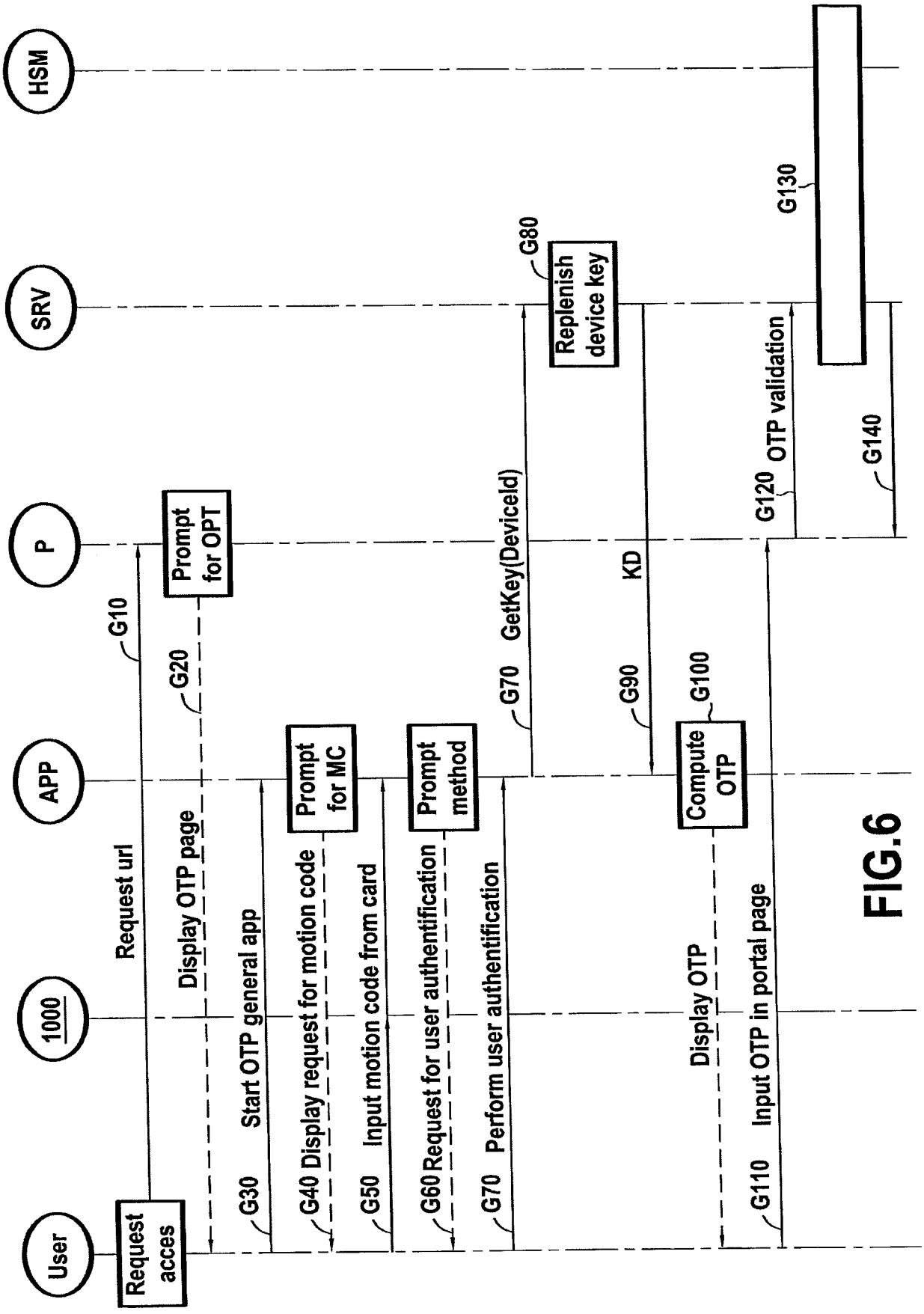
User
1000
APP
P
SRV
HSM
Request acces
Request url
G10
Display OTP page
G20
Prompt for OPT
Start OTP general app
G30
Display request for motion code
G40
Prompt for MC
Input motion code from card
G50
Request for user authentification
G60
Prompt method
Perform user authentification
G70
GetKey(DeviceId)
G70
Replenish device key
G80
KD
G90
Compute OTP
G100
Display OTP
Input OTP in portal page
G110
OTP validation
G120
G130
G140

FIG.6

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/050362

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
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)
G06F H04L H04W

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 2015/195280 A1 (TOYONAGA SABURO [JP] ET AL) 9 July 2015 (2015-07-09) paragraphs [0034] - [0048]; claim 1	1-15
A	EP 2 343 666 A1 (POLSKA WYTWORNIA PAPIEROW WARTOSCIOWYCH S A [PL]) 13 July 2011 (2011-07-13) paragraph [0003]	1-15

☐ 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
24 March 2017	31/03/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veen, Gerardus

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/050362

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015195280 A1	09-07-2015	EP 3092769 A1	16-11-2016
		JP 2015130633 A	16-07-2015
		US 2015195280 A1	09-07-2015
		WO 2015104765 A1	16-07-2015
EP 2343666 A1	13-07-2011	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/050362

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06
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)
G06F H04L H04W

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 2015/195280 A1 (TOYONAGA SABURO [JP] ET AL) 9 juillet 2015 (2015-07-09) alinéas [0034] - [0048]; revendication 1	1-15
A	EP 2 343 666 A1 (POLSKA WYTWORNIA PAPIEROW WARTOSCIOWYCH S A [PL]) 13 juillet 2011 (2011-07-13) alinéa [0003]	1-15

☐ 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
24 mars 2017	31/03/2017

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	Veen, Gerardus

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

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/050362

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2015195280 A1	09-07-2015	EP 3092769 A1	16-11-2016
		JP 2015130633 A	16-07-2015
		US 2015195280 A1	09-07-2015
		WO 2015104765 A1	16-07-2015
EP 2343666 A1	13-07-2011	AUCUN	