

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

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(43) Date de la publication internationale
18 juin 2020 (18.06.2020)

(10) Numéro de publication internationale
WO 2020/120849 A1

(51) Classification internationale des brevets :
G06Q 20/34 (2012.01) G07F 7/08 (2006.01)
G07F 7/12 (2006.01)

(72) Inventeurs : **ABISDID, Charli** ; 6, Rue de Mondovi,
13006 MARSEILLE (FR). **ABISDID, Marlène** ; 6, Rue de
Mondovi, 13006 MARSEILLE (FR).

(21) Numéro de la demande internationale :
PCT/FR2019/051912

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

(22) Date de dépôt international :
07 août 2019 (07.08.2019)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1872665 11 décembre 2018 (11.12.2018) FR

(71) Déposant : **CCS 12 [FR/FR]** ; 6, allée Turcat Mery, 13008
Marseille (FR).

(84) États désignés (sauf indication contraire, pour tout titre de
protection régionale disponible) : ARIPO (BW, GH, GM,

(54) Title: DEVICE AND METHOD FOR SECURING SECURE DATA FOR A BANK PAYMENT CARD

(54) Titre : DISPOSITIF ET PROCÉDÉ POUR SÉCURISER DES DONNÉES SÉCURITAIRES D'UNE CARTE DE PAIEMENT BANCAIRE

Fig. 5a

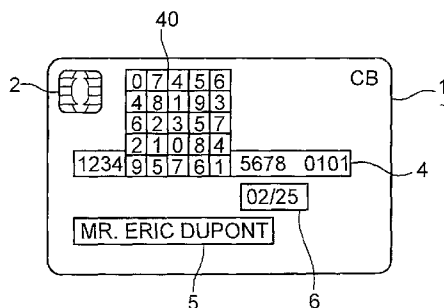
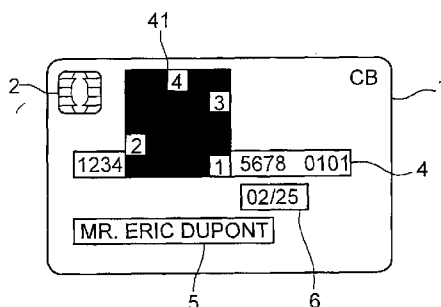


Fig. 5c



(57) Abstract: The invention relates to a method for securing secure data for a bank card associated with a bank account, which secure data are static and include the number of said card, identification data of the holder of said card, the expiration date of said card, and a security code, which bank card number and which security code consist of a plurality of numbers and/or letters, characterized in that the method includes the steps of: - only partially writing the secure data on said card such that secure data are concealed and never visible on said card, which concealed data are formed by: a plurality of numbers and/or letters of the number of said card and/or at least one identification datum of the holder and/or at least one element of the expiration date and/or at least one number and/or letter of the security code; - transmitting, to the holder of the card alone, a means for revealing the concealed data.

KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

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

(57) Abrégé : L'invention concerne un procédé de sécurisation des données sécuritaires d'une carte bancaire associée à un compte bancaire, lesquelles données sécuritaires sont statiques et comportent le numéro de ladite carte, des données d'identification du titulaire de ladite carte, la date d'expiration de ladite carte, et un cryptogramme, lequel numéro de carte bancaire et lequel cryptogramme sont constitués de plusieurs chiffres et/ou lettres, caractérisé en ce qu'il comporte les étapes consistant a : - n'inscrire que partiellement les données sécuritaires sur ladite carte de sorte que des données sécuritaires sont occultés et jamais visibles sur ladite carte, lesquelles données occultées étant formées par : plusieurs chiffres et/ou lettres du numéro de ladite carte et/ou au moins une donnée d'identification du titulaire et/ou au moins un élément de la date d'expiration et/ou au moins un chiffre et/ou lettre du cryptogramme, - transmettre, au seul titulaire de la carte, un moyen de divulgation des données occultées.

Description

Titre: Dispositif et procédé pour sécuriser des données sécuritaires d'une carte de paiement bancaire

Domaine technique.

- [1] L'invention a pour objet un dispositif et un procédé de sécurisation des données sécuritaires d'une carte de paiement bancaire.
- [2] La présente invention concerne le domaine de la sécurisation des données généralement inscrites sur une face d'une carte de paiement bancaire en vue de sécuriser des opérations de paiement.

Technique antérieure.

- [3] Des données sécuritaires associées à un compte bancaire sont apposées sur une carte de paiement, telles que le numéro de la carte, le nom du client, et sa date limite de validité, qui apparaissent généralement ainsi en relief, au recto (ou face avant) de ladite carte. Le code de sécurité ou cryptogramme visuel est apposé au verso (ou face arrière) de la carte. L'utilisateur doit habituellement fournir ces données sécuritaires lorsqu'il réalise une transaction en ligne ou par téléphone,
- [4] Ce mode de paiement est aujourd'hui très largement répandu. Toutefois, malgré les efforts des banques, des e-commerçants et autres entreprises spécialisées dans la sécurité des cartes bancaires, les fraudes par piratage en ligne ou par téléphone, ou tout simplement par vol physique de la carte et du téléphone, de ces données sécuritaires se sont également fortement développées. A un moindre degré, le piratage visuel des données sécuritaires, par exemple, lors d'un paiement direct auprès d'un commerçant est aussi pratiqué. Ce peut être le cas du paiement d'un achat dans un magasin où le vendeur copie les données sécuritaires à l'insu du titulaire de la carte. Le pirate peut alors effectuer des transactions à distance, pour son propre compte en utilisant ces données sécuritaires, au détriment du propriétaire de la carte, ou revendre ces données à un tiers.

- [5] Certains dispositifs ont été développés pour tenter de mieux sécuriser les données des cartes bancaires.
- [6] Les documents brevets FR3051581 ou US 2014/0279555 proposent par exemple des solutions où le cryptogramme n'est plus une donnée statique imprimée sur la carte, mais une donnée dynamique générée par la carte au moment de la confirmation d'une transaction bancaire. Ce type de carte est toutefois particulièrement complexe à réaliser et coûteux. En outre, en cas de vol de la carte, le cryptogramme, même généré de manière dynamique, sera visible par le voleur au moment de la confirmation d'une transaction bancaire frauduleuse. Le cryptogramme changeant protège les données stockées par le e-commerçants. En cas de piratage, cette solution est donc uniquement pertinente pour des cas de hameçonnage (phishing en anglais) consistant en un vol des données stockées chez le e-commerçant par un hacker.
- [7] Le document brevet FR3051060 divulgue un procédé de sécurisation de cryptogramme. Plusieurs cryptogrammes sont imprimés sur la carte, édités et reconnus par la banque. Ces cryptogrammes doivent être utilisés dans un ordre prédéfini. Un repère déplaçable manuellement par rapport aux cryptogrammes, permet au propriétaire de la carte, selon un protocole personnel, de mettre en mémoire la position du cryptogramme qu'il devra utiliser pour la transaction suivante. Si cette solution peut être intéressante sous certains égards, elle présente des inconvénients. En effet, en cas de vol de la carte, le voleur connaîtra l'ensemble des cryptogrammes. Leur nombre étant limité, il suffit de « tester » successivement plusieurs cryptogrammes pour valider une transaction bancaire frauduleuse.
- [8] Le document US 2010/243741 divulgue un procédé de sécurisation conforme au préambule de la revendication principale. Les données occultées sont inscrites sur un support distinct de la carte. En combinant ce support à la carte, l'utilisateur peut retrouver l'ensemble des données sécuritaires. Le document US5326964 divulgue un procédé similaire. Ce type de procédé est relativement limité en termes de sécurisation.
- [9] Un objectif de l'invention est de remédier aux inconvénients de l'art antérieur. Un autre objectif de l'invention est de proposer une solution permettant de mieux

sécuriser les données sécuritaires d'une carte de paiement et de la rendre inutilisable en cas de vol.

Résumé de l'invention.

[10] La solution proposée par l'invention est un procédé de sécurisation des données sécuritaires d'une carte de paiement bancaire associée à un compte bancaire, lesquelles données sécuritaires sont statiques et comportent le numéro de ladite carte, des données d'identification du titulaire de ladite carte, la date d'expiration de ladite carte, et un cryptogramme, lequel numéro de carte bancaire et lequel cryptogramme sont constitués de plusieurs chiffres et/ou lettres.

Ce procédé comporte les étapes consistant à :

- n'inscrire que partiellement les données sécuritaires sur ladite carte de sorte que des données sécuritaires sont occultées, lesquelles données occultées étant formées par : plusieurs chiffres et/ou lettres du numéro de ladite carte et/ou au moins une donnée d'identification du titulaire et/ou au moins un élément de la date d'expiration et/ou au moins un chiffre et/ou lettre du cryptogramme,
- transmettre, au seul titulaire de la carte, un moyen de divulgation des données occultées.

Le procédé comporte en outre les étapes suivantes :

- cacher les données occultées parmi plusieurs données,
- arranger les données dans une grille,
- inscrire de manière visible la grille sur une face de la carte,
- transmettre, au seul titulaire de la carte, un révélateur des données occultées, lequel révélateur :
 - se présente sous la forme matérielle d'un cache ayant une forme complémentaire de la grille et comportant une série de fenêtres transparentes ou ajourées laissant uniquement apparaître les données occultées lorsque ledit cache coopère avec la grille, hormis lesdites fenêtres, le reste dudit cache étant opaque, ou
 - se présente sous la forme matérielle d'un support transparent ayant une forme complémentaire de la grille et comportant des éléments graphiques, lesquels éléments graphiques sont agencés et configurés pour mettre en exergue les données occultées lorsque ledit support est superposé à la grille,

ou

– se présente sous la forme virtuelle d'une image en réalité augmentée générée depuis une application informatique installée dans un terminal mobile du titulaire de la carte, laquelle image du révélateur est affichée sur un écran dudit terminal en se superposant à une image réelle de la grille également affichée sur ledit écran.

[11] Les données sécuritaires ne sont maintenant inscrites - de manière intelligible - que partiellement sur la carte de paiement bancaire. Aussi, si la carte venait à être dérobée, le voleur ne pourra jamais l'utiliser dans la mesure où il lui est impossible de connaître l'ensemble des données sécuritaires. Seul le titulaire de la carte connaît ces données sécuritaires. L'invention vise ainsi à créer un sas de sécurité, notamment avant toute transaction sur internet. En effet, pour effectuer un achat sur internet, il est nécessaire de renseigner certaines données sécuritaires que seul le porteur de la carte sera capable de fournir. En cas de vol de la carte, l'arrangement des données dans la grille rend le nombre de combinaison à « tester » pour valider une transaction bancaire frauduleuse très largement supérieur aux solutions connues de l'art antérieur (environ 10.000 fois plus nombreuse). Ainsi, l'invention sécurise fortement les cartes de paiement, afin de les rendre inutilisable lorsqu'elles sont récupérées frauduleusement par des individus mal intentionnés.

[12] D'autres caractéristiques avantageuses de l'invention sont listées ci-dessous. Chacune de ces caractéristiques peut être considérée seule ou en combinaison avec les caractéristiques remarquables définies ci-dessus, et faire l'objet, le cas échéant, d'une ou plusieurs demandes de brevet divisionnaires :

- Selon un mode de réalisation, le procédé comprend une étape consistant à générer l'image en réalité augmentée du révélateur sous la forme d'une image d'un cache dont la forme est complémentaire de l'image réelle de la grille et comportant une série de fenêtres laissant uniquement apparaître l'image réelle des données occultés lorsque l'image dudit cache est superposée à l'image de ladite grille.

- Selon un mode de réalisation, l'image en réalité augmentée du révélateur est générée sous la forme d'une image mettant en exergue l'image réelle des

données occultées lorsque ladite image en réalité augmentée est superposée à l'image de la grille.

- Advantageusement, le numéro de la carte est constitué de quatre séries de quatre chiffres, le procédé comprenant une étape consistant à occulter la deuxième et/ou la troisième série.
- Le procédé peut comprendre une étape consistant à ranger de manière aléatoire, ou de manière logique, les données occultées dans la grille.

[13] Un autre aspect de l'invention concerne un dispositif de sécurisation des données sécuritaires d'une carte de paiement bancaire associée à un compte bancaire, lesquelles données sécuritaires sont statiques et comportent le numéro de ladite carte, des données d'identification du titulaire de ladite carte, la date d'expiration de ladite carte, et un cryptogramme, lequel numéro de carte bancaire et lequel cryptogramme sont constitués de plusieurs chiffres et/ou lettres.

Le dispositif comprend également les caractéristiques suivantes :

- les données sécuritaires ne sont inscrites que partiellement sur la carte de sorte que des données sécuritaires sont occultés, lesquelles données occultées étant formées par : plusieurs chiffres et/ou lettres du numéro de ladite carte et/ou au moins une donnée d'identification du titulaire et/ou au moins un élément de la date, d'expiration et/ou au moins un chiffre et/ou lettre du cryptogramme,
 - le dispositif comporte un moyen de divulgation des données occultées.
 - les données occultées sont cachées parmi plusieurs données arrangées dans une grille, laquelle grille est inscrite de manière visible sur une face de la carte,
 - le dispositif comporte un révélateur des données occultées, lequel révélateur :
 - se présente sous la forme matérielle d'un cache ayant une forme complémentaire de la grille et comportant une série de fenêtres transparentes ou ajourées laissant uniquement apparaître les données occultés lorsque ledit cache coopère avec la grille, hormis lesdites fenêtres, le reste dudit cache étant opaque, ou
 - se présente sous la forme matérielle d'un support transparent ayant une forme complémentaire de la grille et comportant des éléments graphiques, lesquels éléments graphiques sont agencés et configurés pour mettre en exergue les données occultées lorsque ledit support est superposé à la grille,
- ou

-- se présente sous la forme virtuelle d'une image en réalité augmentée générée depuis une application informatique installée dans un terminal mobile du titulaire de la carte, laquelle image du révélateur est affichée sur un écran dudit terminal en se superposant à une image réelle de la grille également affichée sur ledit écran.

[14] Selon un mode de réalisation, l'image en réalité augmentée du révélateur se présente sous la forme d'une image d'un cache dont la forme est complémentaire de l'image réelle de la grille et comportant une série de fenêtres laissant uniquement apparaître l'image réelle des données occultées lorsque l'image dudit cache est superposée à l'image de ladite grille.

Selon un mode de réalisation, l'image en réalité augmentée du révélateur se présente sous la forme d'une image mettant en exergue l'image réelle des données occultées lorsque ladite image en réalité augmentée est superposée à l'image de la grille.

Selon un mode de réalisation, la grille comporte plusieurs cases contenant chacune un chiffre compris entre 0 et 9, chaque chiffre étant représenté une ou plusieurs fois dans ladite grille.

Brève description des figures.

[15] D'autres avantages et caractéristiques de l'invention apparaîtront mieux à la lecture de la description d'un mode de réalisation préféré qui va suivre, en référence aux dessins annexés, réalisés à titre d'exemples indicatifs et non limitatifs et sur lesquels :

[Fig. 1a] est une vue du recto (face avant) d'une carte conforme à l'invention, selon un mode de réalisation non couvert par les revendications,

[Fig. 1b] est une vue du verso (face arrière) de la carte de la figure 1a,

[Fig. 2a] est une vue du recto d'une carte conforme à l'invention, selon un autre mode de réalisation non couvert par les revendications,

[Fig. 2b] est une vue du verso de la carte de la figure 2a,

[Fig. 3a] est une vue du recto d'une carte conforme à l'invention, selon un autre mode de réalisation non couvert par les revendications,

[Fig. 3b] est une vue du verso de la carte de la figure 3a,

[Fig. 4a] est une vue du recto d'une carte conforme à l'invention, selon un autre mode de réalisation non couvert par les revendications,

[Fig. 4b] est une vue du verso de la carte de la figure 4a,

[Fig. 5a] est une vue du recto d'une carte conforme à l'invention, selon un autre mode de réalisation couvert par les revendications,

[Fig. 5b] schématise un cache utilisé pour découvrir les données occultées dans la carte de la figure 5a,

[Fig. 5c] montre la carte de la figure 5a combinée au cache de la figure 5b,

[Fig. 5d] schématise un autre type révélateur utilisé pour découvrir les données occultées dans la carte de la figure 5a,

[Fig. 5e] montre la carte de la figure 5a combinée au révélateur de la figure 5d,

[Fig. 6a] est une vue de face d'un terminal mobile utilisé pour la mise en œuvre du procédé selon un autre mode de réalisation couvert par les revendications,

[Fig. 6b] schématise une image réelle d'une carte de paiement bancaire affichée sur un écran du terminal mobile de la figure 6a,

[Fig. 6c] schématise une image virtuelle d'un révélateur affichée sur l'écran du terminal mobile de la figure 6b, laquelle image virtuelle est superposée à l'image réelle de la grille également affichée sur ledit écran,

[Fig. 6d] schématise une autre image virtuelle d'un révélateur affichée sur l'écran du terminal mobile de la figure 6b, laquelle image virtuelle est superposée à l'image réelle de la grille également affichée sur ledit écran.

Description des modes de réalisation.

- [16] Les figures annexées représentent une carte de paiement 1, ou carte bancaire (CB). La carte 1 est associée au compte bancaire de son titulaire. Elle se présente de manière classique sous la forme d'une carte plastique mesurant environ 86 mm × 54 mm. Elle est équipée au recto d'une puce électronique 2 à contacts affleurant, et au verso, éventuellement d'une bande magnétique 3. La puce 2 et/ou la bande 3 permettent le paiement, auprès de commerces

physiques possédant un terminal de paiement électronique ou auprès de commerce en ligne. Elle permet également des retraits d'espèces auprès de distributeurs automatiques de billets (DAB).

[17] La carte 1 est associée à des données sécuritaires. Ces données sécuritaires sont statiques, en ce sens qu'elles sont fixes et n'évoluent pas dans le temps. De façon connue, les données sécuritaires comportent le numéro 4 de la carte 1, des données d'identification 5 du titulaire de ladite carte, la date d'expiration 6 de ladite carte, et un cryptogramme 7. Le numéro 4, les données d'identification 5 et la date d'expiration 6 sont typiquement inscrite au recto de la carte 1, tandis que le cryptogramme 7 est inscrit au verso de ladite carte. Le numéro 4 est constitué de plusieurs séries de chiffres, par exemple 4 séries de 4 chiffres, soit 16 chiffres au total. Le numéro 4 peut également être constitué de plusieurs chiffres non arrangés en série, d'un code alphanumérique (combinaison de chiffres et de lettres), ou d'une série de lettres. Les données d'identification 5 comprennent typiquement le nom et le prénom du titulaire de la carte, ou le nom d'une société titulaire du compte bancaire associé à la carte 1. La date 6 est constituée de deux éléments, typiquement le mois d'expiration à deux chiffres (ex : 02 pour février) et l'année d'expiration à deux chiffres (ex : 25 pour 2025). Bien évidemment, le mois et/ou l'année pourrait être constituées de plus ou moins de chiffres et être associés à des lettres. Le cryptogramme 7 est constitué de plusieurs chiffres, typiquement 3 chiffres (ex : 432), mais peut être constitué d'un nombre supérieur (par exemple 4 chiffres) au inférieur (par exemple 2 chiffres). Le cryptogramme 7 peut également être constitué de chiffre(s) et/ou de lettre(s).

[18] Sur les figures 1a et 1b, on sécurise les données sécuritaires en n'inscrivant que partiellement sur la carte 1, le numéro 4. Au moins une série de chiffres est ici occultée de sorte qu'elle n'est jamais visible sur la carte 1. On occulte préférentiellement la deuxième et/ou la troisième série dans la mesure où la première série peut être commune à plusieurs cartes de paiement et la quatrième série apparaît généralement sur les tickets de caisse. Toutes les séries peuvent également être occultées. Les chiffres (et/ou lettres) occultés peuvent être remplacés par des croix (XXXX), des points, des tirets, etc. La deuxième et la troisième série peuvent être occultées en même temps. On peut également

envisager d'occulter un chiffre dans chaque série, de sorte qu'aucune des séries n'est inscrite complètement sur la carte 1.

- [19] Sur les figures 2a et 2b, on sécurise les données sécuritaires en n'inscrivant que partiellement sur la carte 1, l'identifiant 5 du titulaire. Le nom du titulaire (DUPONT) est ici occulté de sorte que seul le prénom (ERIC) est visible sur la carte 1. On peut également occulter le prénom de sorte qu'il ne soit jamais visible, seul le nom étant inscrit. On peut encore occulter le nom et le prénom du titulaire. Les données occultées peuvent être remplacées par des croix (XXXX), des points, des tirets, etc. Il est avantageux de pouvoir identifier le titulaire de la carte 1, alors même que le nom et/ou le prénom du titulaire sont occultés. Pour ce faire, le numéro de la carte d'identité ou de passeport du titulaire, peuvent être inscrit sur la carte 1. Un commerçant voulant s'assurer que la carte 1 appartient bien à son titulaire, pourra alors demander à ce dernier sa carte d'identité ou son passeport.
- [20] Sur les figures 3a et 3b, on sécurise les données sécuritaires en n'inscrivant que partiellement sur la carte 1, la date d'expiration 6. L'année est ici occultée de sorte qu'elle n'est jamais visible. Seul le mois est inscrit. On peut également occulter le mois de sorte qu'il ne soit jamais visible, seule l'année étant inscrite. On peut encore occulter le mois et l'année d'expiration. Les données occultées peuvent être remplacées par des croix (XXXX), des points, des tirets, etc.
- [21] Sur les figures 4a et 4b, on sécurise les données sécuritaires en n'inscrivant que partiellement sur la carte 1, le cryptogramme 7. Au moins un chiffre (et/ou lettre), avantageusement 2 chiffres (et/ou lettres) et préférentiellement l'ensemble des chiffres (et/ou lettres) du cryptogramme sont occultés. Les chiffres (et/ou lettres) occultés peuvent être remplacés par des croix (XXXX), des points, des tirets, etc.
- [22] Les modes de réalisations décrits précédemment peuvent se combiner, en ce sens qu'on peut occulter simultanément plusieurs éléments de données sécuritaires. Par exemple, on peut occulter tout ou partie du numéro 4 et tout ou partie du cryptogramme 7. On peut également occulter tout ou partie du numéro 4 et tout ou partie de la date d'expiration 6. Toutes les combinaisons possibles sont couvertes par la présente invention.

- [23] Dans la suite de la description, les éléments occultés des données sécuritaires sont dénommées « données occultées ». Les données sécuritaires de la carte 1 peuvent être enregistrées dans la puce 2 et/ou dans la bande magnétique 3. Pour éviter tout piratage, on prévoit préférentiellement de supprimer les données occultées de la puce 2 et/ou de la bande magnétique 3.
- [24] On communique au seul titulaire de la carte, un moyen de divulgation de ces données occultées. Ce moyen de divulgation peut consister en un document transmis par voie postale au titulaire de la carte 1 et sur lequel sont imprimées les données occultées. Pour sécuriser la communication des données occultées, ce document peut être un document scellé, envoyé dans un courrier distinct, ou joint à celui de l'envoi de la carte 1. Il peut s'agir du même document sur lequel est imprimé le code secret de la carte 1 (généralement un code à 4 chiffres) permettant de retirer de l'argent aux distributeurs et payer des commerçants. Le titulaire pourra alors mémoriser ou enregistrées ces données occultées qui seront connues de lui seul.
- [25] Pour retirer de l'argent aux distributeurs et payer des commerçants, le titulaire utilisera de manière classique le code secret de la carte 1. Pour des achats en lignes, il lui suffira de compléter les données sécuritaires requises par les données occultées. Ainsi, si le titulaire se fait dérober sa carte 1, le voleur ne pourra pas l'utiliser pour des achats frauduleux en ligne ou par téléphone, dans la mesure où il ne connaîtra jamais les données occultées. Le niveau de sécurité conféré par l'invention est tel qu'elle peut se substituer à l'authentification SMS-OTP généralement utilisée pour sécuriser les paiements en ligne. Le procédé d'authentification SMS-OTP est largement répandu et consiste à envoyer sur le téléphone mobile du titulaire, un SMS (pour Short Message Service) incluant un code à usage unique (OTP ou « One Time Password »). Ce code à usage unique doit être renseigné en plus des données sécuritaires pour valider une transaction en ligne.
- [26] Les figures 5a, 5b et 5c illustrent un mode de réalisation de l'invention couvert par les revendications.. Sur la figure 5a, les données occultées correspondent à la deuxième série de chiffres du numéro 4. Les chiffres occultés sont visibles mais cachés parmi plusieurs chiffres arrangés dans une grille 40. La grille 40 est

préférentiellement imprimée ou inscrite de manière visible sur le recto de la carte 1, au niveau du numéro 4 pour en simplifier l'usage. Elle pourrait toutefois être imprimée au verso.

- [27] Sur la figure 5a, la grille 40 comporte 25 cases contenant chacune un chiffre compris entre 0 et 9. La grille 40 peut avoir un nombre supérieur de cases, par exemple 100 cases contenant chacune un chiffre compris entre 0 et 9, chaque chiffre étant représenté 10 fois. La grille 40 peut également avoir un nombre inférieur de cases, par exemple 10 cases contenant chacune un chiffre compris entre 0 et 9, chaque chiffre étant représenté une seule fois. Les chiffres peuvent être disposés de manière aléatoire dans la grille 40, ou au contraire rangés de manière logique. La grille 40 est préférentiellement constituée de lignes et de colonnes. Le nombre de lignes est compris entre 0 et 10 et le nombre de colonne également compris entre 0 et 10. La grille 40 peut également être constituée d'un ou plusieurs cercles quadrillés concentriques dans lequel sont disposés les chiffres. Bien évidemment, si les données occultées du numéro 4 comporte des lettres, ces lettres pourront être intégrées dans la grille 40.
- [28] En se rapportant à la figure 5b, on fournit au titulaire révélateur permettant de révéler les données occultées, c'est-à-dire les chiffres manquants du numéro 4, dans la grille 40. Ce révélateur se présente sous la forme matérielle d'un cache 41 ayant une forme complémentaire de la grille 40 et comportant une série de fenêtre 410 transparentes ou ajourées. Hormis les fenêtres 410, le reste du cache est opaque. Le cache 41 peut être transmis dans un document scellé, envoyé dans un courrier distinct, ou joint à celui de l'envoi de la carte 1.
- [29] En se rapportant à la figure 5c, lorsque le cache 41 est positionné par dessus la grille 40, ou, en d'autres termes, qu'il coopère avec ladite grille, les fenêtres 410 laissent apparaître les chiffres occultés du numéro 4. L'association cache/grille s'apparente à la technique de cryptographie par grille de Cardan. Dans l'exemple illustré, la série 4321 est révélée, laquelle série correspondant aux données initialement occultées. Le titulaire pourra alors mémoriser ou enregistrer ces données occultées qui seront connues de lui seul. S'il ne se souvient pas des données occultées, le titulaire pourra également réutiliser le cache 41 pour les faire réapparaître.

[30] Dans la variante de réalisation de la figure 5d, le révélateur se présente sous la forme matérielle d'un support 41' transparent ayant une forme complémentaire de la grille 40. Ce support transparent 41' est par exemple réalisé en plastique. Il comporte des éléments graphiques 410' agencés et configurés pour mettre en exergue les données occultées lorsque ledit support est superposé à la grille 40. Sur la figure 5d, ces éléments graphiques 410' se présentent sous la forme de points positionnés sur la surface du support 41'. En se rapportant à la figure 5e, lorsque le support 41' est positionné par dessus la grille 40, les points sont positionnés dans les carreaux de ladite grille dans laquelle sont positionnées les données occultées du numéro 4. Les éléments graphiques 410' permettent donc de révéler uniquement les données occultées.

Les éléments graphiques 410' ne se présentent pas nécessairement sous la forme de points mais peuvent se présenter sous une autre forme, par exemple sous la forme d'une série de cercles entourant les chiffres 4-3-2-1 de la série occultés lorsque le support 41' coopère avec la grille 41.

Le support 41' peut être pourvu d'une marque indiquant la face à positionner contre la grille 40. De même, sur la figure 5d, le support 41' comprend de manière optionnelle une grille similaire à la grille 40, pour faciliter la mise en position dudit support sur ladite grille en faisant coïncider lesdites grilles.

[31] Les figures 6a, 6b, 6c et 6d illustrent un autre mode de réalisation de l'invention couvert par les revendications. Les données occultées correspondent à la deuxième série de chiffres du numéro 4. Les chiffres occultés sont visibles mais cachés parmi plusieurs chiffres arrangés dans une grille 40 comme dans le mode de réalisation des figures 5a à 5c.

[32] La mise en œuvre du procédé selon ce mode de réalisation fait appel à l'utilisation d'un terminal mobile 9 (figure 6a) se présentant préférentiellement sous la forme d'un téléphone mobile ou Smartphone du type iPhone®, Samsung Galaxy®, ou sous la forme d'un autre terminal électronique, fonctionnant avec un système d'exploitation de type Windows, Mac, iOS, Android, etc. Le terminal mobile 9 est celui du titulaire (utilisateur) de la carte 1,

[33] Le terminal mobile 9 comprend notamment, et de manière classique, un ou plusieurs processeurs ou microprocesseurs 90, une ou plusieurs mémoires 91,

une interface graphique 92 et un moyen d'acquisition optique 93, qui sont mutuellement connectés via un bus commun. Une ou plusieurs applications informatiques - ou programmes informatiques - sont stockées dans la ou les mémoires 91 et dont les instructions (ou codes), lorsqu'elles sont exécutées par le ou les processeurs 90 permettent de réaliser les fonctionnalités décrites plus avant dans la description.

- [34] Les données sécuritaires de la carte 1, et a minima les données occultées, sont préférentiellement préenregistrées dans la mémoire 90. Si l'utilisateur possède plusieurs cartes bancaires, les données sécuritaires de chaque carte, et a minima leurs données occultées sont préenregistrées dans la mémoire 90. Il est à noter que la mémoire 91 peut être une mémoire native du terminal 9, ou une mémoire déportée, par exemple intégrée dans un serveur informatique physiquement distant dudit terminal.
- [35] L'interface graphique 92 offre à l'utilisateur la possibilité de saisir, sélectionner et/ou entrer des données ou des instructions, et d'afficher des images acquises par le moyen d'acquisition optique 93. Il se présente par exemple sous la forme d'un écran tactile, d'un écran connecté à un clavier, etc.
- [36] Le moyen d'acquisition optique 93 se présente avantageusement sous la forme d'un lecteur optique, du type caméra et/ou appareil photo intégré dans le terminal mobile 9. Ce moyen d'acquisition optique 93 est associé à une application informatique de lecture.
- [37] L'utilisateur peut être amené à installer une application informatique dans son terminal mobile 9 pour mettre en œuvre tout ou partie de l'invention depuis ledit terminal et notamment l'affichage d'images en réalité augmentée. Cette application informatique peut être préinstallée sur le terminal 9. L'utilisateur a toutefois la possibilité de rechercher cette applications informatiques sur une boutique en ligne telles que Google Play®, Itunes® ou sur un site internet dédié, et ensuite la téléchargée sur son terminal 9.
- [38] Par souci de clarté, il faut comprendre au sens de l'invention que « *le terminal 9 fait quelque chose* » signifie « *l'application informatique exécutée par le processeur ou microprocesseur 90 du terminal 9 fait quelque chose* ». Tout

comme « *l'application informatique fait quelque chose* » signifie « *l'application informatique exécutée par le processeur ou microprocesseur 90 du terminal 9 fait quelque chose* ».

[39] En se rapportant à la figure 6b, l'utilisateur ouvre son application de lecture depuis son terminal mobile 9 et capture tout ou partie de l'image de la carte 1 avec le moyen d'acquisition optique 93. L'image réelle de la carte 1 s'affiche alors sur l'interface graphique 92 du terminal 9.

[40] Le terminal 9, au moyen d'une application de reconnaissance visuelle telle que Google Lens®, reconnaît que l'objet photographié est une carte bancaire et que cette carte comporte la grille 40.

Sur la base d'une reconnaissance optique de caractères de type OCR (acronyme de l'anglais Optical Character Recognition), le terminal 9 va analyser l'image de la grille 40 et plus particulièrement les chiffres qui y sont arrangés.

Le terminal 9 va rechercher dans la mémoire 91 les données occultées (ex : la série 4321) et rechercher dans l'image de la grille 40 ces données (ex chacun des chiffre 4-3-2-1).

Le terminal 9 va alors générée une image en réalité augmentée du révélateur et affichée cette image virtuelle sur l'écran 92 en la superposant à l'image réelle de la grille 40.

[41] Sur la figure 6c, l'image en réalité augmentée du révélateur se présente sous la forme d'une image d'un cache 941 dont la forme est complémentaire de l'image réelle de la grille 40. L'image du cache 941 comporte ici une série de fenêtres laissant uniquement apparaître l'image réelle des données occultés lorsque l'image dudit cache est superposée à l'image de ladite grille. Dans l'exemple sur la figure 6c, la série 4321 est révélée par l'image virtuelle du cache 941, laquelle série correspondant aux données initialement occultées.

[42] Sur la figure 6d, l'image en réalité augmentée du révélateur se présente sous la forme d'une image 941 mettant en exergue l'image réelle des données occultées lorsque ladite image en réalité augmentée est superposée à l'image de la grille 40. Cette image virtuelle est ici une série de cercles entourant l'image des chiffres 4-3-2-1 de la série occultés. Ces chiffres peuvent toutefois être mis

en exergue d'une autre façon, par exemple par une mise en surbrillance, ou avec un grossissement, ou en floutant les autres chiffres inscrits dans la grille 40, etc.

[43] En tout état de cause, l'image virtuelle générée peut inclure les données occultées qui s'affiche dans une zone graphique dédiée 942.

[44] Le système de grille et cache décrit en référence aux figures 5a, 5b, 5c, 6b, 6c, 6d s'applique de manière similaire aux données d'identification 5 (nom et/ou prénom du titulaire, auquel cas la grille 40 comporte une série de lettres), à la date d'expiration 6 et/ou au cryptogramme 7 et/ou le numéro de la carte d'identité ou de passeport du titulaire, ..., dans le cas où les données occultées font parties de ces éléments.

[45] L'agencement des différents éléments et/ou moyens et/ou étapes de l'invention, dans les modes de réalisation décrits ci-dessus, ne doit pas être compris comme exigeant un tel agencement dans toutes les implémentations. Notamment, une ou plusieurs caractéristiques exposées seulement dans un mode de réalisation peuvent être combinées avec une ou plusieurs autres caractéristiques exposées seulement dans un autre mode de réalisation.

Revendications

[Revendication 1] Procédé de sécurisation des données sécuritaires d'une carte de paiement bancaire (1) associée à un compte bancaire, lesquelles données sécuritaires sont statiques et comportent le numéro (4) de ladite carte, des données d'identification (5) du titulaire de ladite carte, la date d'expiration (6) de ladite carte, et un cryptogramme (7), lequel numéro de carte bancaire et lequel cryptogramme sont constitués de plusieurs chiffres et/ou lettres, ledit procédé comportant les étapes consistant à :

- n'inscrire que partiellement les données sécuritaires sur ladite carte de sorte que des données sécuritaires sont occultées, lesquelles données occultées étant formées par : plusieurs chiffres et/ou lettres du numéro (4) de ladite carte et/ou au moins une donnée d'identification (5) du titulaire et/ou au moins un élément de la date, d'expiration (6) et/ou au moins un chiffre et/ou lettre du cryptogramme (7),
- transmettre, au seul titulaire de la carte (1), un moyen de divulgation (41) des données occultées,

caractérisé en ce que ledit procédé comporte les étapes suivantes :

- cacher les données occultées parmi plusieurs données,
- arranger les données dans une grille (40),
- inscrire de manière visible la grille (40) sur une face de la carte (1),
- transmettre, au seul titulaire de la carte (1), un révélateur des données occultées, lequel révélateur :

-- se présente sous la forme matérielle d'un cache (41) ayant une forme complémentaire de la grille (40) et comportant une série de fenêtres (410) transparentes ou ajourées laissant uniquement apparaître les données occultées lorsque ledit cache coopère avec la grille (40), hormis lesdites fenêtres, le reste dudit cache étant opaque,

ou

-- se présente sous la forme matérielle d'un support transparent (41') ayant une forme complémentaire de la grille (40) et comportant des éléments graphiques (410'), lesquels éléments graphiques sont agencés et configurés pour mettre en exergue les données occultées lorsque ledit support est

superposé à la grille,

ou

-- se présente sous la forme virtuelle d'une image en réalité augmentée générée depuis une application informatique installée dans un terminal mobile (90) du titulaire de la carte (1), laquelle image du révélateur est affichée sur un écran dudit terminal en se superposant à une image réelle de la grille (40) également affichée sur ledit écran.

[Revendication 2] Procédé selon la revendication 1, consistant à générer l'image en réalité augmentée du révélateur sous la forme d'une image d'un cache (41') dont la forme est complémentaire de l'image réelle de la grille (40) et comportant une série de fenêtres (410') laissant uniquement apparaître l'image réelle des données occultées lorsque l'image dudit cache est superposée à l'image de ladite grille.

[Revendication 3] Procédé selon la revendication 1, consistant à générer l'image en réalité augmentée du révélateur sous la forme d'une image mettant en exergue l'image réelle des données occultées lorsque ladite image en réalité augmentée est superposée à l'image de la grille (40).

[Revendication 4] Procédé selon l'une des revendications précédentes, dans lequel le numéro (4) de la carte est constitué de quatre séries de quatre chiffres, le procédé comprenant une étape consistant à occulter la deuxième et/ou la troisième série.

[Revendication 5] Procédé selon l'une des revendications 1 à 4, comprenant une étape consistant à ranger de manière aléatoire les données occultées dans la grille (40).

[Revendication 6] Procédé selon l'une des revendications 1 à 4, comprenant une étape consistant à ranger de manière logique les données occultées dans la grille (40).

[Revendication 7] Dispositif de sécurisation des données sécuritaires d'une carte de paiement bancaire (1) associée à un compte bancaire, lesquelles données sécuritaires sont statiques et comportent le numéro (4) de ladite carte, des données d'identification (5) du titulaire de ladite carte, la date d'expiration (6) de ladite carte, et un cryptogramme (7), lequel numéro de carte bancaire et lequel cryptogramme sont constitués de plusieurs chiffres

et/ou lettres, et dans lequel :

- les données sécuritaires ne sont inscrites que partiellement sur la carte (1) de sorte que des données sécuritaires sont occultés, lesquelles données occultées étant formées par : plusieurs chiffres et/ou lettres du numéro (4) de ladite carte et/ou au moins une donnée d'identification (5) du titulaire et/ou au moins un élément de la date, d'expiration (6) et/ou au moins un chiffre et/ou lettre du cryptogramme (7),

- le dispositif comporte un moyen de divulgation (41) des données occultées, caractérisé en ce que :

- les données occultées sont cachées parmi plusieurs données arrangées dans une grille (40), laquelle grille est inscrite de manière visible sur une face de la carte (1),

- le dispositif comporte un révélateur des données occultées, lequel révélateur :

- se présente sous la forme matérielle d'un cache (41) ayant une forme complémentaire de la grille (40) et comportant une série de fenêtres (410) transparentes ou ajourées laissant uniquement apparaître les données occultés lorsque ledit cache coopère avec la grille (40), hormis lesdites fenêtres, le reste dudit cache étant opaque,

ou

- se présente sous la forme matérielle d'un support transparent (41') ayant une forme complémentaire de la grille (40) et comportant des éléments graphiques (410'), lesquels éléments graphiques sont agencés et configurés pour mettre en exergue les données occultées lorsque ledit support est superposé à la grille,

ou

- se présente sous la forme virtuelle d'une image en réalité augmentée générée depuis une application informatique installée dans un terminal mobile (9) du titulaire de la carte (1), laquelle image du révélateur est affichée sur un écran dudit terminal en se superposant à une image réelle de la grille (40) également affichée sur ledit écran.

[Revendication 8] Dispositif selon la revendication 7, dans lequel l'image en réalité augmentée du révélateur se présente sous la forme d'une image d'un

cache (41') dont la forme est complémentaire de l'image réelle de la grille (40) et comportant une série de fenêtres (410') laissant uniquement apparaître l'image réelle des données occultées lorsque l'image dudit cache est superposée à l'image de ladite grille.

[Revendication 9] Dispositif selon la revendication 7, dans lequel l'image en réalité augmentée du révélateur se présente sous la forme d'une image mettant en exergue l'image réelle des données occultées lorsque ladite image en réalité augmentée est superposée à l'image de la grille (40).

[Revendication 10] Dispositif selon l'une des revendications 7 à 9, dans lequel la grille (40) comporte plusieurs cases contenant chacune un chiffre compris entre 0 et 9.

[Revendication 11] Dispositif selon la revendication 10, dans lequel chaque chiffre est représenté plusieurs fois dans la grille (40).

[Revendication 12] Dispositif selon la revendication 10, dans lequel chaque chiffre est représenté une seule fois dans la grille (40).

[Revendication 13] Dispositif selon l'une des revendications 7 à 9, dans lequel les données occultées appartiennent à un numéro de carte d'identité ou passeport du titulaire de la carte (1), inscrit sur ladite carte.

1/7

Fig. 1a

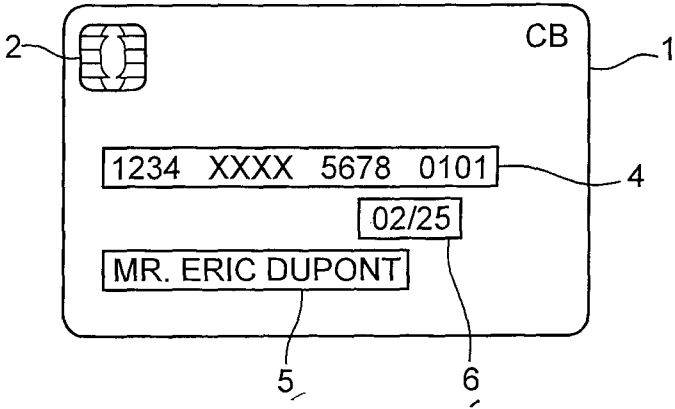


Fig. 1b

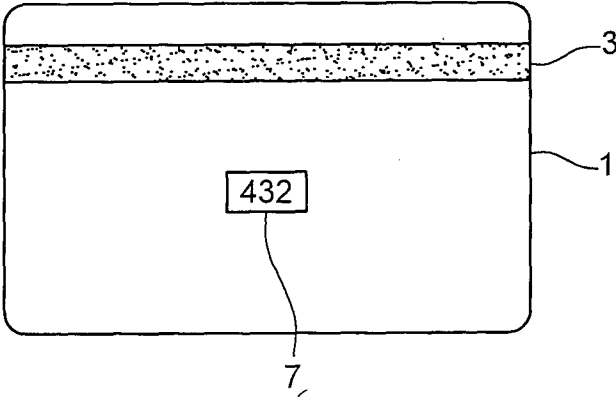


Fig. 2a

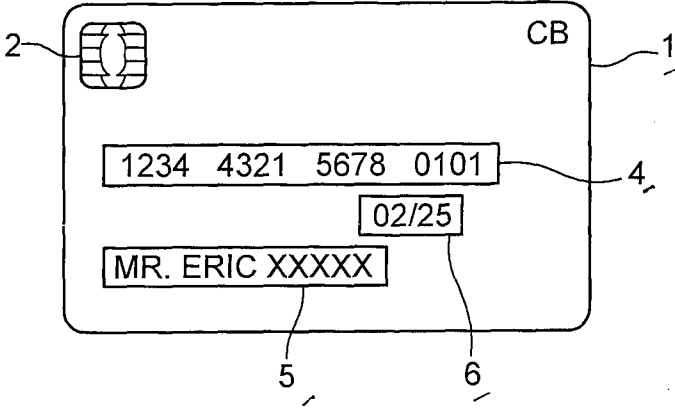
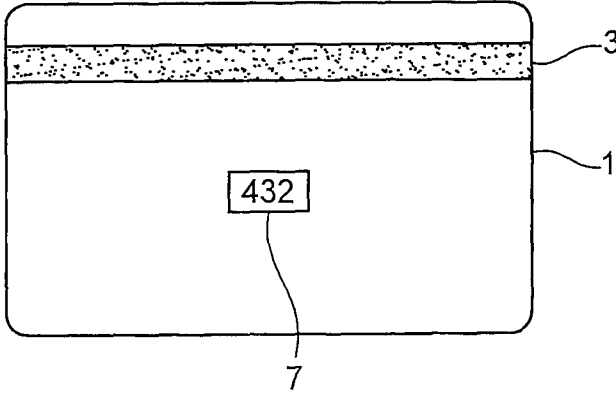


Fig. 2b



2/7

Fig. 3a

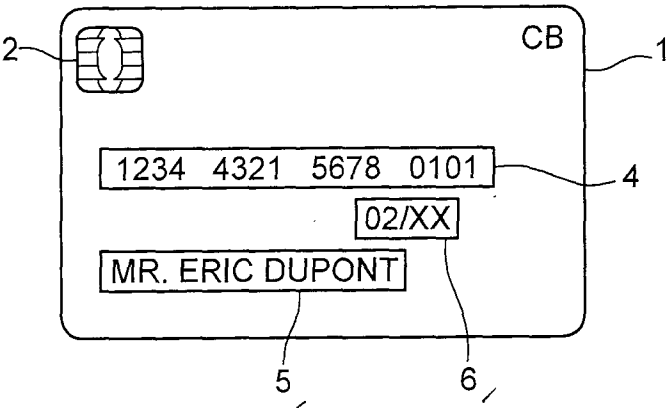


Fig. 3b

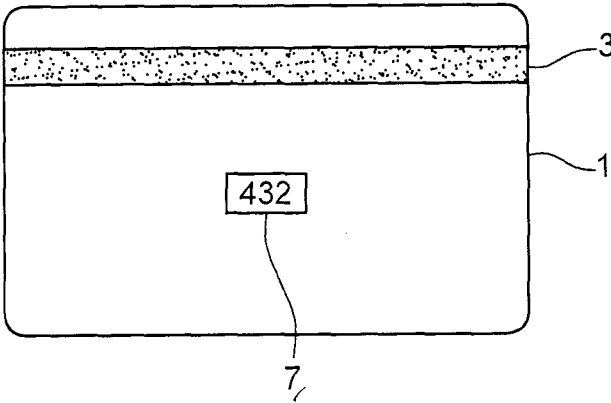


Fig. 4a

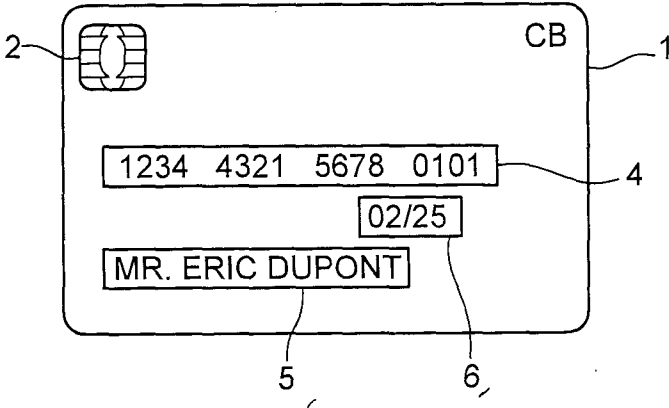
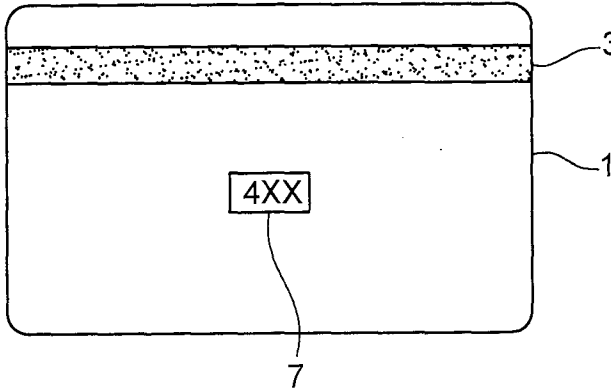


Fig. 4b



3/7

Fig. 5a

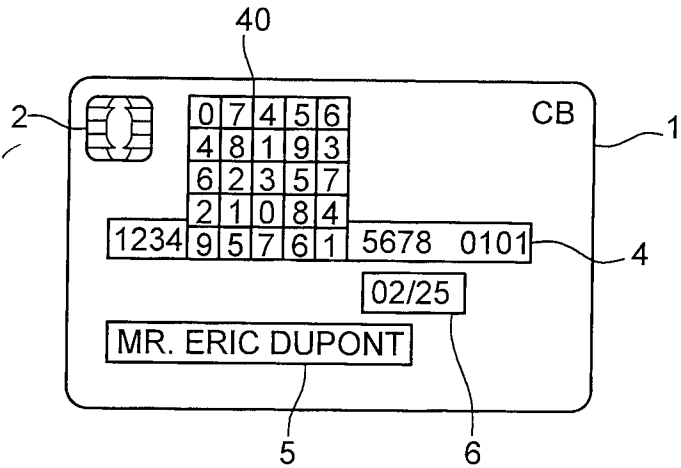


Fig. 5b

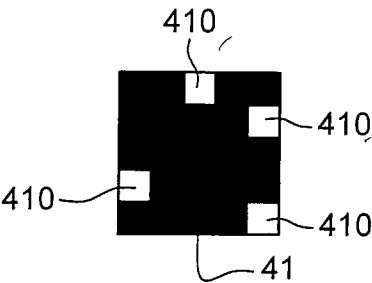


Fig. 5c

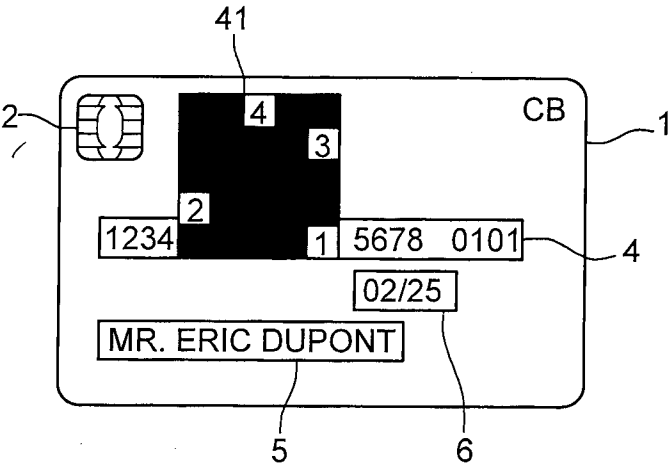
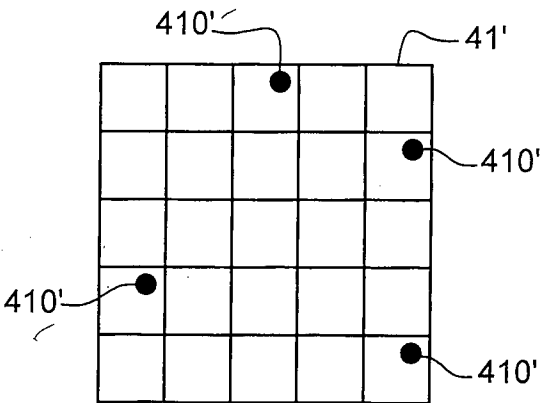


Fig. 5d



4/7

Fig. 5e

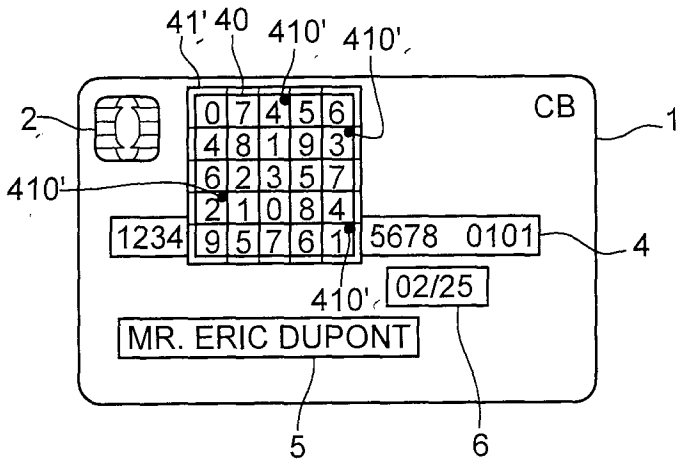
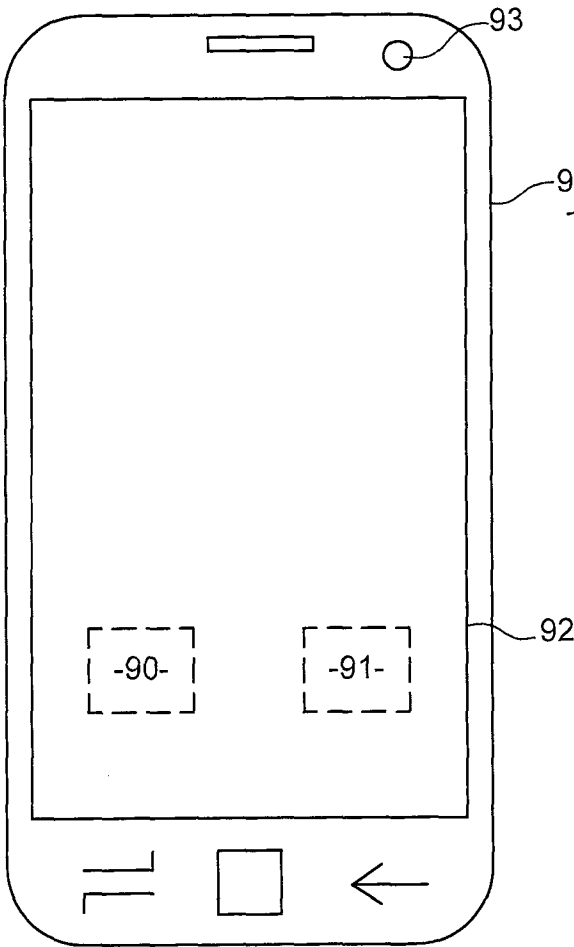
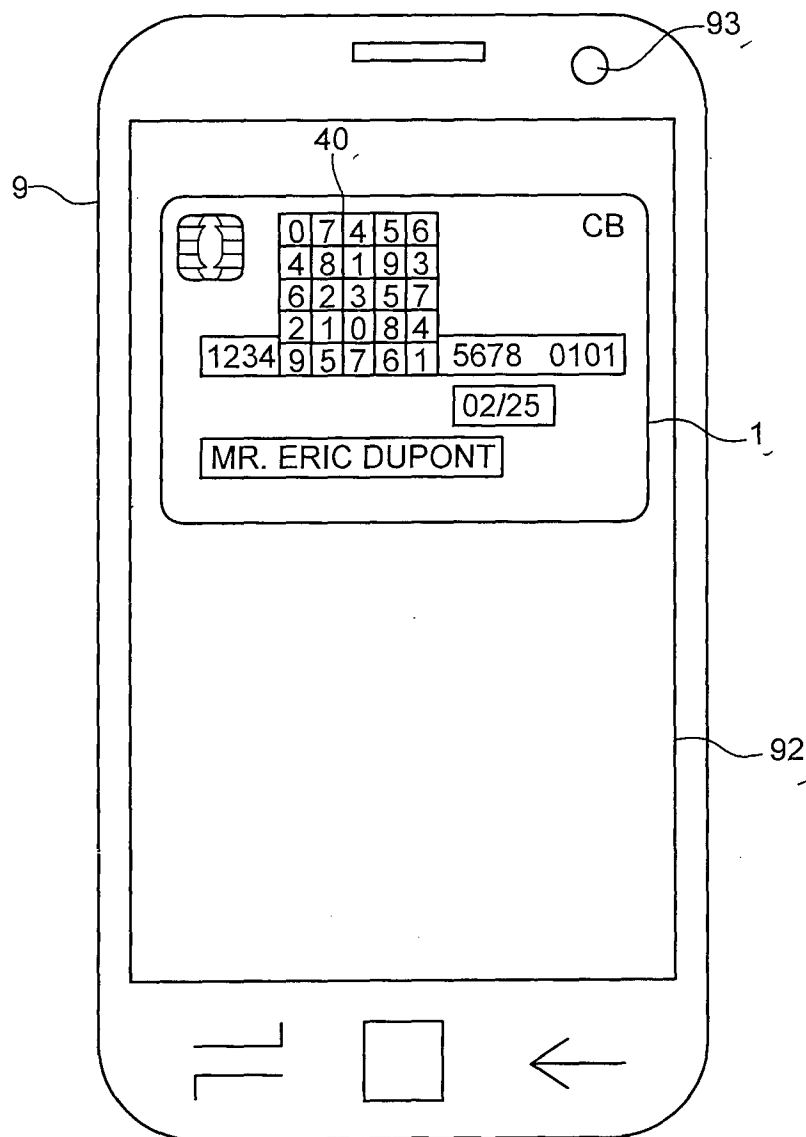


Fig. 6a



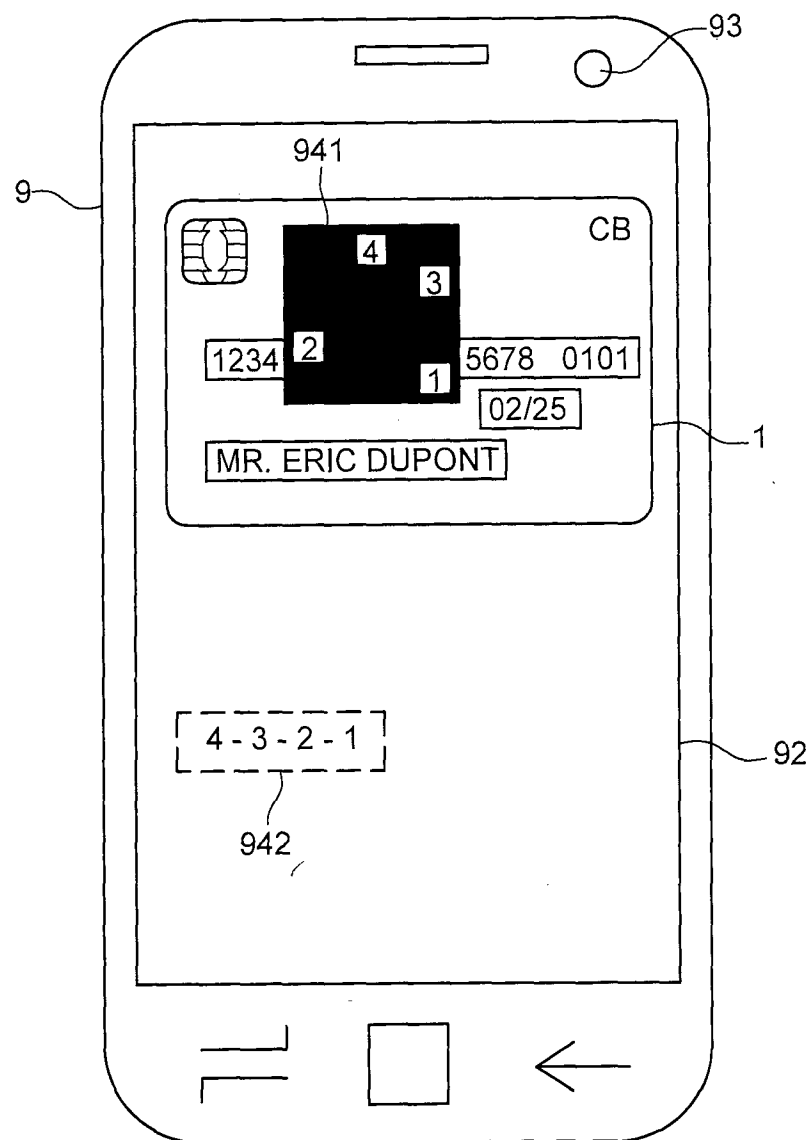
5/7

Fig. 6b



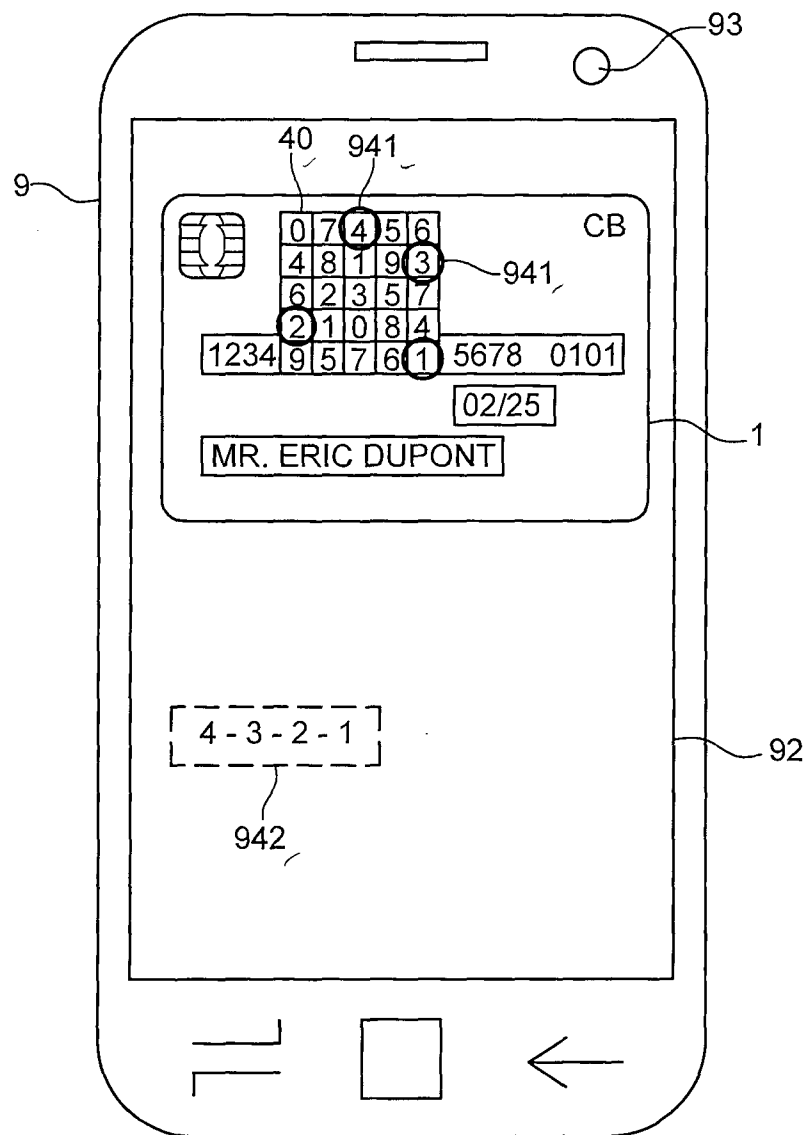
6/7

Fig. 6c



7/7

Fig. 6d



INTERNATIONAL SEARCH REPORT

International application No.

PCT/FR2019/051912

A. CLASSIFICATION OF SUBJECT MATTER**G06Q 20/34**(2012.01)i; **G07F 7/12**(2006.01)i; **G07F 7/08**(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q; G07F

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010243741 A1 (ENG U P PETER [US]) 30 September 2010 (2010-09-30) paragraph [0003] - paragraph [0044] figures	1-13
X	US 5326964 A (RISSER J MARLIN [US]) 05 July 1994 (1994-07-05) column 1, line 36 - column 4, line 69 figures	1-13
A	FR 2974756 A1 (SAIS CHRISTOPHE [FR]) 09 November 2012 (2012-11-09) page 3, line 7 - page 12, paragraph 25 figures	1-13
A	US 6826281 B1 (MENTRUP GEORGE S [US] ET AL) 30 November 2004 (2004-11-30) column 3, line 29 - column 6, line 8	1-13
A	WO 2008028215 A1 (WALKER MATTHEW [AU]) 13 March 2008 (2008-03-13) paragraph [0001] figures	1-13

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

02 October 2019

Date of mailing of the international search report

09 October 2019

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. (+31-70)340-2040

Facsimile No. (+31-70)340-3016

Authorized officer

Rachkov, Vassil

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FR2019/051912

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015161595 A1 (SEARS ROBERT KERN [US]) 11 June 2015 (2015-06-11) paragraph [0017] - paragraph [0036] figure 8	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/FR2019/051912

Patent document cited in search report				Publication date (day/month/year)		Patent family member(s)		Publication date (day/month/year)	
US	2010243741	A1	30 September 2010	US	2010243741	A1	30 September 2010		
				US	2013068366	A1	21 March 2013		
				US	2014203088	A1	24 July 2014		
				US	2016162766	A1	09 June 2016		
US	5326964	A	05 July 1994	NONE					
FR	2974756	A1	09 November 2012	NONE					
US	6826281	B1	30 November 2004	NONE					
WO	2008028215	A1	13 March 2008	AU	2006348113	A1	13 March 2008		
				CN	101536045	A	16 September 2009		
				EP	2062228	A1	27 May 2009		
				US	2009277968	A1	12 November 2009		
				WO	2008028215	A1	13 March 2008		
US	2015161595	A1	11 June 2015	NONE					

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2019/051912

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G06Q20/34 G07F7/12 G07F7/08 ADD.		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) G06Q G07F		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2010/243741 A1 (ENG U P PETER [US]) 30 septembre 2010 (2010-09-30) alinéa [0003] - alinéa [0044] figures -----	1-13
X	US 5 326 964 A (RISSER J MARLIN [US]) 5 juillet 1994 (1994-07-05) colonne 1, ligne 36 - colonne 4, ligne 69 figures -----	1-13
A	FR 2 974 756 A1 (SAIS CHRISTOPHE [FR]) 9 novembre 2012 (2012-11-09) page 3, ligne 7 - page 12, alinéa 25 figures -----	1-13
A	US 6 826 281 B1 (MENTRUP GEORGE S [US] ET AL) 30 novembre 2004 (2004-11-30) colonne 3, ligne 29 - colonne 6, ligne 8 ----- -/--	1-13
☒ Voir la suite du cadre C pour la fin de la liste des documents ☒ Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités:		
"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée	"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets	
Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale	
2 octobre 2019	09/10/2019	
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Rachkov, Vassil	

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 2008/028215 A1 (WALKER MATTHEW [AU]) 13 mars 2008 (2008-03-13) alinéa [0001] figures	1-13
A	----- US 2015/161595 A1 (SEARS ROBERT KERN [US]) 11 juin 2015 (2015-06-11) alinéa [0017] - alinéa [0036] figure 8 -----	1-13

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2019/051912

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2010243741 A1	30-09-2010	US 2010243741 A1	30-09-2010
		US 2013068366 A1	21-03-2013
		US 2014203088 A1	24-07-2014
		US 2016162766 A1	09-06-2016
US 5326964 A	05-07-1994	AUCUN	
FR 2974756 A1	09-11-2012	AUCUN	
US 6826281 B1	30-11-2004	AUCUN	
WO 2008028215 A1	13-03-2008	AU 2006348113 A1	13-03-2008
		CN 101536045 A	16-09-2009
		EP 2062228 A1	27-05-2009
		US 2009277968 A1	12-11-2009
		WO 2008028215 A1	13-03-2008
US 2015161595 A1	11-06-2015	AUCUN	