

①⑨ RÉPUBLIQUE FRANÇAISE
—
**INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE**
—
COURBEVOIE
—

①① N° de publication : **3 031 217**

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

②① N° d'enregistrement national : **14 63458**

⑤① Int Cl⁸ : **G 06 Q 20/40** (2017.01), G 06 F 21/60

①②

BREVET D'INVENTION

B1

⑤④ PROCÉDE DE VERIFICATION D'UNE REQUETE DE PAIEMENT COMPRENANT LA DETERMINATION DE LA LOCALISATION DU PROVISIONNEMENT D'UN JETON DE PAIEMENT.

②② Date de dépôt : 30.12.14.

③③ Priorité :

④③ Date de mise à la disposition du public
de la demande : 01.07.16 Bulletin 16/26.

④⑤ Date de la mise à disposition du public du
brevet d'invention : 09.02.18 Bulletin 18/06.

⑤⑥ Liste des documents cités dans le rapport de
recherche :

Se reporter à la fin du présent fascicule

⑥⑥ Références à d'autres documents nationaux
apparentés :

○ Demande(s) d'extension :

⑦① Demandeur(s) : *OBERTHUR TECHNOLOGIES
Société anonyme — FR et OBERTHUR
TECHNOLOGIES OF AMERICA CORP — US.*

⑦② Inventeur(s) : LASSOUAOUI ERIC et LIMOUSY
FRANCIS.

⑦③ Titulaire(s) : *OBERTHUR TECHNOLOGIES Société
anonyme, OBERTHUR TECHNOLOGIES OF
AMERICA CORP.*

⑦④ Mandataire(s) : SANTARELLI.

FR 3 031 217 - B1



5 Le domaine de l'invention concerne un procédé de vérification d'une requête de paiement, le procédé d'élaboration d'une requête de paiement et un terminal de paiement mobile.

10 Une entité bancaire propose à ses clients des instruments de paiement sécurisés garantissant la protection des transactions bancaires et des données bancaires. On peut citer parmi les instruments de paiement les cartes bancaires à puce électronique, les dispositifs de contrôles d'identité via les plates-formes web et les
15 numéros de carte bancaire virtuelle à usage restreint.

 Une nouvelle tendance est également l'intégration d'une carte de paiement virtuelle hébergée sur une application de paiement mobile d'un téléphone portable. Un souscripteur possède ainsi une version dématérialisée de
20 sa carte bancaire qu'il peut utiliser pour un paiement en champ proche au moyen de la technologie NFC (« Near Field Contact », en anglais). Ces architectures sont couramment appelées HCE (pour « Host Card Emulation » en anglais).

 Selon une architecture de paiement, l'entité
25 bancaire délivre une carte bancaire physique à son client mais aussi une application de paiement hébergeant une carte dématérialisée. Il est prévu de provisionner des jetons de paiement (couramment désignés par « Token Payment » en anglais) à usage restreint à destination d'un

terminal de paiement mobile sur lequel fonctionne l'application de paiement, le plus souvent le téléphone portable. L'utilisateur peut, via un moyen de communication en champs proche (par exemple NFC),
5 utiliser ce jeton de paiement avec un poste de paiement d'un marchand.

Le jeton de paiement est dérivé des données bancaires de la carte de paiement. La sécurité des véritables données bancaires est assurée car lors de la
10 transaction bancaire celles-ci ne sont pas exposées.

Par ailleurs, le jeton de paiement étant à usage restreint en durée de validité et nombre d'utilisation, même en cas de vol par fraude logiciel ou électronique l'exposition financière du client est réduite.

15 Il existe par ailleurs une mesure de vérification connue de l'état de la technique qui consiste à vérifier la localisation de l'utilisateur pour opérer une transaction de paiement. Par exemple, l'entité bancaire restreint une zone géographique d'utilisation de la carte
20 bancaire (physique ou virtuelle) et lorsqu'un paiement est réalisé en dehors de cette zone géographique la requête de paiement peut être refusée et une alerte levée.

On connaît dans l'état de la technique la demande de brevet américain US20140289116 et le brevet américain
25 US857731 décrivant des procédés de vérification consistant à collecter des données de localisation du dispositif GPS (« Global Positioning System » en anglais) du terminal mobile de l'utilisateur lors de la réalisation de la transaction bancaire et vérifier la correspondance avec la
30 localisation du poste de paiement du marchand.

Cependant, pour être efficaces ces méthodes nécessitent une phase de collecte des positions précises des postes de paiement des marchands pour pouvoir être comparées avec la position de l'utilisateur. Cette
5 collecte implique un protocole de relevé des informations de localisation de chaque commerçant et un système de maintenance coûteux.

Il existe donc un besoin de proposer un procédé de vérification géographique des requêtes de paiement moins
10 coûteux.

Par ailleurs, pour les solutions de paiement à base de jetons de paiement provisionnés dans le terminal mobile, il existe un risque de vol de données bancaires tant que celui-ci est provisionné dans le terminal mobile
15 et en attente d'une utilisation. Un fraudeur peut alors exploiter le jeton de paiement avec son propre terminal mobile et fournir sa position comme le ferait le véritable propriétaire de la carte bancaire. Dans ce cas-ci, le fraudeur passerait avec succès les mesures de vérification
20 précitées.

Il existe donc également un besoin d'améliorer la sécurité d'utilisation des jetons de paiement provisionnés dans le terminal mobile de l'utilisateur.

L'invention ci-après propose de résoudre les
25 problèmes précités.

Plus précisément, l'invention concerne un procédé de vérification d'une requête de paiement d'une transaction bancaire pour un serveur de vérification de transaction, la dite requête comprenant au moins un jeton

de paiement préalablement provisionné dans un terminal de paiement mobile d'un utilisateur.

Selon l'invention, le procédé comprend les étapes successives suivantes :

- 5 - l'acquisition d'une première localisation du terminal de paiement de l'utilisateur lors du provisionnement du jeton de paiement dans le terminal de paiement,
- 10 - la détermination d'une condition d'utilisation de la requête de paiement en fonction d'au moins la première localisation,
- la vérification de la condition d'utilisation en fonction d'un critère géographique,
- 15 - l'autorisation de la requête de paiement en fonction du résultat de la vérification.

20 Selon une variante, il comprend également l'acquisition d'une deuxième localisation du terminal de paiement lors de l'élaboration de la requête de paiement, et la condition d'utilisation est fonction de la première localisation et de la deuxième localisation.

Selon une variante, le critère géographique de vérification est une distance maximale autorisée.

25 De préférence, la première localisation et/ou la deuxième localisation sont chiffrées par une application de paiement du terminal de paiement mobile.

Avantageusement, la première localisation et/ou la deuxième localisation sont insérées dans un champ de données de la requête de paiement.

La requête de paiement est conforme à un protocole
5 de communication en champs proche de type ISO/IEC 14443.

De préférence, la première localisation est reçue par le serveur de vérification lors d'un protocole de provisionnement du jeton de paiement dans le terminal de paiement.

10 On notera que la première localisation est calculée par un moyen de localisation du terminal de paiement, par exemple un récepteur de signaux satellitaires.

Selon une variante, la condition d'utilisation est la première localisation et le critère géographique de
15 vérification est une localisation autorisée lors du provisionnement.

Selon une variante, le jeton de paiement est généré par un serveur de provisionnement et est transmis au terminal de paiement mobile via un réseau de téléphonie
20 cellulaire ou un réseau de communication internet.

Selon une variante, le jeton de paiement est généré par le terminal de paiement mobile.

L'invention prévoit également un procédé d'élaboration d'une requête de paiement comprenant un
25 jeton de paiement préalablement provisionné dans un terminal de paiement mobile pour le terminal de paiement mobile. Selon l'invention, le procédé comprend les étapes successives suivantes :

- la détermination d'une première localisation du terminal mobile lors du provisionnement du jeton de paiement,

5 - la transmission de la première localisation à un serveur de vérification pour la vérification de la requête de paiement.

De préférence, il comprend également la détermination d'une deuxième localisation du terminal mobile lors de l'élaboration de la requête de paiement
10 pour la vérification de la requête de paiement.

Dans cette dernière variante, l'élaboration de la requête de paiement comprend le chiffrement de la première localisation et/ou de la deuxième localisation.

L'invention prévoit également un terminal de paiement mobile d'un utilisateur comprenant un moyen pour
15 provisionner un jeton de paiement dans le terminal de paiement et pour l'élaboration d'une requête de paiement comprenant au moins le jeton de paiement.

Selon l'invention, il comprend également :

20 - un moyen de localisation du terminal mobile pour la détermination d'une première localisation lorsque le jeton de paiement est provisionné dans le terminal de paiement,

25 - et un moyen de transmission de la première localisation à un serveur de vérification de la requête de paiement, la première localisation étant transmise lors du provisionnement ou lors de l'élaboration de la requête de paiement.

Selon une variante, le moyen de localisation est apte à déterminer une deuxième localisation du terminal mobile lors de l'élaboration de la requête de paiement, et la requête de paiement comprend également la deuxième
5 localisation.

Selon une variante, le terminal de paiement est un téléphone cellulaire.

Grâce à l'invention, la méthode de vérification de la requête de paiement permet d'affiner les critères de
10 vérification géographique et de s'assurer que le jeton de paiement est utilisé en conformité avec ces critères géographiques fondés notamment en fonction de la localisation de provisionnement du jeton.

La vérification de la distance entre le lieu de
15 provisionnement et le lieu de la transaction de paiement est d'autant plus pertinente car le jeton est généralement utilisé peu de temps, voire immédiatement après son provisionnement.

De plus, l'invention permet d'attacher au jeton de
20 paiement des offres commerciales qui sont valides en fonction du lieu de délivrance du jeton de paiement.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description détaillée qui suit de modes de
25 réalisation de l'invention donnés à titre d'exemples nullement limitatifs et illustrés par les dessins annexés, dans lesquels :

- la figure 1 représente une architecture d'une solution de paiement au moyen de jetons de paiement à usage restreint,

5 - la figure 2 représente un terminal de paiement mobile d'un utilisateur et les applications logicielles de paiement permettant l'acquisition de la localisation de l'utilisateur lors du provisionnement du jeton de paiement,

10 - la figure 3 représente les étapes du procédé de vérification de la requête de paiement selon l'invention.

L'invention proposée consiste à mettre en place un procédé de vérification géographique amélioré pour assurer la sécurité des moyens de paiement d'un utilisateur. L'invention prévoit l'utilisation d'une architecture de paiement de type HCE à base de jetons de paiement à usage restreint dérivés d'un instrument de paiement. L'invention prévoit en particulier de vérifier la distance entre le lieu de provisionnement du jeton de paiement et le lieu d'utilisation du jeton de paiement.

20 La figure 1 représente l'architecture du système de paiement. Il prévoit une entité bancaire, une banque ou un service de paiement, pouvant émettre un instrument de paiement 17. L'instrument de paiement 17 pouvant comprendre plusieurs produits de paiement sous la forme
25 soit d'une carte bancaire, soit d'un service de paiement en ligne via un portail internet ou soit un service de paiement au moyen de jetons de paiement pouvant être provisionnés dans un terminal mobile 12 du souscripteur.

L'instrument de paiement 17 est défini :

- par des données bancaires du souscripteur, comme un numéro de compte attaché à l'instrument de paiement et des données personnelles,

5 - par des critères d'utilisation de l'instrument de paiement, notamment une période de validité, une zone géographique, un plafond de transaction,

10 - et par des données de sécurisation, comme par exemple le cryptogramme de sécurité ou des mécanismes de sécurité électroniques embarqués dans une carte de paiement permettant la vérification des données d'une transaction bancaire.

15 Dans le cas du terminal mobile 12 destiné à recevoir des jetons de paiement 103 (ou à les générer de façon embarquée), l'application de paiement 24 et les mécanismes de sécurité peuvent être hébergés dans un module sécurisé soudé dans le terminal, par exemple un circuit intégré sécurisé communément appelé eSE pour « Embedded Secure Element » en anglais ou un circuit intégré dédié aux communications de type NFC.

20 Dans une autre variante, l'application de paiement 24 et les mécanismes de sécurité peuvent être hébergés au niveau d'un environnement logiciel sécurisé (appelé TEE, pour « Trusted Execution Environment » en anglais). Il s'agit dans ce dernier cas d'une solution entièrement
25 logicielle dans laquelle la zone applicative de l'environnement d'exploitation du terminal mobile exécutant l'application de paiement est considérée comme étant de confiance grâce à divers mécanismes de sécurité. Ces mécanismes peuvent être la vérification de l'intégrité
30 de la zone mémoire, ou des protocoles d'authentification

avec un serveur distant d'authentification 10 pour l'installation d'applications ou de profils de paiement.

De préférence, Le terminal mobile 12 comprend des moyens de communication pour recevoir et émettre des données à distance via le réseau téléphonique cellulaire, un réseau de données de type IP via le réseau téléphonique ou un réseau de données de type IP via un réseau à moyenne portée, par exemple le WIFI.

Par ailleurs, pour l'opération du procédé de vérification des requêtes de paiement 104, le terminal mobile 12 comprend une application de paiement apte à élaborer des requêtes de paiement comprenant au moins le jeton de paiement 103.

Si la requête de paiement 104 est conforme aux normes EMV (« Europay Mastercard Visa », marques déposées), elle comprend notamment les données de la transaction bancaire (montant, devise), un cryptogramme de vérification de type ARQC, un compteur et des données d'application pour que le serveur de vérification puisse générer à son tour le cryptogramme de vérification.

Le terminal mobile comprend par ailleurs un dispositif de localisation géographique pour déterminer une première localisation 108 lors du provisionnement du jeton de paiement 103 dans le terminal mobile 12. La première localisation 108 est transmise au serveur de vérification 16 de l'entité bancaire. La première localisation est la position géographique du terminal mobile 12 lors du provisionnement.

La première localisation 108 est transmise via un premier canal de communication sécurisé au serveur de

vérification 16 via le serveur de provisionnement 11 lors du protocole de provisionnement. Cela permet de bénéficier de la sécurité de transmission du protocole de provisionnement. Le premier canal de communication peut
5 être le réseau cellulaire ou un réseau de communication internet.

En variante, la première location est transmise directement au serveur de vérification 16, notamment lorsque le serveur de vérification et le serveur de
10 provisionnement sont les mêmes structures physiques.

En variante, le provisionnement peut être la génération du jeton de paiement par le terminal mobile 12, sur requête du serveur de provisionnement, sur requête de l'utilisateur ou sur requête de l'application de paiement.
15 Le jeton de paiement est de préférence généré dans un circuit intégré sécurisé.

Dans une variante, le dispositif de localisation géographique peut déterminer une deuxième localisation 109 du terminal mobile 12 lors de l'exécution d'une
20 transaction bancaire. La deuxième localisation est la position géographique du terminal 12 lors de l'élaboration de la requête de paiement.

Plus précisément, la détermination de la deuxième localisation 109 est déclenchée par le protocole
25 d'élaboration de la requête de paiement 104. La deuxième localisation est transmise au serveur de vérification 16 via un deuxième canal de communication sécurisé lors du protocole de paiement. Le deuxième canal de communication sécurisé est un réseau de paiement 15 qui est décrit dans
30 la suite de la description. Il est prévu que la requête de

paiement 104 comprenne également la deuxième localisation 109.

Par ailleurs, il est prévu un serveur d'authentification 10 géré par l'institution bancaire 16
5 ou par un opérateur tiers de services d'authentification. Le serveur d'authentification 10 échange des moyens cryptographiques 102 avec le terminal mobile 12. Ces moyens cryptographiques 102 sont par exemple des clés cryptographiques de sessions, des numéros de transaction
10 temporaires ou des algorithmes de cryptographie permettant d'opérer un protocole d'échange sécurisé. Ces moyens cryptographiques sont échangés via un canal sécurisé pouvant être un protocole de communication HTTPS (« Hyper Text Transfert Protocol Secure » en anglais), CAT_TP
15 (« Card Application Toolkit Transport Protocol ») ou SMS (« Short Message Service »).

De plus, un serveur 11 de génération de jetons 103 dérivés de l'instrument de paiement 17 est également prévu. Le serveur 11 comprend des moyens cryptographiques
20 pour générer un jeton 103 à partir de données bancaires 105 attachées à l'instrument de paiement 17.

Un générateur de données aléatoires peut générer un jeton 103 à partir des données bancaires 105 et d'un moyen de diversification ou dérivation, par exemple un compteur.
25 D'autres moyens de diversification peuvent être mis en œuvre pour la génération du jeton 103 dans le serveur 11.

On notera qu'il est prévu que les données bancaires 105 exploitées par le générateur de données aléatoires peuvent être retrouvées par le serveur 11 de génération de
30 jetons ou par un serveur de vérification partenaire sur la

base des informations de la requête de paiement 104. Les données bancaires sont ainsi protégées et maintenues secrètes dans le du serveur 11.

Par ailleurs, le serveur 11 de génération de jeton
5 103 peut échanger des informations avec l'entité bancaire
16 via un réseau sécurisé de communication de données à
distance sans fil ou via un réseau de communication
filaire si le serveur d'authentification 11 est opéré par
l'entité bancaire 16. Ainsi, l'entité bancaire 16 peut
10 transmettre des données personnelles et bancaires d'un
souscripteur au serveur d'authentification 10 pour les
besoins des protocoles d'authentification entre le
terminal mobile 12 du souscripteur et le serveur
d'authentification.

15 De plus, le serveur 11 de génération de jeton peut
échanger des informations avec le serveur
d'authentification 10 via un réseau sécurisé de
communication de données à distance sans fil ou via un
réseau de communication filaire si les serveurs 10 et 11
20 sont en gestion par le même opérateur. Le serveur
d'authentification 10 échange des moyens cryptographiques
101 avec le serveur 11 de génération de jetons 103. Ces
moyens cryptographiques 101 sont par exemple des clés
cryptographiques de sessions, des numéros de transaction
25 temporaires ou des algorithmes de cryptographie permettant
d'opérer un protocole d'échange sécurisé avec le terminal
12.

Le protocole d'échange sécurisé avec le terminal 12
permet notamment d'échanger des jetons 103 via le premier
30 canal de communication sécurisé pouvant être un protocole
de communication HTTPS, CAT_TP ou SMS.

On notera par ailleurs que dans une variante du procédé de génération d'un jeton de paiement 103, celui-ci peut être généré par une fonction logicielle embarquée dans le terminal mobile 12. La fonction de dérivation et
5 génération du jeton de paiement est alors hébergée dans un circuit intégré sécurisé (de type eSE) soudé dans le terminal mobile 12. Il est alors possible de générer des jetons de paiement en mode hors-ligne, c'est à dire sans communication avec un serveur distant.

10 Un réseau sécurisé de paiement 15 peut être prévu pour transmettre les données bancaires des souscripteurs et les données de transactions bancaires respectant les spécifications des normes EMV, par exemple les données de transaction conventionnelles et les jetons de paiement
15 sécurisés. Le réseau sécurisé de paiement 15 est opéré par un opérateur de service de paiement 14 chargé d'opérer les transactions bancaires de paiement.

L'opérateur de service de paiement utilise le réseau sécurisé 15 pour transmettre les données de
20 transaction reçues des marchands 13, au moyen d'un poste de paiement ou un serveur distant de paiement. Le réseau 15 utilise un réseau de communication sans fil ou filaire sécurisé entre les postes de paiement.

La figure 2 décrit plus précisément le terminal 12.
25 Il comprend une application de paiement 24, hébergée par l'environnement d'exploitation du terminal mobile 12 ou dans un module sécurisé, par exemple eUICC (pour « Embedded Universal Integrated Circuit Card »).

Le terminal mobile 12 comprend des mémoires non
30 volatiles, de type ROM (« Read Only Memory » en anglais),

EEPROM (Electrically Erasable Read Only Memory ») ou FLASH pour l'enregistrement de paramètres et du code d'exécution d'applications et du programme informatique comprenant les instructions pour la mise en œuvre du procédé
5 d'élaboration de la requête de paiement 104, par exemple l'environnement d'exploitation du terminal, des applications ou des bibliothèques de fonctions spécifiques pouvant être utilisées par les applications.

Le terminal comprend notamment des bibliothèques de
10 fonctions, classes ou méthodes, dites API pour « Application Programming Interface » en anglais, pour les échanges avec le serveur 11 de génération de jetons, pour l'exécution de transactions de paiement avec un terminal de paiement 13 et pour l'authentification avec le serveur
15 d'authentification 10. L'application 24 peut faire appel aux fonctions fournies par les APIs.

Le terminal mobile comprend également une mémoire vive, de type RAM (« Random Access Memory » en anglais) pour l'enregistrement de paramètres temporaires, par
20 exemple des données de transaction bancaire ou une requête de paiement 104. La mémoire vive comprend des registres adaptés pour l'enregistrement des variables et paramètres créés lors de l'exécution du programme informatique comprenant les instructions pour la mise en oeuvre du
25 procédé d'élaboration de la requête de paiement 104 lors de son exécution.

Le terminal 12 comprend en plus des interfaces homme-machine pour la saisie et l'affichage de données avec le souscripteur, par exemple pour la saisie d'un code
30 personnel (code PIN en anglais, « Personal Identification Number ») et pour l'interaction avec l'application de

paiement 24. Il est prévu que l'application de paiement affiche des requêtes sur un écran du terminal mobile, par exemple une requête pour approcher le terminal 12 du poste de paiement 13, une requête de saisie d'un code personnel 5 ou une requête pour choisir un instrument de paiement.

Le terminal mobile comprend le processeur de calcul pour l'exécution des fonctions des applications du terminal mobile 12.

L'application de paiement 24 comprend un agent de 10 traitement 23 d'un jeton 103 dérivé d'un instrument de paiement 17 d'un souscripteur et un moyen réception de données 25 d'une transaction de paiement.

L'agent de traitement 23 est une fonction de 15 l'application de paiement 24 permettant le provisionnement du jeton 103 envoyé du serveur 11 de provisionnement de jetons et sa mémorisation dans une mémoire non volatile du terminal mobile. L'agent de traitement 23 est un applicatif logiciel exploitant les fonctions logicielles APIs permettant d'interagir avec le serveur 11 de 20 génération du jeton 103.

Selon la variante de génération embarquée dans le terminal mobile 12, l'agent de traitement 23 est une fonction de l'application de paiement 24 permettant la génération du jeton de paiement 103.

25 Par ailleurs, l'application de paiement 24 héberge un ou plusieurs instruments de paiement 17. Une carte virtuelle de paiement est enregistrée sous la forme d'une application spécifique au profil de la carte de paiement et peut être mémorisée au moyen d'un identifiant 30 d'application. L'instrument de paiement est enregistré

dans l'application de paiement préalablement au premier provisionnement d'un jeton paiement.

Le moyen de réception 25 de données de transaction bancaire est une fonction de l'application de paiement 24 permettant la communication avec le terminal de paiement 5 13. La fonction de réception est capable de piloter un protocole d'échange sans contact selon la norme ISO/IEC 14443, d'enregistrer les données de la transaction dans une mémoire et de retourner des réponses au terminal de 10 paiement 13.

En outre, l'application de paiement 24 comporte des moyens cryptographiques 26 pour certifier des données de la requête de paiement 104, par exemple une clé privée pour la signature de données transmises avec la requête de 15 paiement 104, ou pour certifier des données transmises au serveur de provisionnement 11 ou au serveur de vérification 16.

En particulier, l'invention peut prévoir la signature de la première localisation 108 avant sa 20 transmission au serveur de vérification 16. Ceci permet de garantir que la première localisation 108 est émise par l'utilisateur. La signature peut être conditionnée à la saisie d'un mot de passe ou code personnel.

En outre, le terminal 12 comprend un moyen de 25 localisation 27 du terminal mobile 12 pour la détermination de la première localisation 108 lorsque le jeton de paiement 103 est provisionné dans le terminal de paiement 12.

De préférence, le moyen de localisation 27 détermine également la deuxième localisation 109 lorsque la requête de paiement 104 est élaborée.

Le moyen de localisation 27 est de préférence un
5 récepteur de signaux satellitaires provenant d'un système de géolocalisation 200 comprenant une constellation de satellites. L'utilisation des signaux satellitaires offre une précision de l'ordre de quelques mètres. Les première et deuxième localisations 108, 109 sont des coordonnées en
10 latitudes et longitudes correspondant au positionnement terrestre.

Dans une autre variante, la localisation peut être déterminée à partir des données de réseaux de communication sans fil, par exemple le réseau cellulaire
15 ou un réseau WIFI. La précision est de l'ordre de plusieurs centaines de mètres. En particulier, Il peut être prévu pour la détermination de la première localisation que le terminal de paiement mobile 12 transmette des données de réseau au serveur de
20 vérification pour sa localisation.

Il est prévu que l'application de paiement transmette au serveur de vérification 16 (directement ou via le serveur de provisionnement 11) la première localisation 108. La première localisation est de
25 préférence transmise au serveur de vérification 16 via le serveur de provisionnement 11 lors du protocole de provisionnement du jeton 103.

En variante, la première localisation 108 est transmise avec la requête de paiement 104 comprenant le
30 jeton de paiement 103 via le réseau de paiement 15. Pour

assurer la sécurité de la première localisation, celle-ci est alors chiffrée grâce au moyens cryptographiques 26, par exemple par une signature.

La deuxième location 109 est transmise avec la
5 requête de paiement 104, chiffrée identiquement à la première localisation 108.

Le moyen de traitement 23 du jeton de paiement 103 élabore la requête de paiement 104. Celle-ci comprenant au moins le jeton de paiement 103 (de préférence signé par
10 l'utilisateur pour assurer qu'il est utilisé par le souscripteur de l'instrument de paiement), les données de la transaction bancaire reçues du poste de paiement du marchand et des cryptogrammes de vérification.

On notera que la requête de paiement peut
15 comprendre également la première localisation 108 et/ou la deuxième localisation 109, selon le mode de vérification prévu.

La figure 3 représente un mode de réalisation du procédé de vérification d'une requête de paiement 104
20 exécuté par le serveur de vérification 16 et le procédé d'élaboration de la requête de paiement 104 correspondante exécuté par le terminal mobile 12.

Le procédé d'élaboration de la requête de paiement 104 comprenant au moins le jeton de paiement 103
25 préalablement provisionné dans le terminal mobile 12 comprend les étapes successives suivantes :

- la détermination 301 de la première localisation 108 du terminal mobile 12 lors du provisionnement du jeton de paiement 103 dans le terminal mobile,

- la transmission 302 de la première localisation 108 au serveur de vérification 16 pour une vérification ultérieure de la requête de paiement 104 comprenant le jeton de paiement 103.

5 La première localisation 108 correspond au lieu du provisionnement du jeton de paiement (par exemple le domicile du souscripteur, lieu d'un commerce etc..). Le provisionnement est déclenché sur requête de l'utilisateur ou de l'entité bancaire.

10 Dans cette variante, la première localisation 108 est transmise via le serveur de provisionnement 11 lors du provisionnement du jeton. La transmission bénéficie ainsi de la sécurité du protocole de provisionnement quand le jeton de paiement 103 est reçu du serveur de provisionnement 11. La première localisation 108 est de préférence transmise avant la réalisation de la transaction bancaire utilisant le jeton de paiement 103.

20 Dans une autre variante, quand le terminal mobile 12 comprend un circuit intégré sécurisé exécutant des fonctions de génération du jeton de paiement 103, le provisionnement correspond à une étape de génération du jeton 103 par le terminal mobile 12. La génération du jeton peut être déclenchée suite à une requête issue du serveur de provisionnement 11 ou suite à une requête de l'utilisateur. La première localisation 108 est transmise via un protocole d'échange sécurisé (HTTPS ou CAT_TP par exemple) au serveur de vérification 16, via le serveur de provisionnement 11 ou non.

30 Ensuite, lorsqu'une transaction bancaire est déclenchée, notamment lors d'un échange NFC, le procédé

d'élaboration de la requête de paiement comprend la création 303 de la requête de paiement 104. Lors de la création 303, des cryptogrammes de vérification sont notamment générés à partir des données de la transaction
5 reçues du poste de paiement du marchand (non représenté sur la figure 3).

La requête de paiement 104 est conforme à un protocole de communication en champs proche de type ISO/IEC 14443. La requête de paiement 104 est transmise au
10 serveur de vérification 16 conformément au protocole de paiement prévu.

De plus, dans la variante préférée, le procédé d'élaboration de la requête de paiement comprend la détermination 304 de la deuxième localisation 109. Celle-
15 ci est alors transmise avec la requête de paiement 104 au serveur de vérification 16. La deuxième localisation 109 est de préférence déterminée par des données de géolocalisation satellitaires et signée par l'application de paiement.

20 De préférence, la deuxième localisation est insérée dans un champ de données de la requête de paiement 104 normalisé dans les protocoles de transaction EMV, par exemple le champ « Track 2 discretionary Data » ou tout champ de données libre.

25 Dans une autre variante, la deuxième localisation est déterminée à partir de données de localisation du poste de paiement du marchand.

Le serveur de vérification 16 exécute le procédé de vérification de la requête de paiement 104. Il comprend
30 l'acquisition 401 de la première localisation 108 du

terminal de paiement 12 de l'utilisateur lors du provisionnement du jeton de paiement 103 dans le terminal de paiement. La première localisation 108 est acquise via le serveur de provisionnement 11 ou directement du terminal mobile 12.

Le procédé comprend l'acquisition 402 de la deuxième localisation 109 du terminal de paiement 12 lors de l'élaboration de la requête de paiement 104. La deuxième localisation 109 est reçue avec la requête de paiement 104. La requête de paiement est reçue via le réseau de paiement 15. Il est prévu que la requête de paiement ait été préalablement vérifiée par le serveur de provisionnement pour déterminer l'identité bancaire 105 du souscripteur attachée au jeton de paiement.

Le procédé comprend ensuite la détermination 403 d'une condition d'utilisation de la requête de paiement 104 en fonction de la première localisation 108 et de la deuxième localisation 109. La condition d'utilisation est déterminée par un traitement des données de localisation reçues par le serveur de vérification 16. La condition d'utilisation est le calcul de la distance entre la première localisation 108 et la deuxième localisation 109.

Le procédé de vérification comprend ensuite la vérification 404 de la condition d'utilisation avec un critère géographique. La vérification comprend des règles de risque dont les critères géographiques sont élaborés par l'entité bancaire émettrice de l'instrument de paiement 17. Le critère géographique de vérification est une distance maximale autorisée. La distance maximale autorisée peut être de plusieurs centaines de kilomètres.

Par exemple, si la distance entre la première localisation 108 et la deuxième localisation 109 est supérieure à 200km, la vérification peut refuser la requête de paiement.

5 En variante, le critère géographique peut être une correspondance entre la première localisation et la deuxième localisation. Par exemple, le critère géographique peut être une correspondance entre un pays lors du provisionnement et un pays lors de l'élaboration
10 de la requête de paiement. Une première règle de correspondance peut être que le pays lors du provisionnement est identique au pays lors de l'élaboration de la requête de paiement. Une deuxième règle de correspondance peut être que le pays lors de
15 l'élaboration de la requête de paiement est un pays limitrophe de celui lors du provisionnement.

Le procédé de vérification comprend finalement l'autorisation 405 de la requête de paiement 104 en fonction du résultat de la vérification 404 au regard du
20 critère géographique. L'autorisation est transmise au poste de paiement 13 du marchand.

On notera que le protocole de vérification comprend également la vérification de cryptogrammes de vérification (par exemple ARQC).

25 Dans une variante du procédé de vérification, la condition d'utilisation est la première localisation uniquement et le critère géographique de vérification est une localisation autorisée lors du provisionnement. En particulier, une vérification peut être opérée uniquement
30 sur la première localisation. La transaction bancaire est

alors refusée si le jeton de paiement a été provisionné dans une zone géographique non habilitée par l'entité bancaire, par exemple un pays étranger non déclaré par l'utilisateur. Ceci permet notamment de détecter une
5 fraude sur le protocole de provisionnement.

Dans cette dernière variante, la première localisation 108 est transmise avec la requête de paiement 104. Elle est enregistrée dans le terminal mobile entre l'instant de provisionnement et celui de la transaction
10 bancaire avec un poste de paiement du marchand.

Il est prévu que le procédé de vérification contrôle les première et deuxième localisations 108, 109 lorsque celles-ci sont chiffrées. Par exemple, le procédé comprend la vérification d'une signature ou un
15 déchiffrement. Le procédé de vérification contrôle si les localisations ont été émises par l'utilisateur.

REVENDICATIONS

1. Procédé de vérification d'une requête de paiement
5 (104) d'une transaction bancaire pour un serveur (16) de
vérification de transaction, la dite requête (104) comprenant
au moins un jeton de paiement (103) préalablement provisionné
dans un terminal de paiement mobile d'un utilisateur,
caractérisé en ce qu'il comprend les étapes successives
10 suivantes :

- l'acquisition (401) d'une première localisation (108)
du terminal de paiement de l'utilisateur (12) lors du
provisionnement du jeton de paiement (103) dans le terminal de
paiement, la première localisation (108) étant chiffrée par
15 une application de paiement (24) du terminal mobile de
paiement,

- la détermination (403) d'une condition d'utilisation
de la requête de paiement (104) en fonction d'au moins la
première localisation (108),

20 - la vérification (404) de la condition d'utilisation
en fonction d'un critère géographique,

- l'autorisation (405) de la requête de paiement (104)
en fonction du résultat de la vérification.

2. Procédé selon la revendication 1, caractérisé en ce
25 qu'il comprend également l'acquisition (402) d'une deuxième
localisation du terminal de paiement (12) lors de
l'élaboration de la requête de paiement (104), et en ce que la
condition d'utilisation est fonction de la première
localisation (108) et de la deuxième localisation (109).

3. Procédé selon la revendication 2, caractérisé en ce que le critère géographique de vérification est une distance maximale autorisée.

5 4. Procédé selon la revendication 2 ou 3, caractérisé en ce que la deuxième localisation (109) est chiffrée par l'application de paiement du terminal de paiement mobile.

10 5. Procédé selon l'une quelconque des revendications 2 à 4, caractérisé en ce que la première localisation (108) et/ou la deuxième localisation (109) sont insérées dans un champ de données de la requête de paiement (104).

15 6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que la première localisation (108) est calculée par un moyen de localisation (27) du terminal de paiement (12), par exemple un récepteur de signaux satellitaires.

7. Procédé selon la revendication 1, caractérisé en ce que la condition d'utilisation est la première localisation et le critère géographique de vérification est une localisation autorisée lors du provisionnement.

20 8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le jeton de paiement (103) est généré par un serveur de provisionnement (11) et est transmis au terminal de paiement mobile (12) via un réseau de téléphonie cellulaire ou un réseau de communication internet.

25 9. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le jeton de paiement (103) est généré par le terminal de paiement mobile (12).

30 10. Procédé d'élaboration d'une requête de paiement (104) comprenant un jeton de paiement (103) préalablement provisionné dans un terminal de paiement mobile (12) pour le

terminal de paiement mobile (12), caractérisé en ce qu'il comprend les étapes successives suivantes :

5 - la détermination (301) d'une première localisation (108) du terminal mobile (12) lors du provisionnement du jeton de paiement (103),

- le chiffrement de la première localisation (108) par l'application de paiement (24),

10 - la transmission de la première localisation (108) avec la requête de paiement (104) comprenant le jeton de paiement (103) à un serveur de vérification (16) pour la vérification de la requête de paiement (104).

11. Procédé selon la revendication 10, caractérisé en ce qu'il comprend également la détermination (304) d'une deuxième localisation (109) du terminal mobile (12) lors de l'élaboration de la requête de paiement (104) pour la
15 vérification de la requête de paiement (104).

12. Procédé selon la revendication 11, caractérisé en ce que l'élaboration de la requête de paiement (104) comprend le chiffrement de la deuxième localisation (109).

20 13. Procédé selon l'une quelconque des revendications 10 à 12, caractérisé en ce que la création (303) de la requête de paiement (104) est configurée de sorte que la requête de paiement soit conforme à un protocole de communication en champs proche de type ISO/IEC 14443.

25 14. Terminal de paiement mobile (12) d'un utilisateur comprenant un moyen pour provisionner (23) un jeton de paiement (103) dans le terminal de paiement (12) et pour l'élaboration d'une requête de paiement (104) comprenant au moins le jeton de paiement (103), caractérisé en ce qu'il
30 comprend également :

- un moyen de localisation (27) du terminal mobile (12) pour la détermination d'une première localisation (108) lorsque le jeton de paiement (103) est provisionné dans le terminal de paiement (12),

5 - des moyens cryptographiques (26) de l'application de paiement (24) pour certifier des données de la requête de paiement (104), la première localisation (108) étant chiffrée par les moyens cryptographiques (26),

10 - et un moyen de transmission de la première localisation (108) à un serveur de vérification de la requête de paiement, la première localisation (108) étant transmise avec la requête de paiement (104).

15 15. Terminal selon la revendication 14, caractérisé en ce que le moyen de localisation (27) est apte à déterminer une deuxième localisation (109) du terminal mobile (12) lors de l'élaboration de la requête de paiement (104), et en ce que la requête de paiement (104) comprend également la deuxième localisation (109).

20 16. Terminal selon la revendication 14 ou 15, caractérisé en ce qu'il est un téléphone cellulaire.

1/3

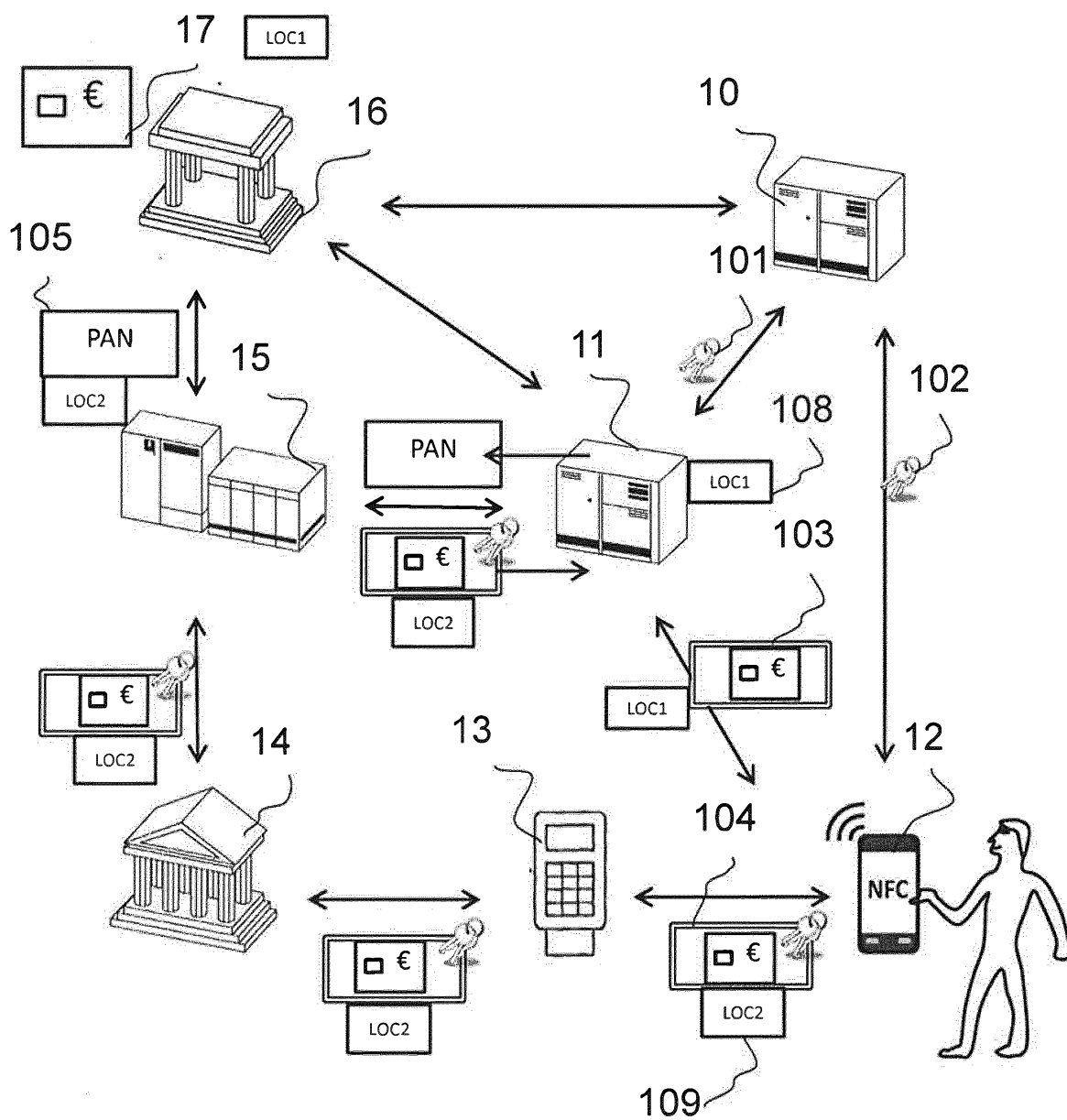


Fig. 1

2/3

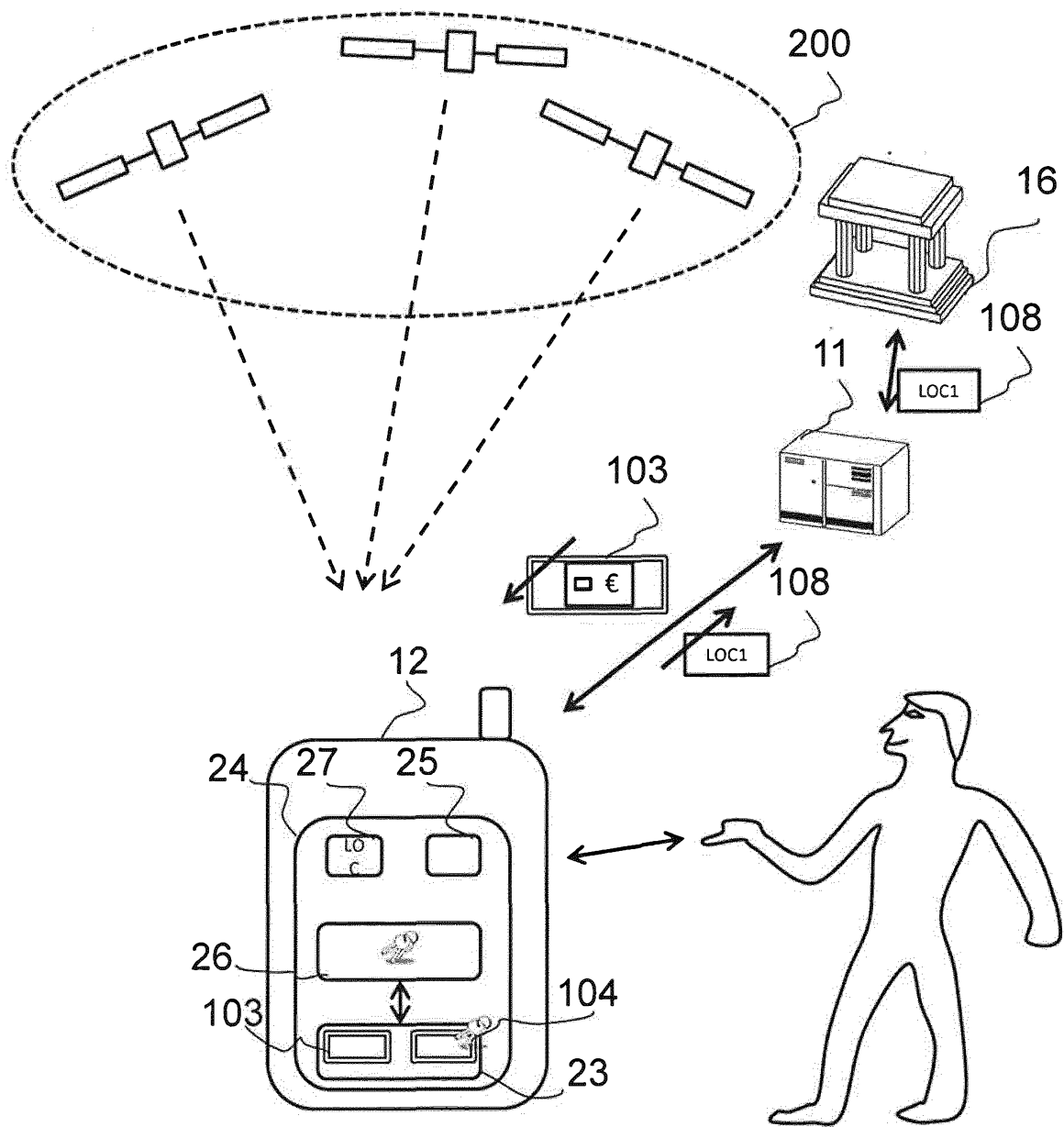


Fig. 2

3/3

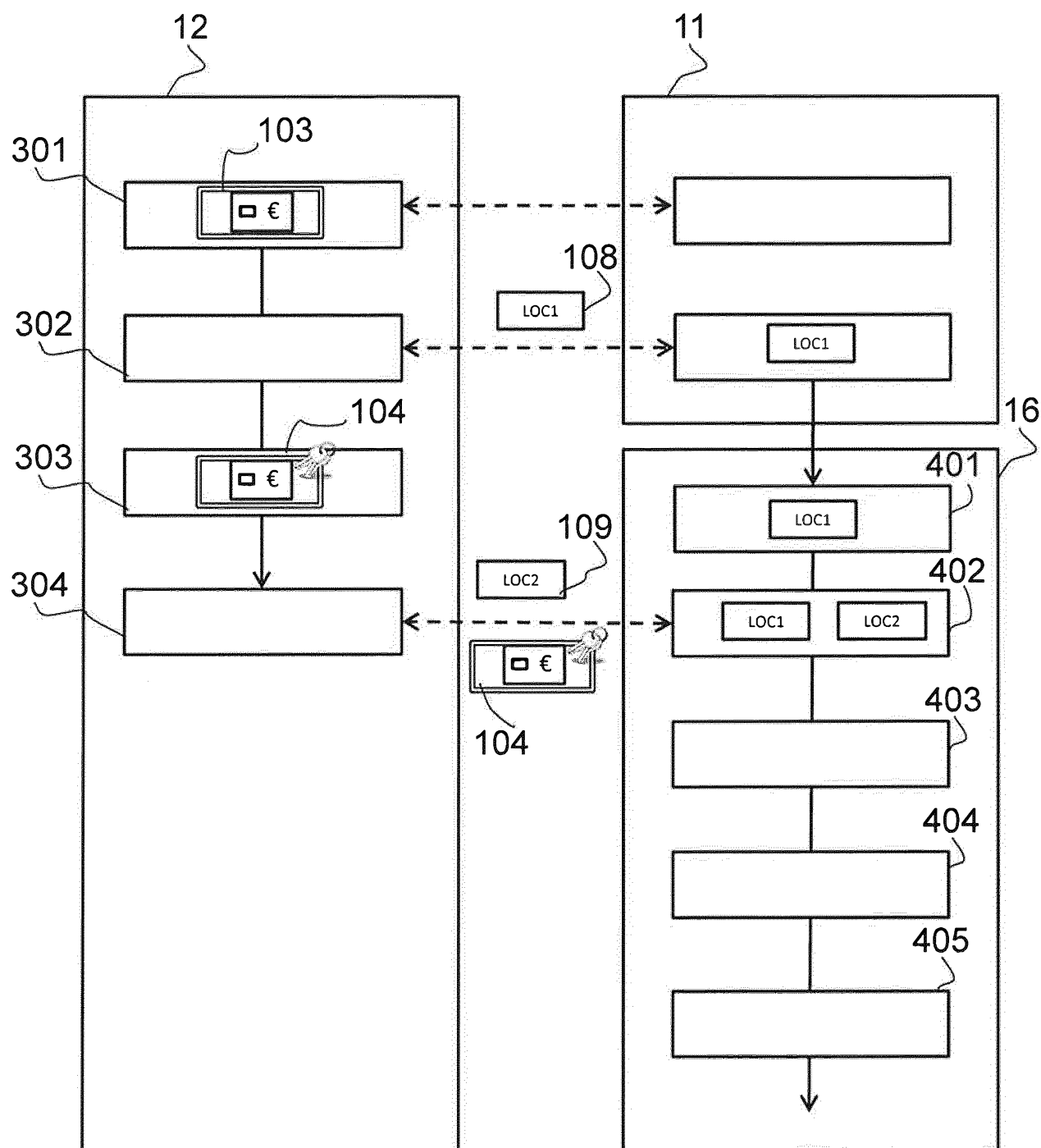


Fig. 3

RAPPORT DE RECHERCHE

articles L.612-14, L.612-17 et R.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveau) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ÉTABLISSEMENT DU PRÉSENT RAPPORT DE RECHERCHE

- Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.
- Le demandeur a maintenu les revendications.
- Le demandeur a modifié les revendications.
- Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.
- Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.
- Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITÉS DANS LE PRÉSENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

- Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.
- Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.
- Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.
- Aucun document n'a été cité en cours de procédure.

**1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN
CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION**

US 2014/040139 A1 (BRUDNICKI DAVID [US] ET AL)
6 février 2014 (2014-02-06)

**2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN
TECHNOLOGIQUE GENERAL**

NEANT

**3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND
DE LA VALIDITE DES PRIORITES**

NEANT