(19) LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

(11) N° de publication : **LU100841**

(12) **BREVET D'INVENTION** **B1**

(21) N° de dépôt: LU100841

(51) Int. Cl.:
G06Q 20/34

(22) Date de dépôt: 15/06/2018

(30) Priorité:

(43) Date de mise à disposition du public: 30/12/2019

(47) Date de délivrance: 30/12/2019

(73) Titulaire(s):
FLESCHEN Marc – 1147 Luxembourg (Luxembourg)

(72) Inventeur(s):
MAYER Cédric – 77176 Savigny-le-Temple (France),
FLESCHEN Marc – 1147 Luxembourg (Luxembourg)

(74) Mandataire(s):
OFFICE FREYLINGER S.A. –
8001 STRASSEN (Luxembourg)

(54) **Dispostifs et procédé sécurisés de paiement.**

(57) L'invention concerne un procédé sécurisé de paiement électronique, ainsi que des dispositifs correspondants, notamment une carte de paiement et un terminal de paiement électronique.

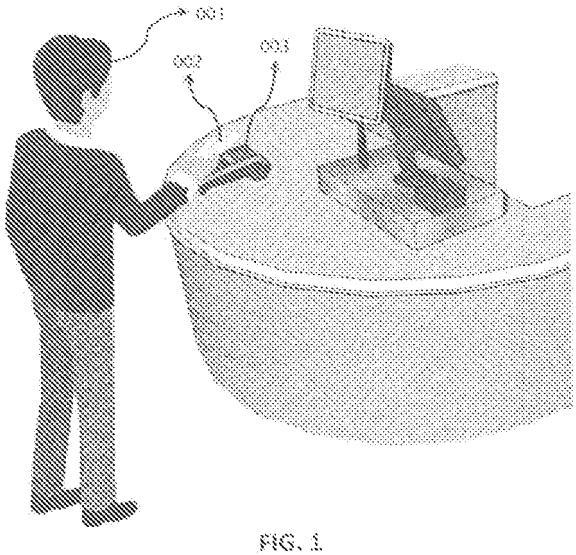

FIG. 1

DISPOSITIFS ET PROCÉDÉ SÉCURISÉS DE PAIEMENT

Domaine technique

[0001] La présente invention concerne un procédé sécurisé de paiement électronique, ainsi que des dispositifs correspondants, notamment une carte de paiement et un terminal de paiement électronique.

Etat de la technique

[0002] Les cartes à puce utilisant une transaction dynamique avec l'interface EuroPay-Mastercard-Visa ("EMV") sont les cartes à puce les plus populaires. Et cette norme bancaire concerne également le terminal de paiement électronique (TPE) qui adopte la même norme EMV. Depuis ces dernières années, avec les nouvelles technologies de la communication, en particulier avec Near Field Communication (NFC), les transactions de paiement sans contact apparaissent sur le marché pour opérer des transactions de paiement plus rapidement. Ainsi, la carte à puce sans fil et TPE compatibles, avec les transactions sans contact, en accord avec le protocole EMV et la norme ISO14443, augmentent rapidement leur part de marché.

[0003] Parallèlement, les TPE ont suivi les dernières innovations dans le domaine du paiement sans contact. D'abord en raison de l'apparition du NFC à l'intérieur des cartes de paiement, comme les cartes VISA ou Master et dans la deuxième partie en raison de l'utilisation du smartphone pour payer certaines transactions. Ainsi, les TPE se devaient d'intégrer directement ou via un accessoire certaines technologies radiofréquences telles que NFC, WiFi ou Bluetooth pour être compatibles avec la dernière évolution de carte de crédit ou de débit et des smartphones.

[0004] En raison de la possibilité de faire une transaction à quelques centimètres de cette carte à puce, certains périphériques de piratage peuvent pirater ce signal de 13,56 MHz pour collecter de l'argent avec un montant autorisé, mais plusieurs fois en très peu de temps, ce qui rend les cartes à puce NFC vulnérables.

[0005] Avec toutes ces technologies pour sécuriser les transactions de paiement, le point important pour assurer une bonne transaction et est de s'assurer que l'autorisation est opérée avec la bonne personne. Dans ce but, différentes inventions récentes de cartes à puce ont été mises en œuvre différentes alternatives comme l'empreinte digitale sur carte à puce pour assurer l'identification du bon utilisateur. Mais même, dans ce cas, une communication RF entièrement duplex se produit et nous ne sommes pas totalement sûrs contre le piratage du signal RF.

[0006] Dans le même contexte d'autres inventions ont décrit l'utilisation de l'affichage numérique pour générer un code PIN de sécurité à l'arrière de la carte à puce. Il est particulièrement intéressant si la carte à puce est volée et que la carte à puce doit être utilisée pour une transaction électronique, au cours de laquelle le code de sécurité est demandé.

Objet de l'invention

[0007] Un objet de la présente invention est par conséquent de proposer des dispositifs et un procédé permettant de sécuriser davantage et de préférence faciliter les transactions au niveau des points de vente (POS, point of sale). Il serait en outre souhaitable que du moins certaines des solutions proposées puissent être implémentées sans requérir le remplacement des dispositifs existants.

Description générale de l'invention

[0008] Afin de résoudre le problème mentionné ci-dessus, la présente invention propose, dans un premier aspect, une carte de paiement de crédit ou de débit (encore appelée OSC ci-après), comprenant une face avant comportant des caractéristiques courantes, par exemple le numéro de la carte de paiement, le nom du titulaire, un logo, la date d'expiration et/ou une puce électronique, et une face arrière comportant des caractéristiques courantes, par exemple une bande magnétique, un panneau de signature, un hologramme et/ou un code de sécurité de la carte. La carte de paiement comprend en outre les composants électriques suivants : une batterie ; un module électronique de contrôle comprenant un microcontrôleur et une mémoire de stockage ; et au moins une photocellule ou photodiode et au moins une LED comme émetteur/récepteur OLC, de préférence

VLC/LiFi et/ou IRDA, orientés de préférence vers la face arrière de la carte de paiement et un interrupteur de mise sous tension des composants électriques, de préférence un interrupteur sensitif. Le module électronique de contrôle est configuré pour contrôler la ou les photocellule(s) ou photodiode(s) et LED suivant un protocole de communication OLC, de préférence un protocole de communication VLC/LiFi et/ou IRDA.

[0009] La carte de paiement comprend en outre de préférence un émetteur/récepteur NFC et/ou une puce RFID, contrôlable(s) par le module électronique de contrôle.

[0010] Dans une des variantes, la carte de paiement selon l'invention, comprend en outre un dispositif électromagnétique à induction et/ou une ou plusieurs photodiodes organiques, de préférence de type polymère photovoltaïque, couvrant de manière particulièrement préférée partiellement ou totalement la face avant et/ou arrière de la carte de paiement, pour charger la batterie.

[0011] Avantageusement, la carte de paiement comprend également un capteur d'empreinte digitale contrôlable par le module électronique de contrôle, le capteur d'empreinte digitale étant de préférence associé à l'interrupteur.

[0012] La carte de paiement peut également comprendre, par exemple sur la face arrière un affichage, de préférence un affichage numérique ou un écran e-ink, notamment pour afficher le code de sécurité de la carte.

[0013] Le module électronique de contrôle de la carte de paiement comprend de préférence en outre un module de communication WiFi et/ou Bluetooth pour augmenter son universalité et/ou pour augmenter la sécurité par distribution du flux de données sur plusieurs types de communication.

[0014] Un deuxième aspect de l'invention concerne un terminal de paiement électronique comprenant au moins une photocellule ou photodiode et au moins une LED comme émetteur/récepteur OLC, de préférence VLC/LiFi et/ou IRDA, adapté pour l'émission et la réception d'un flux de données conformément à un protocole de communication OLC, de préférence un protocole de communication VLC/LiFi et/ou IRDA, notamment des données d'identification d'un utilisateur, des données de coordonnées bancaires et/ou des données de transaction de paiement à effectuer ; un processeur pour convertir et/ou gérer le flux de

données ; des moyens de stockage adaptés pour stocker du moins temporairement le flux de données reçues du réseau de données ; des moyens de connexion à un réseau de données, de préférence à un serveur distant configuré pour corroborer et le cas échéant confirmer les données d'identification de l'utilisateur, les données de coordonnées bancaires et les données concernant la transaction de paiement à effectuer.

[0015] De préférence, le terminal de paiement électronique comprend en outre un émetteur/récepteur NFC adapté pour l'émission et la réception d'un flux de données conformément à un protocole de communication NFC, notamment des données d'identification d'un utilisateur, des données de coordonnées bancaires et/ou des données de transaction de paiement à effectuer.

[0016] Le processeur du terminal de paiement électronique est de manière préférée configuré pour déterminer le protocole de communication à utiliser en fonction d'informations d'intensité lumineuse ambiante et/ou de présence ou d'absence de réception d'un signal OLC, de préférence VLC/LiFi et/ou IRDA, et/ou NFC et/ou après négociation avec un smartphone et/ou une carte de paiement requérant l'entrée en communication, de préférence une carte de paiement selon la présente invention.

[0017] Dans certaines variantes du terminal de paiement électronique selon l'invention, son processeur est configuré pour émettre et recevoir le flux de données en utilisant un des émetteurs/récepteurs OLC, de préférence VLC/LiFi et/ou IRDA, ou NFC pour l'émission et un autre de ces émetteurs/récepteurs OLC ou NFC pour la réception.

[0018] Dans d'autres variantes du terminal de paiement électronique selon l'invention, son processeur est configuré pour émettre et recevoir le flux de données en le découpant et en le distribuant entre le ou les émetteur(s)/récepteur(s) OLC, VLC/LiFi ou IRDA, et l'émetteur/récepteur NFC selon un algorithme de sécurisation.

[0019] Selon la configuration du terminal de paiement électronique, en l'occurrence pour des nouveaux terminaux, l'émetteur/récepteur OLC, de préférence VLC/LiFi et/ou IRDA, et optionnellement un émetteur/récepteur NFC, est/sont directement intégré(s) dans le boitier du terminal de paiement

électronique. Dans le cas de terminaux existants conventionnels, l'émetteur/récepteur OLC, de préférence VLC/LiFi et/ou IRDA, et optionnellement un émetteur/récepteur NFC, est/sont disposé(s) dans un boitier séparé relié au terminal de paiement électronique par une connexion filaire, notamment USB ou Ethernet.

[0020] Un troisième aspect décrit un procédé de paiement électronique sécurisé par un terminal de paiement électronique selon l'invention au moyen d'une communication sans fil avec une carte de paiement, de préférence une carte de paiement selon l'invention, le procédé comprenant les étapes :

(a) déclenché par une transaction de paiement à effectuer, le terminal de paiement électronique envoie une requête de connexion par l'émetteur OLC, de préférence VLC/LiFi et/ou IRDA,

(b) (b1) le smartphone a un émetteur/récepteur IRDA, reçoit la requête et envoi une confirmation de connexion au terminal de paiement électronique d'utiliser la technologie IRDA ; ou

(b2) la carte de paiement a un émetteur/récepteur VLC/LiFi, reçoit la requête et envoi une confirmation de connexion au terminal de paiement électronique d'utiliser la technologie VLC/LiFi ; ou

(b3) la carte de paiement n'a pas d'émetteur/récepteur OLC, ce dernier n'est pas activé ou n'est pas placé de manière appropriée devant l'émetteur du terminal de paiement électronique, la carte de paiement ne répond pas endéans un lapse de temps déterminé et le terminal de paiement électronique renvoie sa requête de connexion par un émetteur/récepteur NFC, lorsque la carte de paiement reçoit une telle requête de connexion par NFC, il envoie la confirmation de connexion au terminal de paiement électronique d'utiliser la technologie NFC,

(b4) en cas de non-réponse à chacune des requêtes de connexion, la transaction est soit présenté par le terminal de paiement électronique pour paiement électronique avec carte de crédit ou débit, soit annulée,

(c) après établissement de la connexion à l'étape (b1), (b2) ou (b3), le terminal de paiement électronique envoie les informations concernant la transaction de paiement à effectuer en utilisant la technologie déterminée à l'étape (b1), (b2) ou (b3),

(d) la carte de paiement requiert l'identification de l'utilisateur et l'accord sur la transaction à opérer et cas d'identification correcte et d'accord sur la transaction de paiement à effectuer, la carte de paiement envoie les données d'identification de l'utilisateur, les données de coordonnées bancaires et/ou les données de transaction de paiement accordé au terminal de paiement électronique,

(e) le terminal de paiement électronique corrobore et le cas échéant confirme les données d'identification de l'utilisateur, les données de coordonnées bancaires et les données concernant la transaction de paiement accordé avec un serveur distant qui approuve ou non la transaction de paiement,

(f) en cas d'approbation de la transaction de paiement, le terminal de paiement électronique envoie à la carte de paiement la confirmation que la transaction de paiement est approuvée en requérant ou non une confirmation explicite que la transaction est acceptée par l'utilisateur et peut être effectuée,

(g) en cas de confirmation de la requête de confirmation explicite par l'utilisateur ou en l'absence de requête de confirmation explicite par le terminal de paiement électronique, ce dernier confirme au serveur distant que la transaction de paiement a été effectuée ou est à effectuer et termine la connexion avec la carte de paiement.

[0021] Dans une variante avantageuse du procédé, la carte de paiement envoie, avec sa confirmation de connexion à l'étape (b1), (b2) ou (b3), les types de technologies de communication sans fil dont elle dispose au terminal de paiement électronique et le terminal de paiement électronique est configuré pour utiliser une ou plusieurs de ces technologies en variante ou en plus de la technologie de la connexion établie à l'étape (b1) ou (b2), dans la mesure où il en dispose. Il est à noter que les étapes (b1) et (b2) peuvent également être réalisées dans l'autre ordre, donc d'abord (b2), puis (b1).

[0022] Dans le procédé il est préféré que le terminal de paiement électronique utilise l'un des émetteurs/récepteurs OLC, de préférence VLC/LiFi ou IRDA, ou NFC pour l'émission et un autre de ces émetteurs/récepteurs OLC, de préférence IRDA ou VLC/LiFi, ou NFC pour la réception.

[0023] En variante, le terminal de paiement électronique émet et reçoit les données en les découpant et en les distribuant entre le ou les émetteur(s)/récepteur(s) OLC et/ou l'émetteur/récepteur NFC selon un algorithme de sécurisation.

[0024] Conscient que l'invention connait les règles de confidentialité d'échanges de données dans le secteur bancaire, l'invention utilise les dernières protections informatiques en vigueur ainsi que les derniers algorithmes utilisés dans ce cas.

[0025] Afin de trouver une solution au piratage d'un signal RF, la VLC (Visible Light Communication) ou de manière plus large l'OLC (Optical Light Communication) incluant outre le domaine visible VLC, également notamment les infra-rouges IRDA, est une technologie émergente dans laquelle les émetteurs, la lumière, transmettent des informations sans fil à l'aide d'un spectre lumineux visible. Cette technologie fonctionne comme les communications optiques basées sur l'infrarouge ou laser. VLC, ou LiFi, possède déjà une norme internationale IEEE 802.15.7. VLC est moyen de transmission qui couvre le bas débit comme la technologie Bluetooth, ou le haut-débit comme la technologie WiFi ou des débits très élevés jusqu'à 10 Gbit/s.

[0026] OLC/VLC est une communication entre une source de lumière LED et la caméra d'un smartphone, d'une tablette ou tout appareil avec une cellule photosensible ou photodiode ou photodiode organique ou caméra. La OLC/VLC est considérée comme étant de faible coût, de faible consommation énergétique et donc comme une technologie de communication verte. Le domaine des applications pour la technologie OLC/VLC est très large, du géo-marketing, à l'automobile, l'avionique, la ville intelligente, l'hôpital, l'éducation ou encore l'armée.

[0027] Dans ce contexte, la technologie OLC/VLC est vraiment adaptée dans le cadre de la sécurisation d'une transaction électronique et dématérialisée. Par contre, contrairement à la technologie à base de radiofréquences, la lumière est directionnelle et ne peut être piratée, lorsque nous ne sommes pas sous l'éclairage, au lieu de la NFC ou d'autres technologies radiofréquences qui peuvent être piratées à quelques mètres du terminal.

[0028] Dans ce contexte, même avec toutes les expériences académiques sur cette technologie, aucun de ces développements n'a eu l'idée d'adapter un TPE et une carte de paiement intelligente pour que ces appareils soient compatibles avec cette nouvelle technologie et ainsi apporter une solution réelle pour sécuriser une transaction dynamique sans fil.

[0029] Enfin, dans ce contexte, la carte de crédit ou de débit intelligente a besoin d'énergie pour activer toutes ces fonctionnalités et à notre connaissance, seule l'induction électromagnétique lors d'une transaction NFC a été utilisée, mais aucune cellule photovoltaïque organique n'a été utilisée pour stocker de l'énergie à l'intérieur d'une carte à puce.

[0030] Selon un objet de la présente invention, la carte à puce a une petite LED avec une PCB électronique dédiée pour assurer une transaction de paiement par communication lumineuse visible ou étendue à l'Infrarouge.

[0031] Un objet de la présente invention fournit un procédé pour sécuriser la transaction électronique de paiement par l'intermédiaire de la OSC et TPE en utilisant la technologie VLC.

[0032] Selon un objet de la présente invention, chaque TPE peut être modifié avec, sur le dessus du dispositif, une photodiode dédiée ou une photocellule.

[0033] Selon un autre objet de l'invention, comme tout TPE n'est pas compatible avec cette technologie de communication VLC, un accessoire a été conçu pour adapter la technologie VLC au TPE et utiliser la VLC comme protocole de communication pour sécuriser la transaction électronique de paiement. Cet accessoire est connecté au TPE via un USB ou autre type de connecteur.

[0034] Selon un objet de la présente invention, l'accessoire pour TPE possède une photocellule ou une photodiode, un module NFC et/ou un module IRDA, pour assurer à la fois la communication par VLC et NFC aussi.

[0035] Un autre objet de la présente invention fournit également l'utilisation de la détection d'empreintes digitales de l'OSC pour sécuriser un paiement électronique vers un TPE.

[0036] Selon un objet de la présente invention, l'OSC dispose d'un module NFC pour une partie du processus du paiement.

[0037] Selon un objet de la présente invention, un capteur est situé sous l'empreinte digitale pour activer l'électronique de OSC et en particulier la LED.

[0038] Un autre objet de la présente invention fournit également l'utilisation de cellules photovoltaïques organiques (OPC) couvrant la surface de OSC pour charger sa batterie intégrée.

[0039] Un autre objet de la présente invention fournit également l'utilisation d'un dispositif d'induction électromagnétique pour charger une batterie incorporée à l'intérieur de l'OSC, en complément ou en lieu et place de l'OPC.

[0040] Selon un objet de la présente invention, un procédé basé sur un centre de traitement de transaction et l'envoi de SMS est utilisé pour assurer la sécurité de la transaction de paiement.

[0041] En résumé, et outre ce qui a été mentionné ci-dessus, la présente invention peut être décrite de la manière suivante :

[0042] L'invention a pour objet une carte de paiement de crédit ou de débit avec une LED incorporée et une électronique dédiée pour utiliser la technologie de communication par lumière visible (VLC) ou IRDA dans le cadre d'une transaction électronique de paiement sans fil et/ou sans contact.

[0043] L'invention a pour objet une carte de paiement de crédit ou de débit avec une LED incorporée dans la gamme optique infrarouge et une électronique dédiée pour utiliser la technologie de communication optique (OLC) dans une transaction de paiement.

[0044] L'invention a pour revendication une carte de paiement de crédit ou de débit avec un commutateur LED pour utiliser VLC ou OLC dans le cadre d'une transaction de paiement.

[0045] L'invention a pour objet une empreinte digitale couplée aux commutateurs LED et aux technologies VLC ou OLC pour sécuriser la transaction électronique de paiement.

[0046] L'invention a pour objet une carte de paiement de crédit ou de débit avec un dispositif électromagnétique à induction pour charger la batterie intégrée pour alimenter en énergie et utiliser la technologie VLC ou l'OLC dans une transaction de paiement.

[0047] L'invention a pour objet une carte de paiement de crédit ou de débit avec une photodiode organique couvrant partiellement ou totalement la surface de la carte à puce pour charger la batterie intégrée, pour l'alimenter en énergie.

[0048] L'invention a pour objet différentes phases d'une transaction sécurisée entre un TPE compatible avec la VLC et l'OLC, d'un téléphone intelligent via les SMS pour autoriser et sécuriser la transaction électronique de paiement, en fonction du montant et de la fréquence d'utilisation du paiement par carte à puce.

[0049] L'invention a pour objet un TPE compatible avec la technologie de communication OLC étendue à la communication optique de façon large, avec ou sans accessoire.

[0050] L'invention a pour objet un TPE avec une photodiode dédiée, ou photocellule organique intégrée dans l'appareil pour la technologie OLC afin de sécuriser une transaction électronique de paiement.

[0051] L'invention a pour objet un TPE avec intégrée une LED dédiée ou une LED IRDA pour la technologie OLC, en envoyant des données via la OLC afin de sécuriser une transaction électronique de paiement.

[0052] L'invention a pour objet un accessoire pour TPE afin d'adapter la technologie OLC, notamment LiFi/VLC ou IRDA à un TPE classique, en connectant cet accessoire au TPE par quelque manière que ce soit comme un câble, afin de le doter d'un protocole de communication pour sécuriser une transaction électronique de paiement.

[0053] L'invention a pour objet un accessoire pour TPE, qui pourra se connecter avec le TPE de quelque manière que ce soit comme un câble USB ou Ethernet, ayant une photocellule organique ou une photodiode, un module NFC et un module OLC, pour assurer une communication OLC et NFC.

[0054] Le sigle IRDA désigne dans le contexte de la présente invention un nombre de protocoles de communication par infrarouges établis par l'IrDA (Infrared Data Association). Conventionnellement ces protocoles sont utilisés dans le domaine des télécommandes, etc. Dans le cadre de l'invention, il s'agit généralement d'un des protocoles spécifiques IrPHY, IrLAP, IrLMP, Tiny TP, IrCOMM, OBEX, IrLAN, IrSimple, IrSimpleShot et leurs dérivés.

[0055] Le terme radiofréquence (souvent abrégé en RF) désigne les ondes radio dont le spectre est situé entre 3 kHz et 300 GHz, ce qui inclut les fréquences utilisées par différents moyens de radiocommunication, notamment la téléphonie mobile, le Wi-Fi ou la radiodiffusion.

[0056] Dans l'invention, nous entendons par le terme WiFi la norme internationale IEEE 802.11 et ses dérivés, par Bluetooth, la norme internationale IEEE 802.15.1 et ses dérivés.

Brève description des dessins

[0057] D'autres particularités et caractéristiques de l'invention ressortiront de la description détaillée de quelques modes de réalisation avantageux présentés ci-dessous, à titre d'illustration, en se référant aux dessins annexés. Ceux-ci montrent:

[0058] La figure 1 est une vue représentative de l'utilisateur payant par TPE avec son OSC.

[0059] La figure 2 est une vue de face d'une carte de crédit ou de débit intelligente présentant ses différentes fonctionnalités de sécurité.

[0060] La figure 3 est une vue arrière d'une carte de crédit ou de débit intelligente montrant ses différentes fonctionnalités de sécurité et la puce LED.

[0061] La figure 4 est une vue interne d'une carte de crédit ou de débit intelligente montrant ses différents modules électroniques.

[0062] La figure 5 est une vue schématique du module électronique principal à l'intérieur de la carte à puce.

[0063] La figure 6 est une vue schématique d'un TPE avec une option interne de VLC et une vue d'un accessoire branché à un TPE pour une transaction par OLC.

[0064] La figure 7 est un zoom du TPE permettant une transaction par VLC et d'une vue détaillée du TPE avec un accessoire branché permettant une transaction par OLC.

[0065] La figure 8 est un zoom et une vue détaillée de l'accessoire branché pour un TPE.

[0066] La figure 9 est un schéma synoptique d'une carte de crédit, de débit ou de crédit, avec une empreinte digitale et des fonctionnalités de OLC, pour une transaction sécurisée avec un TPE.

[0067] La figure 10 est un schéma fonctionnel d'une carte à puce, de débit ou de crédit, avec des fonctionnalités d'interrupteur et de OLC, pour une transaction sécurisée avec un TPE à travers une application mobile.

[0068] La figure 11 est une représentation schématique des données de transmission lorsqu'une autorisation de paiement nécessite une réponse du smartphone du consommateur.

[0069] La figure 12 est une représentation détaillée des données de transmission lorsqu'une autorisation de paiement nécessite la réponse du smartphone du consommateur.

Description d'une exécution préférée

[0070] La figure 1 est une vue générale du cas d'utilisation de cette invention. Un utilisateur (001) paie ses achats avec sa carte à puce (002) sans contact, également appelée OSC dans le cadre de la présente invention, en pointant sa carte à puce sur le TPE (003). Le caissier peut voir la transaction autorisée.

[0071] La figure 2 est une vue de face d'une carte de crédit ou de débit intelligente montrant ses différentes fonctionnalités. Sur le devant, la carte à puce présente les éléments typiques sur le support (002), la puce principale (004), le numéro de la carte (005), le nom du titulaire (006), un logo (008), la date d'expiration (007), logo NFC (110) et nouveaux éléments. L'interrupteur sensitif (100) comme un composant électronique organique, l'homme d'art connaîtra le choix du meilleur matériau, muni au même niveau d'un capteur d'empreinte digitale (101) pouvant être implémenté par-dessus. L'empreinte digitale peut être couplée à la technologie OLC et constitue un avantage réel pour augmenter la sécurité du paiement. L'interrupteur permet de contrôler la LED, l'utilisation du NFC et par conséquent la consommation énergétique. Cet interrupteur permet également d'augmenter la sécurité de la carte à puce car le NFC et la OLC ne se produiront que lorsque l'interrupteur sera activé. Le dernier élément couvre la zone totale ou partielle de l'avant de la carte à puce correspondant à une cellule du type polymère photovoltaïque (OPV) (102). L'homme d'art choisira le meilleur matériel

pour mettre en œuvre le meilleur OPV pour répondre aux besoins d'énergie. La cellule OPV pourra être mise en sus de l'induction électromagnétique.

[0072] La figure 3 est une vue arrière d'une carte de crédit ou de débit intelligente (002) montrant la bande magnétique (009), le panneau de signature (010), un hologramme (012), le code de sécurité de la carte (CVV) (011), en trois Chiffre ou quatre chiffres, près du panneau de signature qui peut être imprimé ou sous forme d'affichage numérique pour augmenter également la transaction de sécurité en particulier pour le paiement électronique. Le dernier module est la LED (103), généralement une LED inorganique, mais aussi une LED organique, en couleur blanche, ou en RGB, ou en infrarouge et non limité à la nature des LED. À cette date, certains LED avec une épaisseur inférieure à 0,4 mm sont déjà commerciales. Cette LED est réglée à l'opposé de l'interrupteur près du panneau de signature. Pour la mémoire, l'interrupteur est situé sur le côté avant juste derrière l'hologramme.

[0073] La figure 4 est une vue interne d'une carte de crédit ou de débit intelligente montrant ses différents modules électroniques stratifiés dans la carte. Un PCB flexible organique (104) pourra être utilisée pour le processus industrialisation. Une antenne interne (108) est utilisée pour la partie NFC connectée à la puce RFID (109), elle-même liée à un deuxième module électronique principal (107) et la puce habituelle (004), pour carte de crédit dans laquelle toutes les informations du titulaire sont stockées. Le module (107) gère toutes les fonctionnalités électroniques de la carte à puce. L'empreinte digitale (101) et l'interrupteur (100) sont également commandés par le module 107. L'antenne OPV (102) et/ou également l'antenne magnétique (106) fournissent l'énergie pour la batterie interne (105). Le dernier composant est la LED (103), directement connectée au module électronique (107).

[0074] La figure 5 est une vue schématique du module électronique (107). Ce module a pour fonction principale de gérer – l'énergie obtenue par induction et/ou OPV, – reconnaissance digitale numérique, – l'interrupteur, – données de stockage, – allocation de la nature de la transmission de données en ce qui concerne NFC ou OLC, – modules de communication OLC et NFC et les données de transmission au TPE, – et d'autres fonctions si la carte à puce en possède comme code numérique de sécurité sur la carte à puce (011). Ainsi, pour gérer

toutes ces fonctionnalités, un microcontrôleur (302) comme un FPGA ou ASIC ou DSP, l'homme d'art choisira le meilleur, un module OLC (303), une mémoire de stockage (304). Tous ces composants sont situés sur un PCB souple (301) ou directement au PCB flexible principal (104), selon les contraintes industrielles. Dans certains cas, pour étendre le cas d'utilisation de cette invention, ce module pourrait également avoir des puces WiFi (305) et/ou une dernière génération de chipset Bluetooth (306). Le microcontrôleur est programmé pour recevoir toutes les informations du TPE par NFC et pour envoyer les données sensibles par OLC, les autres données mineures peuvent être transmises par RF. Dans tous les cas de transmission OLC et RF, le signal suit les différents critères de cryptologie requis par les consortiums bancaires.

[0075] La figure 6 est un zoom sur différentes possibilités décrites dans le cas de cette invention concernant le TPE. Dans le premier cas, mais non limité, l'OSC (002) communique par OLC avec TPE (003), qui ont dans ce cas une photocellule (200) pour recevoir le signal de OSC. Le deuxième cas, l'OSC (002) communique (300) à travers un accessoire (013) connecté à TPE.

[0076] La figure 7 est un zoom du TPE modifié (200). Ce TPE a un aspect général pour ce type d'appareil, avec un fond, un écran et vers le haut, un verre rectangulaire ou un plastique (201). Sous cette protection, deux types de photocellules peuvent être utilisés soit une grande photocellule organique ou inorganique (202), soit plusieurs photodiodes très proches (203). Dans les deux derniers cas, ce dispositif de réception de la communication de la lumière visible suffit pour recevoir une bonne qualité du signal de l'OSC. La Figure montre aussi un zoom d'un TPE avec un accessoire pour utiliser TPE (200) avec la technologie OLC. Cet accessoire (210) est connecté à TPE avec un connecteur USB mal (212) et par un fil (211).

[0077] La figure 8 détaille l'accessoire du TPE (013). Cet accessoire est comme un petit panneau avec un plastique transparent et protecteur (202) sur son dessus. Derrière, un premier PCB (204) est présent. Ce PCB prend en charge différents composants électroniques tels que la photodiode (206) ou la photocellule, inorganique ou organique, la cellule IRDA (207) pour une communication bidirectionnelle avec la carte OSC ou un smartphone, lorsque le smartphone est compatible avec cette technologie, le module NFC (208) et un

dispositif alternatif avec un module IRDA. Derrière ce première PCB est connecté un deuxième module (214) qui contient différents composants électroniques permettant une communication sécurisée. Sur ce PCB (205), un module OLC (214), un module NFC (210), un microcontrôleur (213) et d'autres composants électroniques (212) parmi ceux pour la sécurisation de la transaction. Le fil (211) avec un connecteur USB mal est également connecté à ce PCB (205). La cellule IRDA (207) est intégrée à cet accessoire pour être compatible avec un téléphone intelligent ayant un protocole de communication optique intégré.

[0078] La figure 9 est un schéma fonctionnel montrant la procédure d'un transfert de paiement entre OSC et un TPE. Le TPE envoie un signal NFC à OSC (400). L'OSC reçoit ce signal et est activé (401) mais rien ne se produit tant que le doigt de l'utilisateur n'a pas été reconnu. Si l'empreinte digitale est reconnue (402), la LED est allumée (403) et envoie les données (404) au TPE, une communication hybride et une transaction se produisent entre le TPE et l'OSC (405) pour finaliser le paiement (406). Si, l'empreinte digitale n'est pas reconnue (407), aucune communication à travers la LED n'est établie (408) et un code PIN est requis sur le TPE (409) pour effectuer la transaction de paiement (410).

[0079] La figure 10 est un organigramme du processus opérationnel de la transaction. Comme avec du NFC, cette invention a sécurisé la transaction avec un paiement limité, en particulier dans le cas où aucune empreinte digitale n'est intégrée dans l'OSC. Le TPE envoie un signal NFC (411). L'OSC reçoit ce signal NFC (412) et lorsque l'utilisateur met son doigt sur le commutateur LED (413), la LED fonctionne (414) et l'OSC envoie une donnée au TPE (415). Si la transaction est inférieure à un certain montant (20 € par exemple) (416) et si c'est la première fois depuis un certain temps (définir par la banque), dans la figure une heure, par exemple, ou s'il s'agit de la nième fois (N <x, x est une valeur définie par la banque) pendant la durée prédéfinie par la banque, la transaction se produit (417) et le paiement est accepté. Mais, si la quantité de transaction, signifie n> x (418), une confirmation du paiement est requise par SMS (420) sur le smartphone de l'utilisateur. Une réponse "Y", sur le smartphone de l'utilisateur, autorise la transaction pour la nième fois. Une réponse "N" annule la transaction. Dans le cas où la transaction est supérieure au (419) montant défini par la banque (dans notre cas, 20 €), une confirmation par SMS est nécessaire comme précédemment

(420). Ensuite, la transaction se produit ou pas suivant la réponse "Y" ou "N" de l'utilisateur.

[0080] La figure 11 décrit la communication entre l'utilisateur lors d'une transaction de paiement avec son smartphone (310). Lorsque l'utilisateur (001) effectue la transaction avec sa carte OSC (002) et le TPE (003), si une autorisation par téléphone est nécessaire, un centre de traitement de transaction comprenant la banque, l'émetteur OSC, l'opérateur de téléphonie cellulaire et/ou les services de paiement. Ainsi, lorsque le TPE envoie une demande à un Centre de traitement des transactions bancaires (422), y compris un serveur de service, des serveurs de transactions financières, un serveur établissement et le centre de traitement des transactions, appelé TPC (422), ouvre un canal de communication sécurisé entre l'OSC et TPE (421), OSC vers TPC et 425, TPC vers OSC) et TPC et Smartphone (310) d'utilisateur, (Smartphone vers TPC, 424, et TPC vers smartphone, 423).

[0081] La figure 12 détaille entièrement le processus de la transaction avec le smartphone. Lorsque l'utilisateur (001) est dans le cas d'un paiement avec autorisation via le smartphone, une communication (421) avec TPC (422) est engagée. Tout d'abord, le TPC envoie au téléphone (423) par un SMS un message (310) comme "Un montant de montant XX doit être chargé sur votre carte de crédit 4000XXXXX 9010, Répondez Y pour confirmer ou N pour refuser la transaction" (428). Lorsque l'émetteur envoie la réponse SMS avec la réponse (427), le SMS est envoyé à TPC (424) pour analyse et si la réponse est Y (429), le paiement est approuvé (425) et l'utilisateur reçoit un SMS pour confirmer LI paiement (430). Ce sera le même processus si la réponse est N, un SMS pour confirmer l'annulation du paiement.

Revendications

1. Carte de paiement (002) de crédit ou de débit, comprenant une face avant comportant des caractéristiques courantes, par exemple le numéro de la carte de paiement (005), le nom du titulaire (006), un logo (008), la date d'expiration (007) et/ou une puce électronique (004), et une face arrière comportant des caractéristiques courantes, par exemple une bande magnétique (009), un panneau de signature (010), un hologramme (012) et/ou un code de sécurité de la carte (011), la carte de paiement comprenant en outre les composants électriques suivants : une batterie (105) ; un module électronique de contrôle (107) comprenant un microcontrôleur (302) et une mémoire de stockage (304) ; et au moins une photocellule ou photodiode et au moins une LED (103) comme émetteur/récepteur OLC, de préférence VLC/LiFi et/ou IRDA, orientée de préférence vers la face arrière de la carte de paiement et un interrupteur (100) de mise sous tension des composants électriques, le module électronique de contrôle (107) étant configuré pour contrôler la ou les photocellule(s) ou photodiode(s) et LED (103) suivant un protocole de communication OLC, de préférence un protocole de communication VLC/LiFi et/ou IRDA.

2. Carte de paiement (002) selon la revendication 1 comprenant en outre un émetteur/récepteur NFC (108,109) et/ou une puce RFID (109) contrôlable(s) par le module électronique de contrôle (107).

3. Carte de paiement (002) selon l'une des revendications 1 ou 2, comprenant en outre un dispositif électromagnétique à induction (106) pour charger la batterie (105).

4. Carte de paiement (002) selon l'une quelconque des revendications précédentes, comprenant une ou plusieurs photodiodes organiques (102), de préférence de type polymère photovoltaïque, couvrant de manière particulièrement préférée partiellement ou totalement la face avant et/ou arrière de la carte de paiement pour charger la batterie (105).

5. Carte de paiement (002) selon l'une quelconque des revendications précédentes, comprenant un capteur d'empreinte digitale (101) contrôlable par

le module électronique de contrôle (107), le capteur d'empreinte digitale (101) étant de préférence associé à l'interrupteur (100).

6. Carte de paiement (002) selon l'une quelconque des revendications précédentes, comprenant sur la face arrière un affichage, de préférence un affichage numérique ou un écran e-ink, pour afficher le code de sécurité de la carte (011).

7. Carte de paiement (002) selon l'une quelconque des revendications précédentes, dans laquelle le module électronique de contrôle (107) comprend en outre un module de communication WiFi (305) et/ou Bluetooth (306).

8. Terminal de paiement électronique (003) comprenant au moins une photocellule ou photodiode (200, 202, 203) et au moins une LED (204) comme émetteur/récepteur OLC, de préférence VLC/LiFi et/ou IRDA, adapté pour l'émission et la réception d'un flux de données conformément à un protocole de communication OLC, de préférence VLC/LiFi et/ou IRDA, notamment des données d'identification d'un utilisateur, des données de coordonnées bancaires et/ou des données de transaction de paiement à effectuer ; un processeur pour convertir et/ou gérer le flux de données ; des moyens de stockage adaptés pour stocker du moins temporairement le flux de données reçues du réseau de données ; des moyens de connexion à un réseau de données, de préférence à un serveur distant configuré pour corroborer et le cas échéant confirmer les données d'identification de l'utilisateur, les données de coordonnées bancaires et les données concernant la transaction de paiement à effectuer.

9. Terminal de paiement électronique selon la revendication 8, comprenant en outre un émetteur/récepteur NFC adapté pour l'émission et la réception d'un flux de données conformément à un protocole de communication NFC, notamment des données d'identification d'un utilisateur, des données de coordonnées bancaires et/ou des données de transaction de paiement à effectuer.

10. Terminal de paiement électronique selon la revendication 9, le processeur étant configuré pour déterminer le protocole de communication à utiliser en fonction d'informations d'intensité lumineuse ambiante et/ou de présence ou

d'absence de réception d'un signal OLC et/ou NFC et/ou après négociation avec un smartphone et/ou une carte de paiement requérant l'entrée en communication, de préférence une carte de paiement selon l'une quelconque des revendications 1 à 7.

11. Terminal de paiement électronique selon la revendication 9 ou 10, dans lequel le processeur est configuré pour émettre et recevoir le flux de données en utilisant un des émetteurs/récepteurs OLC ou NFC pour l'émission et l'autre de ces émetteurs/récepteurs OLC ou NFC pour la réception.

12. Terminal de paiement électronique selon la revendication 9 ou 10, dans lequel le processeur est configuré pour émettre et recevoir le flux de données en le découpant et en le distribuant entre l'émetteur/récepteur OLC, et l'émetteur/récepteur NFC selon un algorithme de sécurisation.

13. Terminal de paiement électronique selon l'une quelconque des revendications 8 à 12, dans lequel l'émetteur/récepteur OLC, et optionnellement un émetteur/récepteur NFC, est/sont intégré(s) dans le boitier du terminal de paiement électronique (003) ; ou dans lequel l'émetteur/récepteur OLC, et optionnellement un émetteur/récepteur NFC, est/sont disposé(s) dans un boitier séparé (013) relié au terminal de paiement électronique (003) par une connexion filaire (014), notamment USB (015) ou Ethernet.

14. Procédé de paiement électronique sécurisé par un terminal de paiement électronique selon l'une quelconque des revendications 8 à 13 au moyen d'une communication sans fil avec une carte de paiement, de préférence une carte de paiement selon l'une quelconque des revendications 1 à 7, le procédé comprenant les étapes :

    (a) déclenché par une transaction de paiement à effectuer, le terminal de paiement électronique envoie une requête de connexion par l'émetteur OLC, de préférence VLC/LiFi et/ou IRDA,

    (b) (b1) la carte de paiement a un émetteur/récepteur IRDA, reçoit la requête et envoi une confirmation de connexion au terminal de paiement électronique d'utiliser la technologie IRDA ; ou

(b2) la carte de paiement a un émetteur/récepteur VLC/LiFi, reçoit la requête et envoi une confirmation de connexion au terminal de paiement électronique d'utiliser la technologie VLC/LiFi ; ou

(b3) la carte de paiement n'a pas d'émetteur/récepteur OLC, ce dernier n'est pas activé ou n'est pas placé de manière appropriée devant l'émetteur du terminal de paiement électronique, la carte de paiement ne répond pas endéans un lapse de temps déterminé et le terminal de paiement électronique renvoie sa requête de connexion par un émetteur/récepteur NFC, lorsque la carte de paiement reçoit une telle requête de connexion par NFC, il envoie la confirmation de connexion au terminal de paiement électronique d'utiliser la technologie NFC,

(b4) en cas de non-réponse à chacune des requêtes de connexion, la transaction est soit présenté par le terminal de paiement électronique pour paiement électronique avec carte de crédit ou débit, soit annulée,

les étapes (b1) et (b2) pouvant être réalisées dans n'importe quel ordre,

(c) après établissement de la connexion à l'étape (b1), (b2) ou (b3), le terminal de paiement électronique envoie les informations concernant la transaction de paiement à effectuer en utilisant la technologie déterminée à l'étape (b1), (b2) ou (b3),

(d) la carte de paiement requiert l'identification de l'utilisateur et l'accord sur la transaction à opérer et cas d'identification correcte et d'accord sur la transaction de paiement à effectuer, la carte de paiement envoie les données d'identification de l'utilisateur, les données de coordonnées bancaires et/ou les données de transaction de paiement accordé au terminal de paiement électronique,

(e) le terminal de paiement électronique corrobore et le cas échéant confirme les données d'identification de l'utilisateur, les données de coordonnées bancaires et les données concernant la transaction de paiement accordé avec un serveur distant qui approuve ou non la transaction de paiement,

(f) en cas d'approbation de la transaction de paiement, le terminal de paiement électronique envoie à la carte de paiement la confirmation

que la transaction de paiement est approuvée en requérant ou non une confirmation explicite que la transaction est acceptée par l'utilisateur et peut être effectuée,

(g) en cas de confirmation de la requête de confirmation explicite par l'utilisateur ou en l'absence de requête de confirmation explicite par le terminal de paiement électronique, ce dernier confirme au serveur distant que la transaction de paiement a été effectuée ou est à effectuer et termine la connexion avec la carte de paiement.

15. Procédé selon la revendication 14, dans lequel la carte de paiement envoie, avec sa confirmation de connexion à l'étape (b1), (b2) ou (b3), les types de technologies de communication sans fil dont elle dispose au terminal de paiement électronique et le terminal de paiement électronique est configuré pour utiliser une ou plusieurs de ces technologies en variante ou en plus de la technologie de la connexion établie à l'étape (b1), (b2) ou (b3), dans la mesure où il en dispose.

16. Procédé selon la revendication 14 ou 15, dans lequel le terminal de paiement électronique utilise l'un des émetteurs/récepteurs OLC, de préférence VLC/LiFi ou IRDA, ou NFC pour l'émission et un autre de ces émetteurs/récepteurs OLC, de préférence IRDA ou VLC/LiFi, ou NFC pour la réception.

17. Procédé selon la revendication 14 ou 15, dans lequel le terminal de paiement électronique émet et reçoit les données en les découpant et en les distribuant entre au moins deux émetteurs/récepteurs choisis parmi l'émetteur/récepteur IRDA, l'émetteur/récepteur VLC/LiFi et l'émetteur/récepteur NFC, selon un algorithme de sécurisation.

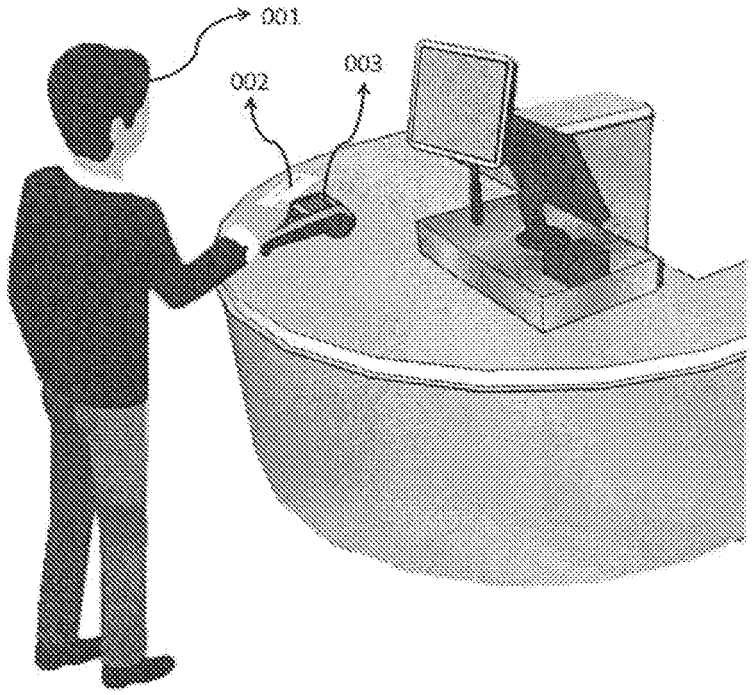
001
002
003

FIG. 1

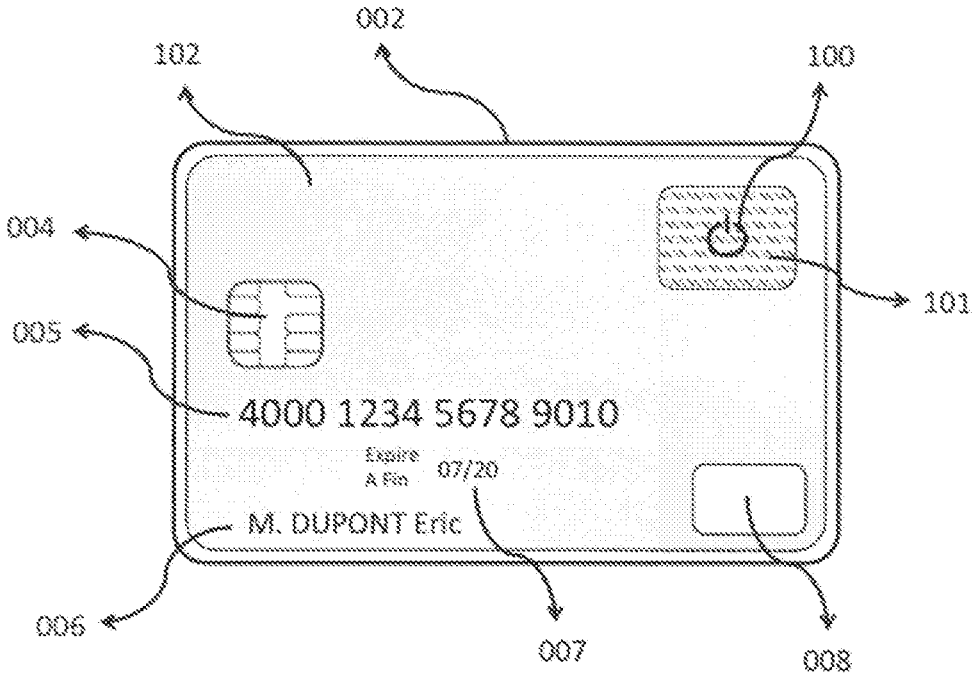
002
102
100
004
101
005
4000 1234 5678 9010
Expire
A Fin
07/20
M. DUPONT Eric
006
007
008

FIG. 2

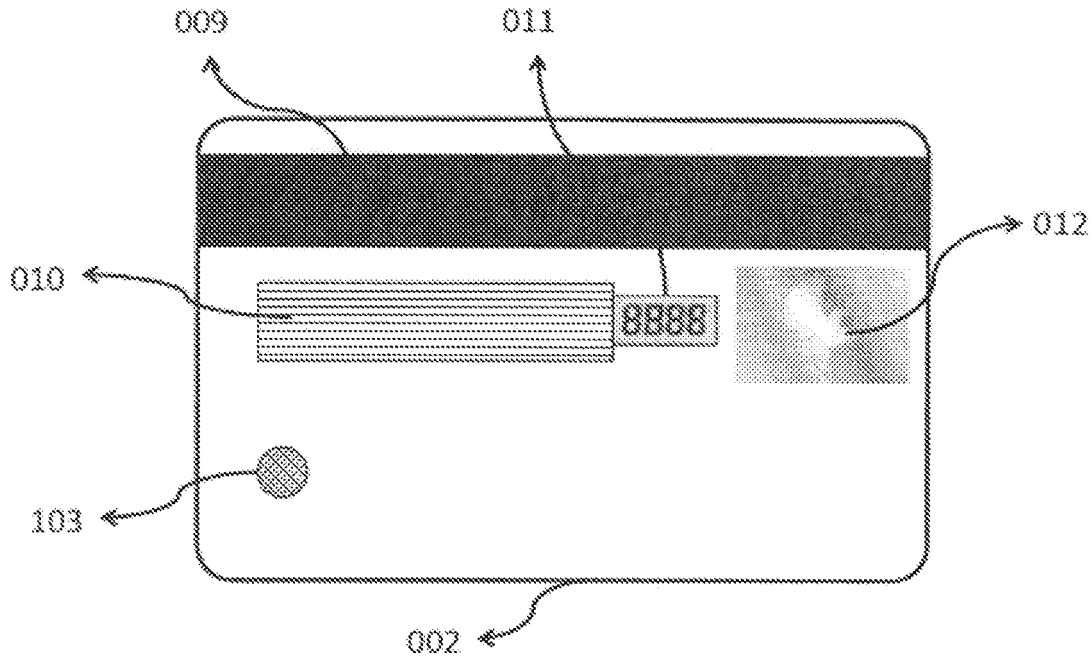
009
011
012
010
8888
103
002

FIG. 3

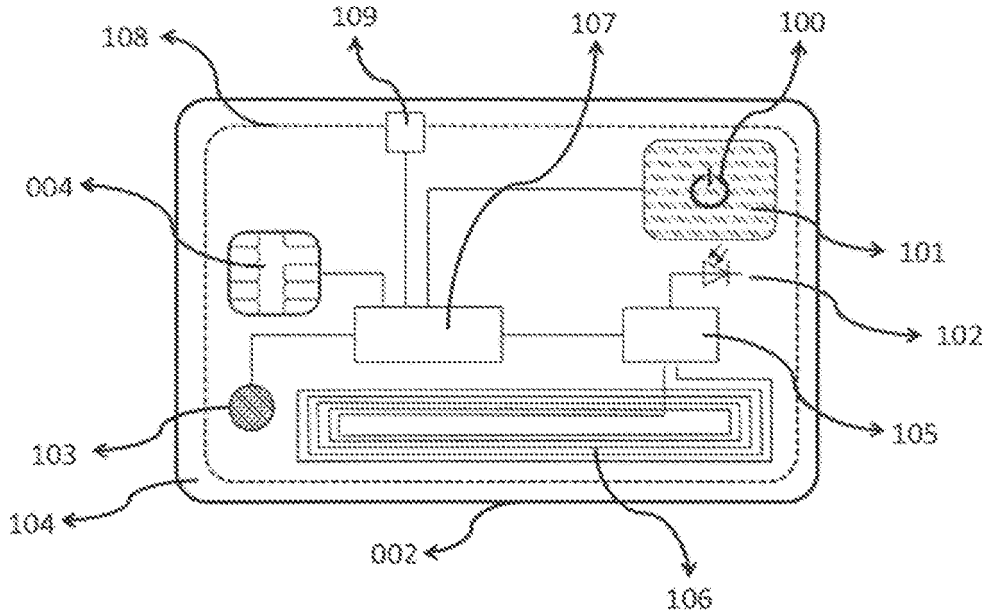
108
109
107
100
004
101
102
103
105
104
002
106

FIG. 4

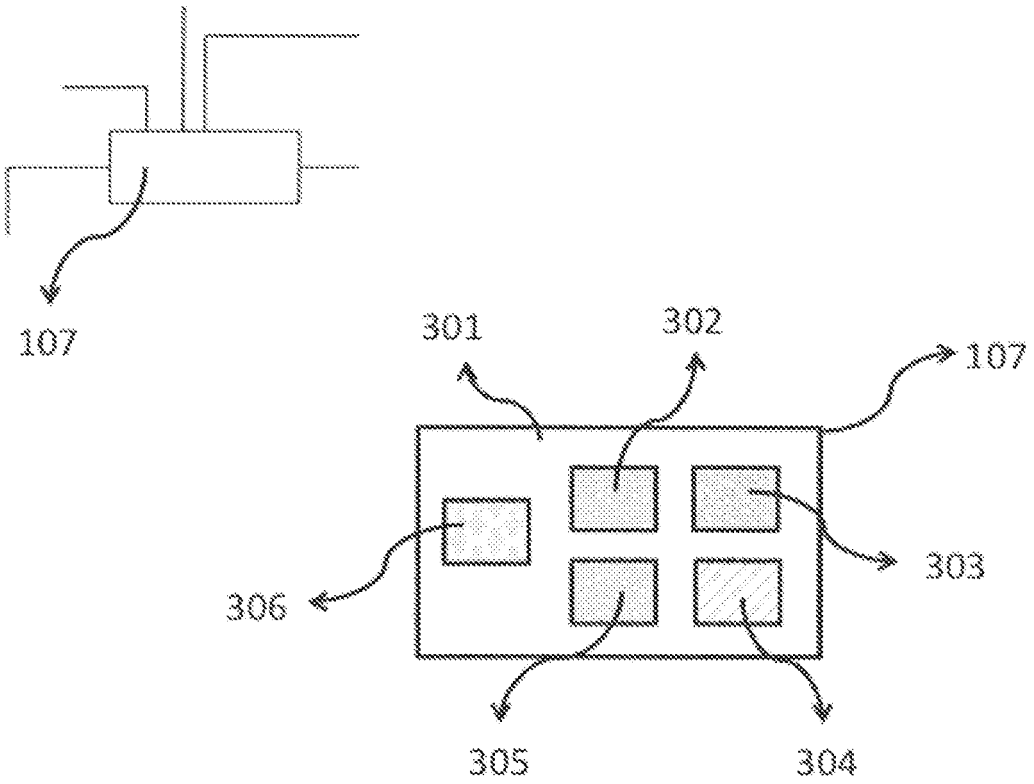

FIG. 5

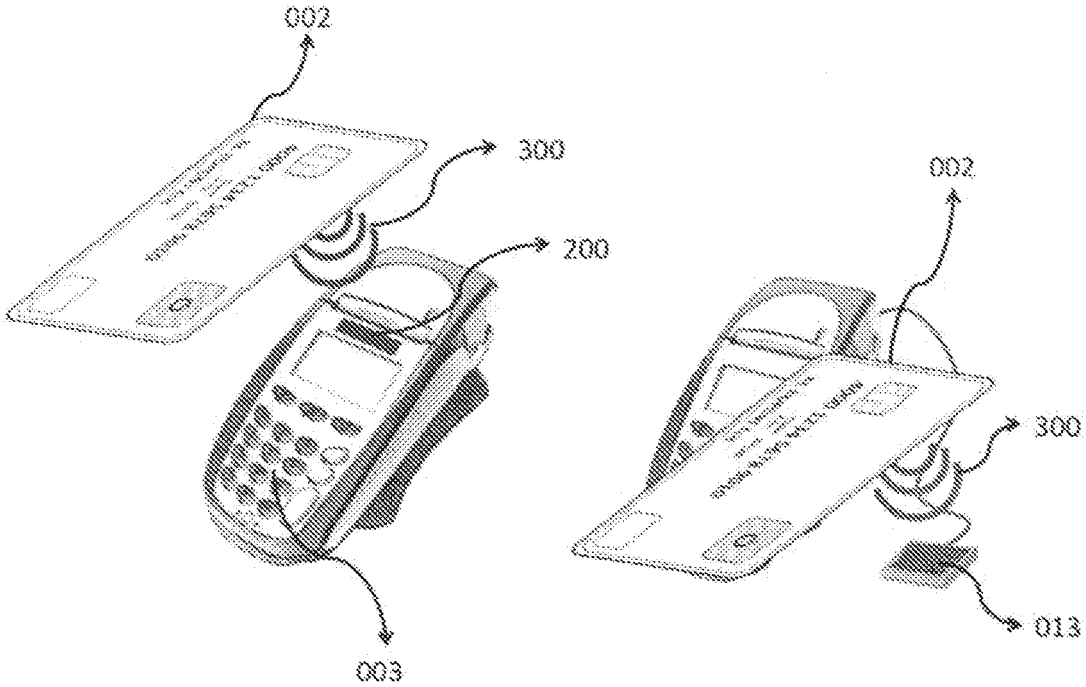

FIG. 6

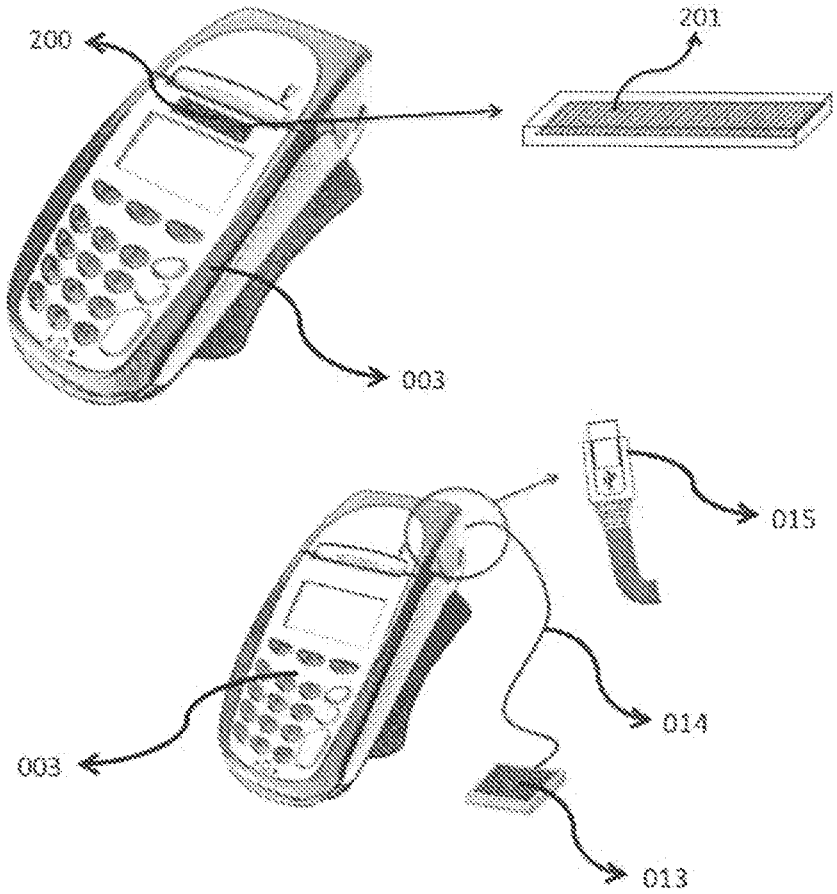
200
201
003
015
014
003
013

FIG. 7

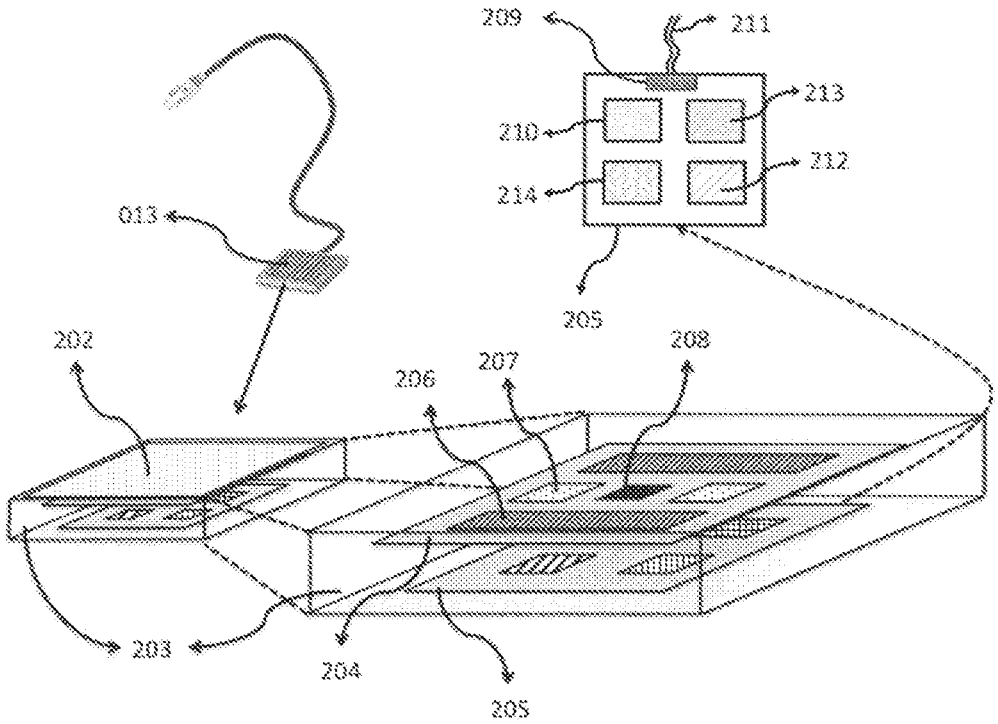
209
211
213
210
212
214
013
205
202
206
207
208
203
204
205

FIG. 8

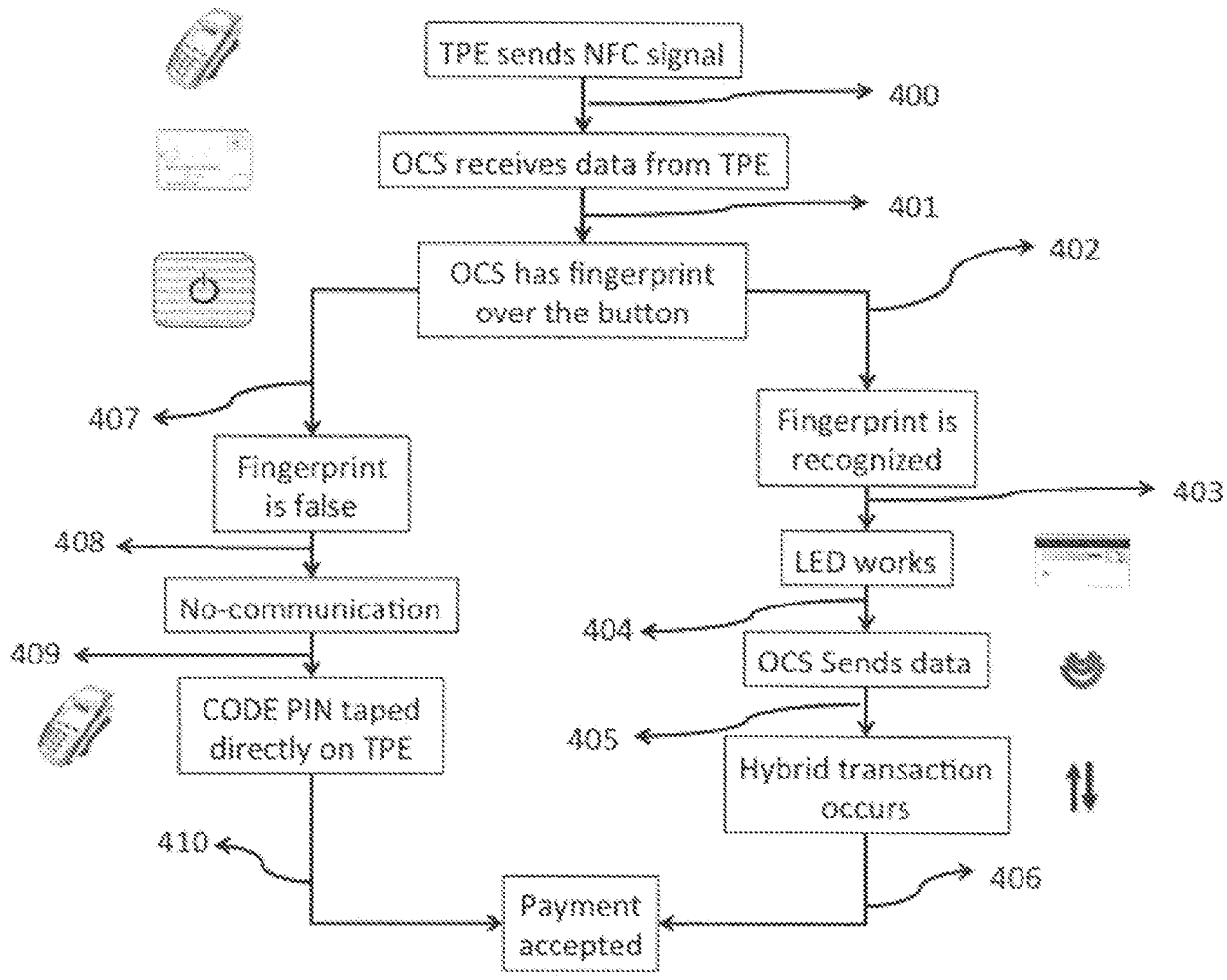
TPE sends NFC signal
400
OCS receives data from TPE
401
OCS has fingerprint over the button
402
407
Fingerprint is false
Fingerprint is recognized
403
408
LED works
No-communication
404
OCS Sends data
409
CODE PIN taped directly on TPE
405
Hybrid transaction occurs
410
406
Payment accepted

FIG. 9

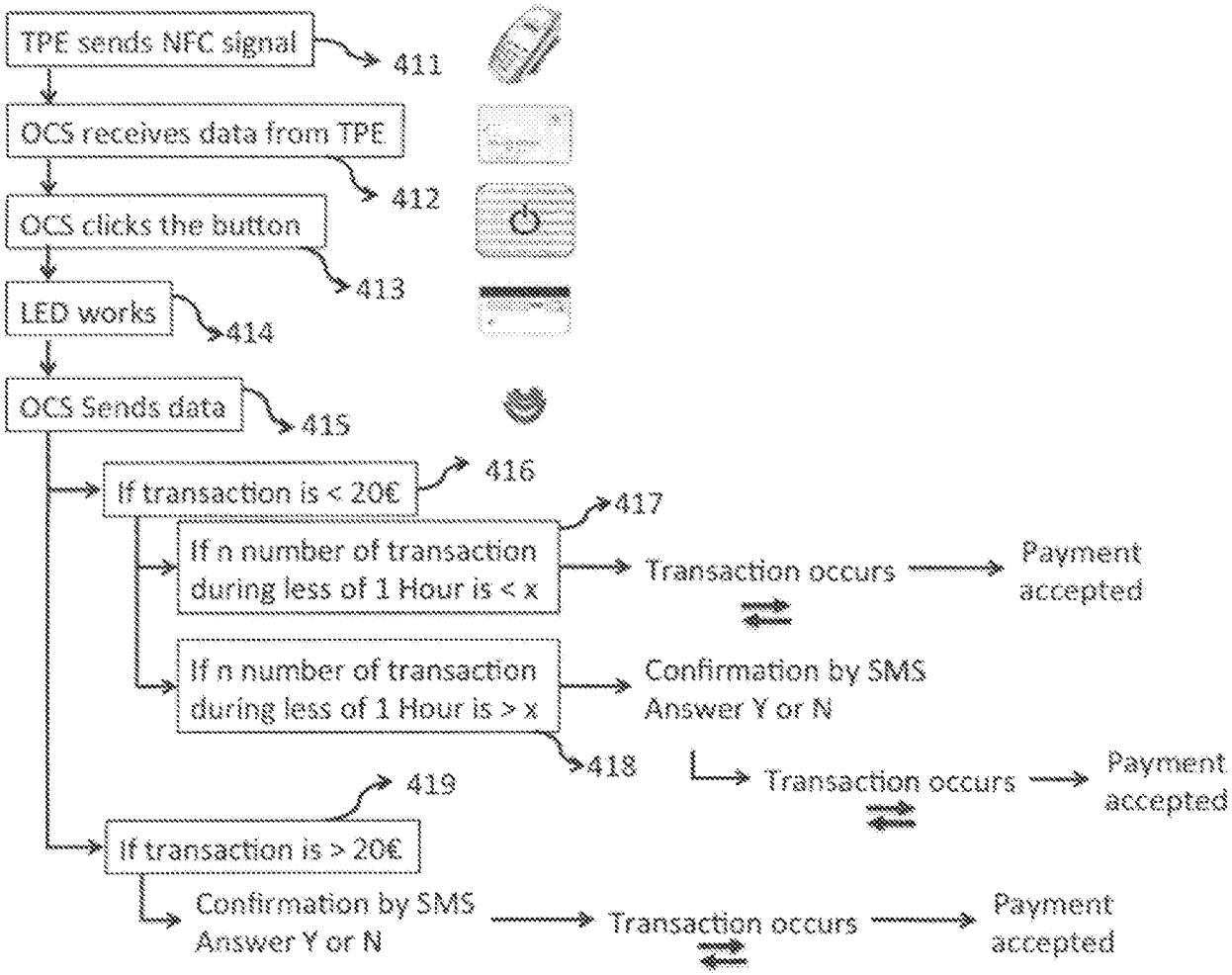
TPE sends NFC signal
411
OCS receives data from TPE
412
OCS clicks the button
413
LED works
414
OCS Sends data
415
If transaction is < 20€
416
417
If n number of transaction during less of 1 Hour is < x
Transaction occurs
Payment accepted
If n number of transaction during less of 1 Hour is > x
Confirmation by SMS Answer Y or N
418
Transaction occurs
Payment accepted
419
If transaction is > 20€
Confirmation by SMS Answer Y or N
Transaction occurs
Payment accepted

FIG. 10

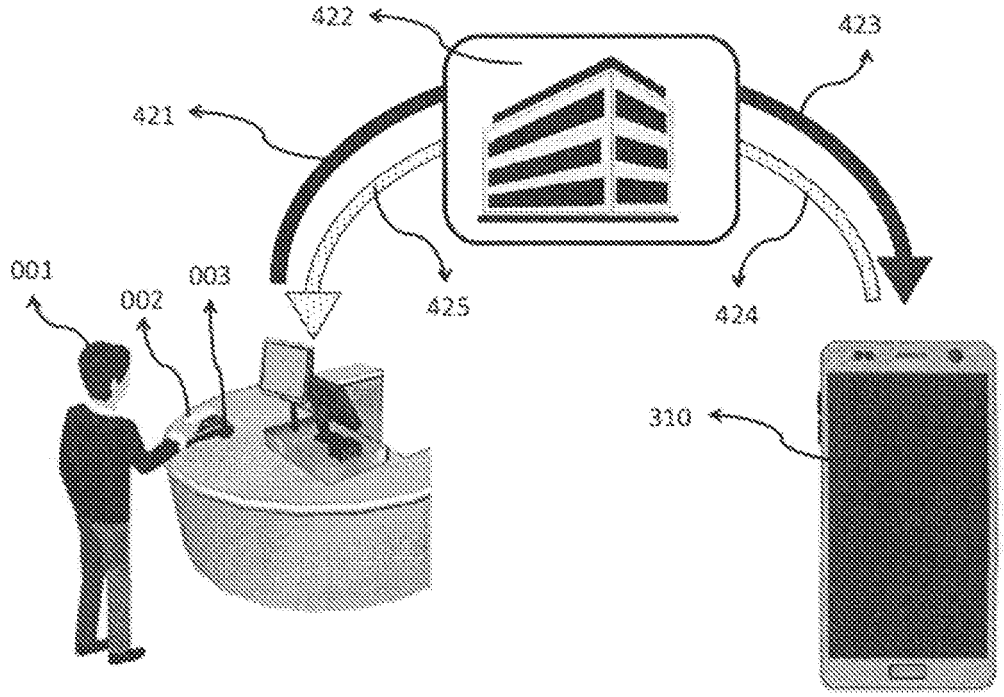
422
423
421
001
002
003
425
424
310

FIG. 11

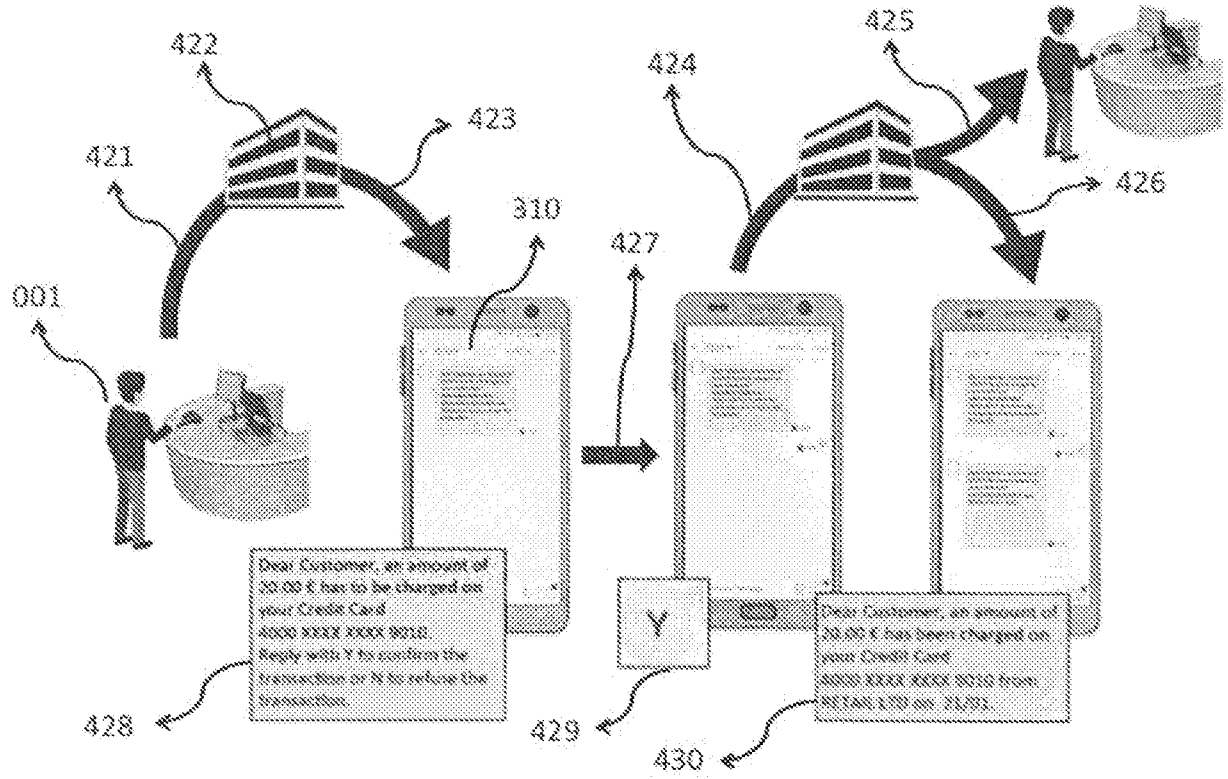
422
423
421
310
001
427
424
425
426
Dear Customer, an amount of
30.00 € has to be charged on
your Credit Card
4000 XXXX XXXX 9010
Reply with Y to confirm the
transaction or N to refuse the
transaction.
Y
Dear Customer, an amount of
30.00 € has been charged on
your Credit Card
4000 XXXX XXXX 9010 from
RETAIL LTD on 31/01.
428
429
430

FIG. 12