(19) ORGANISATION AFRICAINE DE LA PROPRIETE INTELLECTUELLE

(51) Inter. Cl.[8] G06K 19/06 (2019.01); G06Q 20/12 (2019.01); G06Q 20/32 (2019.01); G06Q 20/34 (2019.01); G06Q 20/40 (2019.01); G07F 7/08 (2019.01); G07F 7/12 (2019.01); H04W 12/06 (2019.01)

(11) N° 21548

FASCICULE DE BREVET D'INVENTION

(21) Numéro de dépôt : 1202300347
PCT/EP2022/054274

(22) Date de dépôt : 21/02/2022

(30) Priorité(s) :

FR n° FR2101800 du 24/02/2021

(24) Délivré le : 31/05/2024

(45) Publié le : 04.10.2024

(73) Titulaire(s) :

CCS12,
Bâtiment A3 - 3ème étage,
6 Allée Turcat Mery,
13008 MARSEILLE (FR)

(72) Inventeur(s) :
SMADJA, William (FR);
ABISDID, Marléne (FR)

(74) Mandataire : Cabinet EKANI-CONSEILS,
B.P. 5852, YAOUNDE (CM).

(54) **Titre : Carte de paiement, procédé d'authentification et d'utilisation pour un paiement à distance.**

(57) **Abrégé :**

L'invention concerne une carte de paiement (1) qui comporte sur une face (10, 11) au moins un cryptogramme d'authentification (3) comprenant un nombre de caractères compris entre 200 et 10 000, ce cryptogramme d'authentification (3) est unique et propriétaire de la carte de paiement (1), le cryptogramme d'authentification (3) étant apposé sur la carte de paiement (1), ce cryptogramme d'authentification (3) constitue un moyen d'identification de la carte de paiement (1) par reconnaissance optique, ce moyen d'identification étant lié à un compte bancaire auquel la carte de paiement (1) est liée. L'invention se rapporte aussi à un procédé d'authentification de la carte de paiement (1) et du porteur (100) de cette carte de paiement (1), ceci en vue de réaliser une opération sécurisée relative à des données personnelles du porteur (100) de la carte de paiement (1). Enfin l invention concerne une utilisation du procédé d'authentification pour effectuer un paiement à distance à l'aide de la carte de paiement (1).

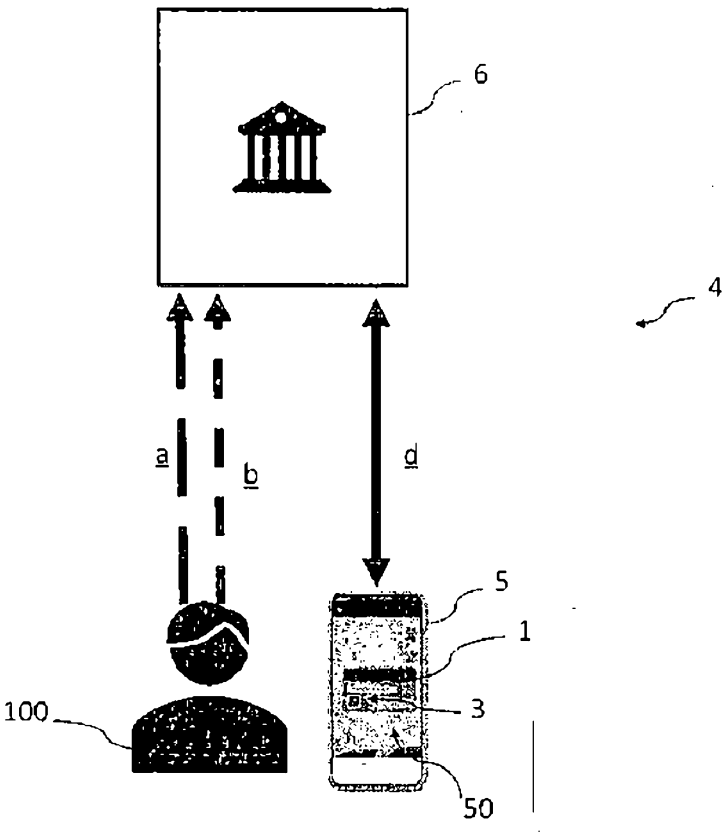


Fig. 6

Description

Titre de l'invention : Carte de paiement, procédé d'authentification et utilisation pour un paiement à distance

La présente invention entre dans le domaine de la sécurisation des transactions financières par carte bancaire, et plus particulièrement des paiements bancaires à distance opérés sur internet.

Pour rappel, une carte bancaire est une carte en matière plastique, voire en papier ou en carton, de quelques centimètres de côté et d'un à deux millimètres d'épaisseur. La carte porte classiquement au moins un circuit intégré capable de contenir de l'information. Ce circuit intégré correspond à la puce et peut contenir un microprocesseur capable de traiter cette information ou être limité à des circuits de mémoire non volatile et, éventuellement, un composant de sécurité tel qu'une carte mémoire.

Lors d'un paiement à distance par carte bancaire, il est nécessaire de renseigner les données « dites données sécuritaires » de la carte bancaire afin de procéder à la transaction financière.

Ces données sécuritaires sont généralement inscrites sur l'une ou l'autre des faces de cette carte à puce. Typiquement, une carte bancaire comprend des données d'identification d'un compte bancaire et/ou du propriétaire de la carte bancaire. Ces données d'identification sont généralement inscrites sur la face recto de la carte bancaire. Plus précisément, le numéro de carte, également appelé numéro PAN, est lié à un compte bancaire. En complément, la plupart des cartes bancaires comporte, d'une part, l'identité du titulaire de la carte bancaire (nom et prénom et/ou raison social). D'autre part, les organismes bancaires inscrivent également la date limite de validité de la carte de paiement.

Ces données d'identification d'un compte et/ou du propriétaire de la carte à puce sont généralement inscrites par impression ou en relief sur la face recto de la carte bancaire. Généralement, ces inscriptions sont réalisées par une technique d'embossage (face avant) de la carte à puce ou par sérigraphie.

La majorité des cartes bancaires comprennent aussi un code de sécurité ou un cryptogramme visuel apposé au verso (ou face arrière) de la carte bancaire.

En pratique, le propriétaire ou porteur de la carte bancaire est invité à fournir ces données d'identification lorsqu'il réalise un paiement en ligne ou par téléphone.

Depuis le début du XXIème siècle le commerce en ligne et plus généralement le paiement en ligne affichent une croissance quasi exponentielle du nombre de transactions mais aussi du volume financier de ces transactions.

Face à cette augmentation du volume de paiements en ligne, la question de la cybersécurité semble critique. En effet, en parallèle de cette augmentation des paiements en ligne on observe également une augmentation, des fraudes à la carte bancaire notamment au travers du piratage en ligne ou par téléphone.

Parmi ces nombreuses fraudes, on distingue deux types ; l'un avec usage de la carte bancaire, dit CP pour carte présente, l'autre sans carte dit CNP pour carte non présente. Une fraude du premier type implique un vol physique de la carte bancaire et le pirate, en possession de cette carte volée, disposant par ailleurs des données sécuritaires qui lui permettent d'usurper l'identité du porteur de la carte bancaire en vue de procéder à des paiements en ligne. Le piratage visuel des données sécuritaires, peut être aussi assimilé à ce premier type de fraude par usurpation d'identité. En effet, le piratage visuel intervient en principe lors d'un paiement en magasin, le vendeur copiant les données sécuritaires à l'insu du titulaire / porteur de la carte. Le pirate est alors en possession des données sécuritaires de la carte bancaire et peut effectuer des transactions à distance, soit pour son propre compte, soit pour les revendre à un tiers.

L'hameçonnage ou « phishing » constitue le deuxième type de fraudes à l'usurpation d'identité. Cette technique est sans doute celle qui s'est le plus développée ces dernières années. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance telle qu'une banque, une administration, ceci afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte d'identité, date de naissance, etc. Ceci peut être réalisé en reproduisant un site internet entier, par envoi d'un courriel ou encore par envoie d'un texto. Résultat, le pirate se retrouve en possession des données sécuritaires de la carte bancaire qui lui permettent également de réaliser des transactions pour son propre compte.

Pour prévenir ce type de fraudes, les organismes bancaires ont mis en place des procédés de sécurisation du paiement au travers de l'envoi d'un texto ou « sms » de confirmation de paiement sur le téléphone portable du porteur de la carte bancaire. Ce texto comprend généralement un code alphanumérique envoyé par l'organisme bancaire afin de valider le paiement. Ce service porte le nom authentification par « 3D-Secure® ». Bien que ce système apporte une certaine sécurité, il possède quelques failles qui permettent aux pirates de le contourner. Tout d'abord, toutes les banques ne proposent pas un tel service. De même, le système de paiement de tous les sites marchands ne permettent pas l'utilisation de ce procédé de sécurisation de la transaction financière. De sorte qu'à ce jour seules 40% de transactions en ligne françaises sont validées par ce système. Par ailleurs, ce système permet de changer le numéro de téléphone vers

lequel le code alphanumérique est envoyé. Une aubaine pour le pirate qui peut ainsi détourner l'envoi du code alphanumérique vers son propre téléphone portable.

Ces inconvénients ont poussé, dans une décision récente, la Commission Européenne à établir de nouvelles normes européennes plus strictes qui requièrent un niveau de sécurisation plus élevé en ce qui concerne les paiements en ligne. Le calendrier ambitieux de l'application de ces nouvelles normes visait une entrée en vigueur courant 2021, avec un inconvénient majeur, celui de laisser aux banques le choix des solutions avec le risque d'un défaut d'harmonisation.

Des solutions alternatives existent pour sécuriser les transactions. Par exemple, il existe un type de carte bancaire qui comporte un cryptogramme CVV dynamique. Le cryptogramme CVV correspond à la suite de trois chiffres qui se trouve généralement sur la face recto de la carte bancaire.

Le cryptogramme CVV est dit dynamique, puisque la série de trois chiffres évolue de manière aléatoire, automatiquement et à fréquence régulière. Ainsi, il est possible de confier sans crainte les informations d'une carte bancaire dynamique pour des transactions en ligne. En effet, même en cas de piratage par hameçonnage, les données sécuritaires de la carte bancaire seront inutilisables, puisque le cryptogramme change régulièrement.

La carte bancaire à cryptogramme dynamique n'est qu'une réponse partielle à la problématique de l'hameçonnage. Cependant, elle ne répond pas à la problématique de vol physique de la carte bancaire. Outre le fait que la technique embarquée sur une telle carte est une prouesse technologique, notamment au travers de l'intégration à la fois d'une batterie et d'un écran dans l'épaisseur de la carte, cette technologie est très couteuse et non écologique, ce qui retarde sa généralisation.

Il est à noter que la demanderesse propose déjà une solution pour lutter contre l'usurpation d'identité à la suite d'un vol physique de la carte bancaire et/ou de son piratage visuel. La solution propose d'intégrer un cryptogramme en lieu et place du trois chiffres du numéro PAN de la carte bancaire. Cette solution est notamment décrite dans le document WO 2020/120849. Bien qu'en possession de la carte bancaire, le pirate ne possède pas l'entièreté des données sécuritaires afin de procéder à des paiements en ligne pour son propre compte. En effet, le titulaire de ce type de carte de bancaire reçoit, d'une part, une carte bancaire dont une partie du chiffre PAN est masqué, et d'autre part, le numéro masqué. Ce numéro masqué peut être révélé par un procédé numérique également développé par la demanderesse a également fait l'objet d'un dépôt d'une demande de brevet français FR 20 05961.

Bien que cette solution d'encrypter le numéro PAN de la carte bancaire ait fait ses preuves contre le vol physique et/ou le piratage visuel d'une carte bancaire, elle ne

permet pas de prévenir un piratage par hameçonnage des données sécuritaires de la carte bancaire.

En conséquence, au jour de la rédaction de ce document, nous sommes forcés de constater que les organismes bancaires et les acteurs du commerce en ligne n'ont pas encore trouvés une solution idoine afin de sécuriser les transactions en ligne par carte bancaire.

Pour pallier ces inconvénients, la demanderesse a développé une solution technique qui vise à sécuriser le paiement en ligne au travers d'une double authentification assurant l'authentification de la carte bancaire et du titulaire de cette carte bancaire.

Un premier aspect de la présente invention concerne une carte de paiement comprenant une face recto et une face verso, la carte de paiement intègre aussi une puce électronique, la face recto comprenant des données sécuritaires qui incluent, au moins, un numéro PAN, une identité du porteur de la carte de paiement et une date limite de validité de la carte de paiement, la face verso possédant un cryptogramme CVV généralement constitué de trois chiffres.

La carte de paiement se caractérise en ce qu'elle comporte sur une face au moins un cryptogramme d'authentification comprenant un nombre de caractères compris entre 200 et 10 000, ce cryptogramme d'authentification est unique et propriétaire de la carte de paiement sur laquelle le cryptogramme d'authentification est apposé, ce cryptogramme d'authentification constitue un moyen d'identification de la carte de paiement par reconnaissance optique, ce moyen d'identification étant lié à un compte bancaire auquel la carte de paiement est liée.

La carte de paiement selon l'invention est équipée d'un cryptogramme d'authentification propriétaire qui est apposé sur une face de la carte de paiement. Ce cryptogramme d'authentification comporte un nombre important de caractère qui le rend unique. De fait, le cryptogramme d'authentification contribue à fournir un moyen d'authentification de la carte de paiement par reconnaissance optique du cryptogramme d'authentification. Ce cryptogramme d'authentification contribue à améliorer la sécurité d'opérations sécurisées, en limitant, les fraudes par hameçonnage. En effet, lorsqu'un pirate est parvenu à dérober les données sécuritaires de la carte de paiement, un procédé d'authentification selon l'invention requiert la validation de l'opération sécurisée par reconnaissance optique du cryptogramme d'authentification. Ainsi, si le pirate ne détient pas la carte de paiement et ses données sécuritaires, il ne peut pas utiliser la carte paiement à son profit.

Selon une deuxième caractéristique du premier aspect de l'invention, le cryptogramme d'authentification est un code matriciel constitué d'un nombre déterminé de modules noirs disposés dans un fond blanc de manière à former un motif unique,

chaque module noir constituant un caractère du cryptogramme d'authentification. Ce type de code matriciel fournit un grand nombre de combinaison qui permet à chaque carte de paiement de comporter un cryptogramme d'authentification unique encore appelé « propriétaire ».

Selon une troisième caractéristique du premier aspect de l'invention, le numéro PAN est constitué de quatre séries de quatre chiffres, la carte de paiement comprenant un cryptogramme PAN substituant au moins une série de quatre chiffres du numéro PAN. Le cryptogramme PAN fournit une sécurité supplémentaire qui permet de lutter contre le vol physique et/ou le piratage visuel de la carte de paiement. En effet, même en cas de vol physique et/ou de piratage visuel, le pirate ne détient pas l'intégralité du numéro PAN de la carte de paiement. Celle-ci est par conséquent inutilisable.

En particulier, le cryptogramme PAN comprend entre 16 et 100 caractères, de préférence, le cryptogramme PAN comprend entre 36 et 64 caractères. Selon l'invention, le cryptogramme PAN est une grille de cardan.

Selon une quatrième caractéristique du premier aspect de l'invention, le cryptogramme CVV peut être substitué par un cryptogramme possédant un nombre de caractères supérieur à trois. Cette caractéristique vise à également à masquer les données sécuritaires de la carte de paiement en vue de lutter contre le vol physique et/ou le piratage visuel de la carte de paiement.

Un deuxième aspect de l'invention concerne un procédé d'authentification d'une carte de paiement définie selon le premier aspect de l'invention, et du porteur de cette carte de paiement. Le procédé d'authentification vise à réaliser une opération sécurisée relative à des données personnelles du porteur de la carte de paiement. Dans cette optique, le procédé d'authentification comprend au moins :

a) Une première étape d'authentification de la carte de paiement par renseignement des données sécuritaires de la carte de paiement et/ou une première authentification du porteur de la carte paiement, le porteur de la carte de paiement renseignant son identité et/ou un identifiant ;

b) Une étape de requête d'une opération sécurisée relative à des données personnelles du porteur de la carte de paiement, la requête effectuée auprès d'un espace numérique sécurisé lié au compte bancaire de la carte de paiement ouvert auprès d'un organisme bancaire, l'espace numérique sécurisé étant stocké sur un serveur distant géré l'organisme bancaire ;

c) Une étape de vérification des données sécuritaires renseignées de la carte de paiement, cette étape étant effectuée par comparaison des données sécuritaires renseignées avec des données de références stockées sur l'espace numérique sécurisé ;

d) Une seconde étape d'authentification de de la carte de paiement et du porteur de la carte paiement, la seconde étape d'authentification étant opérée par reconnaissance du cryptogramme d'authentification propriétaire de la carte de paiement, cette étape étant réalisée au travers d'un module de reconnaissance numérique disponible ou accessible via un terminal numérique appartenant au porteur de la carte de paiement, et ;

e) Une étape de finalisation de l'opération sécurisée relative aux données personnelles du porteur de la carte de paiement.

Au travers des deux étapes d'authentification a) et d), le procédé selon l'invention intègre une double authentification de la carte de paiement et/ou du porteur de cette carte. Cette double authentification renforce la sécurisation d'une opération sécurisée telle qu'un paiement à distance. En effet, ce procédé implique de renseigner les données sécuritaires de la carte de paiement, mais aussi que se soit le porteur de cette carte qui effectue cette opération pour ouvrir le module de reconnaissance, et enfin que le porteur de la carte de paiement détienne sa carte de paiement pour le cryptogramme propriétaire de la carte de paiement soit reconnu. De fait, le procédé d'authentification rend le piratage par hameçonnage, tel qu'on le connait aujourd'hui, inefficace puisque ce type de piratage ne permet pas de récupérer le cryptogramme d'authentification propriétaire de la carte de paiement.

Selon une première caractéristique du deuxième aspect de l'invention, la seconde étape d'authentification d), est opérée par une ouverture d'un canal de communication sécurisé entre l'espace numérique sécurisé du compte bancaire et le terminal numérique du porteur de la carte de paiement, l'espace numérique sécurisé du compte bancaire appelant alors l'ouverture du module de reconnaissance numérique.

Selon une deuxième caractéristique du deuxième aspect de l'invention, le procédé d'authentification comporte, à l'ouverture du module de reconnaissance, une opération d'authentification biométrique et/ou codifiée du porteur de la carte de paiement, en cas de succès de l'authentification du porteur de la carte de paiement, le module de reconnaissance donne accès à une caméra du terminal numérique pour permettre une capture numérique du cryptogramme d'authentification de la carte de paiement.

Selon une troisième caractéristique du deuxième aspect de l'invention, le procédé comporte une comparaison du cryptogramme d'authentification apposé sur la carte de paiement, avec une image numérique de référence du cryptogramme d'authentification stockée dans l'espace numérique sécurisé du compte bancaire.

Selon une quatrième caractéristique du deuxième aspect de l'invention, lorsque l'étape de connexion a) est opérée sur un portail en ligne sécurisé distinct de l'espace numérique sécurisé 6, un canal de communication sécurisé est ouvert entre le portail en

ligne sécurisé et un espace numérique sécurisé et relié au compte bancaire de la carte de paiement.

Selon une cinquième caractéristique du deuxième aspect de l'invention, le procédé d'authentification comporte une étape de géolocalisation du terminal numérique du porteur de la carte de paiement.

Un troisième aspect de l'invention concerne une utilisation du procédé d'authentification défini selon le deuxième aspect de l'invention, pour opérer une validation de paiement à distance et notamment d'un paiement à distance réalisé via un site internet, le paiement à distance étant opéré au travers d'une carte de paiement définie selon le premier aspect de l'invention.

D'autres particularités et avantages apparaitront dans la description détaillée qui suit, de deux exemples de réalisation, non limitatifs, de l'invention illustrés par les figures 1 à 6 placées en annexe et dans lesquelles :

[Fig. 1] est une représentation d'une face recto d'une carte de paiement conforme de l'invention.

[Fig. 2] est une représentation d'une face verso de la carte de paiement de la figure 1.

[Fig. 3] est une représentation d'un terminal numérique recevant un appel d'un serveur bancaire en vue d'authentifier une carte de paiement.

[Fig. 4] est une représentation d'une étape de reconnaissance du cryptogramme d'authentification de la carte de paiement des figures 1 et 2.

[Fig. 5] est une représentation d'un système et d'un procédé d'authentification d'une carte de paiement conforme d'un premier exemple de réalisation de l'invention.

[Fig.6] est une représentation d'un système et d'un procédé d'authentification d'une carte de paiement conforme d'un second exemple de réalisation de l'invention.

Comme illustrée aux figures 1 à 5, l'invention concerne une carte de paiement 1. Cette carte de paiement 1 correspond à une carte bancaire. De fait, la carte de paiement 1 selon l'invention est reliée à un compte bancaire ouvert auprès d'un organisme bancaire. Le compte bancaire et la carte de paiement 1 sont attribués à un utilisateur encore appelé titulaire du compte bancaire, ou porteur 100 de la carte de paiement 1.

La carte de paiement 1 comprend une face recto 10 et une face verso 11. De manière classique, la carte de paiement 1 intègre aussi une puce électronique 12. Cette puce électronique 12 comprend un processeur et une mémoire configurées pour exécuter un algorithme et/ou stocker des données.

Comme cela est illustré à la figure 1, la face recto 10 comprend des données sécuritaires 2. Les données sécuritaires 2 incluent au moins un numéro PAN 20. Le numéro PAN 20 est composé de plusieurs séries de chiffres, par exemple quatre séries de quatre chiffres, soit seize chiffres au total. L'appellation PAN est courante dans le jargon bancaire. Dans cet exemple, en lisant la carte de paiement 1 de gauche à droite, le numéro PAN 20 comporte une première série 200 de chiffres, une deuxième série 201 de chiffres, une troisième série de chiffres et une quatrième série de chiffres 203.

Comme illustré à la figure 1, il est possible de substituer au moins une série de quatre chiffres du numéro PAN 20 par un cryptogramme PAN 21. Dans cet exemple, le cryptogramme PAN 21 substitue la troisième série de chiffres du numéro PAN 2. Toutefois, de manière alternative, il est possible que le cryptogramme PAN 21 substitue la quatrième série 203 de chiffres du numéro PAN 2.

Selon l'invention le cryptogramme PAN 21 comprend entre 16 et 100 caractères. De préférence, le cryptogramme PAN 21 comprend entre 36 et 64 caractères. Dans l'exemple de la figure 1, le cryptogramme PAN 21 est constitué par une grille de cardan. Néanmoins, il est tout à fait possible d'envisager l'utilisation d'un autre type de cryptogramme PAN 21 tel qu'un code barre simple ou un code barre matriciel.

Il est à noter que cette technique d'encryptage du numéro PAN utilisant la grille de cardan comme cryptogramme PAN 21 est décrite plus en détails dans la demande internationale WO 2020/120849 déposée par la demanderesse. En complément, un procédé de révélation numérique de la série de chiffre encryptée est décrit dans la demande de brevet français FR 20 05961 également déposée par la demanderesse. Comme cela est exposé dans la partie introductive, l'encryptage d'une série de chiffre du numéro PAN 21 permet de lutter efficacement contre les fraudes d'usurpation d'identité suite notamment à un vol physique de la carte de paiement.

Comme illustré à la figure 1, les données sécuritaires 2 comprennent également l'identité 22 du porteur 100 de la carte de paiement 1. De plus, les données sécuritaires 2 comportent une date limite 23 de validité de la carte de paiement 1.

Classiquement, les données sécuritaires 2, 20, 21, 22, 23 apposées sur la face recto 10 de la carte de paiement 1 sont inscrites par impression et/ou embossage, voire par sérigraphie à la surface de la carte de paiement 1. Dans cet exemple, à l'exception du cryptogramme PAN 21 qui est imprimé, les autres données sécuritaires 2, 20, 22, 23 sont apposées par embossage.

Comme illustré à la figure 2, la face verso 11 possède un cryptogramme CVV 24. Ce cryptogramme CVV 24 est généralement constitué de trois chiffres. De façon

optionnelle, il est également possible de substituer le cryptogramme CVV 24 par un cryptogramme possédant un nombre de caractères supérieur à trois. A titre informatif, un cryptogramme de type grille de cardan, code barre simple ou code barre matriciel peut être utilisé pour substituer le cryptogramme CVV 24.

Le cryptogramme CVV 24 fait également parti des données sécuritaires 2 de la carte de paiement 1. On parle de données sécuritaires puisque lors d'un paiement à distance, ces données sécuritaires 2 sont utilisées pour authentifier la carte de paiement 1 auprès de l'organisme de gestion bancaire.

Selon l'invention, la carte de paiement 1 comporte au moins un cryptogramme d'authentification 3. Il est unique et propriétaire de la carte de paiement 1. Ce cryptogramme d'authentification 3 constitue un moyen d'authentification de la carte de paiement 1 par reconnaissance optique. Il est relié au compte bancaire de la carte de paiement 1.

Le cryptogramme d'authentification 3 peut être apposé sur une face 10, 11 de la carte de paiement 1. Dans l'exemple de la figure 2, le cryptogramme d'authentification 3 est apposé sur la face verso 11. Toutefois, le cryptogramme d'authentification 3 pourrait également être disposé sur la face recto 10 de la carte de paiement 1.

Selon l'invention le cryptogramme d'authentification 3 comprend un nombre de caractères compris entre 200 et 10 000.

Dans l'exemple illustré aux figures 2, 4 et 5, le cryptogramme d'authentification 3 est constitué par un code matriciel. Le code matriciel est également appelé « code-barres bidimensionnel ». En pratique, le code matriciel est constitué d'un nombre déterminé de modules noirs disposés dans un fond blanc de manière à former un motif unique. Dès lors, chaque module noir constitue un caractère du cryptogramme d'authentification 3. Chaque module noir possède des dimensions déterminées. Ce type de code matriciel est connu sous le nom de « QR code® ». Le nombre élevé de caractère du cryptogramme 3 d'authentification lui confère son caractère unique.

Il est à noter que le cryptogramme 3 d'authentification pourrait être constitué par un autre type de cryptogramme visuel tel qu'un cryptogramme holographique, une grille de cardan, etc. L'avantage d'un cryptogramme de type data matrix, consiste en ce qu'il est d'ores et déjà susceptible d'être lu, reconnu par un smartphone et les applications bancaires actuelles.

Comme illustré aux figures 5 et 6, l'invention concerne aussi un système d'authentification 4 d'une carte de paiement 1 et du porteur 100. La double authentification du porteur 100 et de sa carte de paiement 1 contribue à réaliser une

opération sécurisée relative à des données personnelles du porteur 100 de la carte de paiement 1. Par exemple, l'opération sécurisée peut correspondre à un paiement à distance réalisé à l'aide de la carte de paiement 1 (figure 5). Cette double authentification est plus particulièrement utile pour un paiement à distance via internet. Toutefois, la double authentification peut également servir pour réaliser une signature numérique, opération sur un compte fidélité, un transfert de fonds bancaires etc.

Dans l'exemple des figures 5 et 6, le système d'authentification 4 comporte un terminal numérique 5. Le terminal numérique 5 peut consister en un « smartphone » ou téléphone portable intelligent, une tablette numérique etc. Plus largement, il est possible de mettre en œuvre l'invention avec un dispositif électronique équipé de moyens de visualisation tel qu'un écran, d'un outil de capture multimédia tel qu'un appareil photo ou une caméra, d'une mémoire et d'un processeur afin de stocker et exécuter des applications algorithmiques. Le dispositif électronique peut également comprendre des moyens de communications au travers d'un réseau de télécommunication tels qu'un réseau de téléphonie mobile, un réseau de téléphonie filaire, internet etc.

Selon l'invention, le terminal numérique 5 intègre un module de reconnaissance 50 du cryptogramme d'authentification 3 propriétaire de la carte de paiement 1. Le module de reconnaissance 50 est configuré pour une capture numérique du cryptogramme d'authentification 3. A ces fins, le module de reconnaissance 50 est intégré à un système applicatif configuré pour prendre le contrôle de la caméra du terminal numérique 5. A titre indicatif, le module de reconnaissance 50 peut être intégré à une application de gestion du compte bancaire lié à la carte de paiement 1. Cette application de gestion du compte bancaire est bien entendu stockée et exécutée par le terminal numérique 5. Il à noter qu'au jour de la rédaction de ce document, chaque organisme bancaire, met à disposition de ses clients, une application de gestion bancaire. Le module de reconnaissance 50 est donc une brique algorithmique qui peut s'ajouter à une application déjà préexistante ou correspondre à un algorithme applicatif à proprement parlé.

Le terminal numérique 5 est configuré pour communiquer à distance au travers d'un réseau de communication sans fil. A cet effet, le terminal numérique 5 peut comprendre des moyens de communication tels qu'un émetteur/récepteur de téléphonie mobile. A titre d'exemple, l'émetteur/récepteur peut être de type GSM, 2G, 3G, 4G, 5G, 6G. En complément, le terminal numérique 5 peut comprendre un émetteur/récepteur de champs proche, tel que Bluetooth, Wifi ou autre. Il est à noter que la plupart des terminaux numériques comprennent un émetteur/récepteur Wifi et un émetteur/récepteur

Bluetooth. Par ailleurs, les téléphones portables ou smartphones comprennent en sus un émetteur/récepteur de téléphonie mobile.

Comme illustré aux figures 5 et 6, le système d'authentification 4 selon l'invention comprend en outre un espace numérique sécurisé 6. L'espace numérique sécurisé 6 est relié au compte bancaire de la carte de paiement 1. De manière générale, l'espace numérique sécurisé 6 est géré par un organisme bancaire gérant ledit compte bancaire du porteur de la carte de paiement 1. L'espace numérique sécurisé 6 est stocké par un serveur distant. De manière connue, cet espace numérique sécurisé 6 est accessible à distance via des protocoles sécurisés, tels que l'appel de service. Cet appel de service est de même type que celui qui est utilisé par les terminaux de paiement électronique (TPE) pour effectuer des paiements bancaires à la suite de la lecture d'une carte de paiement bancaire.

Typiquement, un appel de service peut être sécurisé par un protocole sécuritaire de type APA, HTTPS, OAuth2.

L'espace numérique sécurisé 6 est également configuré pour ouvrir un canal de communication sécurisé utilisant un système de validation de paiement, de type PSP ou « Payment service provider » par exemple. Un tel système de validation de paiement PSP correspond à une interface de programmation d'application encore appelée « API ». L'API de ce système de validation de paiement est configurée pour ouvrir un canal de communication sécurisé entre l'espace numérique sécurisé 6 et le titulaire du compte bancaire, en vue de confirmer un paiement à distance. Dans cet exemple, le système de validation de paiement employé est configuré pour établir une communication sécurisée entre l'espace numérique sécurisé 6 et le terminal numérique 5 du porteur 100 de la carte de paiement 1 relié audit compte bancaire.

Dans l'exemple illustré à la figure 5, le système d'authentification 4 peut comprendre un portail en ligne 7 sécurisé. Le portail en ligne 7 est lui-même stocké sur un serveur distant qui est distinct du serveur bancaire. Dans cet exemple, le portail en ligne 7 est configuré pour communiquer avec le serveur distant stockant un espace numérique sécurisé 6 d'un compte bancaire. Lorsque le porteur 100 souhaite effectuer une opération de paiement en ligne, le portail en ligne 7 est un portail de paiement hébergé sur un site internet tel qu'un site marchand.

Selon l'invention, le portail en ligne 7 est configuré pour réaliser une opération sécurisée relative à des données personnelles du porteur 100 de la carte de paiement 1. Ladite opération sécurisée peut correspondre, comme décrit précédemment, à un paiement à

distance, une signature numérique, une opération sur un compte fidélité, un transfert de fonds bancaires etc.

Dans l'exemple de la figure 6, le portail en ligne 7 peut se confondre avec l'espace numérique sécurisé 6. Cette possibilité est plus spécifique d'une opération de transfert de fonds bancaire ou d'une opération sur une carte de fidélité. Dans cette configuration, le porteur 100 dialogue directement avec son terminal numérique 5 avec l'espace numérique sécurisé 6.

Ainsi, dans le cadre du système d'authentification 4, l'espace numérique sécurisé 6 est configuré pour communiquer à distance au travers d'un réseau de communication sans fil avec le terminal numérique 5 et/ou le portail en ligne 7.

Dans tous les cas, l'opération sécurisée relative aux données personnelles du porteur 100 est opérée après une double authentification de la carte de paiement 1 du porteur 100 de la carte de paiement 1. En pratique, le système d'authentification 4 implique une première authentification classique dans toutes opérations de paiement en ligne. Cette première authentification correspond, d'une part, à une authentification du porteur 100 par sa connexion à un espace numérique personnel. Cette authentification du porteur 100 comprend le renseignement d'un identifiant et d'un mot de passe ou encore une reconnaissance biométrique. D'autre part, la première authentification implique également un renseignement des données sécuritaires 20, 21, 22, 23, 24, 200, 201, 203 de la carte de paiement 1. Il est à noter que dans le présent exemple le numéro PAN 20 comporte un cryptogramme PAN 21. Lorsque le porteur 100 n'a pas en mémoire la série de chiffres substituée par le cryptogramme PAN 21, le porteur 100 peut révéler cette série de chiffres via un procédé de révélation décrit par la demande de brevet français FR 20 05961 également détenue par la demanderesse. Dans l'exemple de la figure 5, la première authentification est opérée par connexion à un portail en ligne 7. A l'inverse, dans l'exemple de figure 6, la première authentification est opérée directement auprès de l'espace numérique sécurisé 6 lié à la carte de paiement 1.

Dans un second temps, le système d'authentification 4 implique une seconde authentification. Cette seconde authentification se déroule au travers d'un canal de communication sécurisé ouvert entre l'espace numérique sécurisé 6 et le terminal numérique 5 du porteur 100 de la carte de paiement 1.

En pratique, cette seconde authentification correspond, d'une part, à une authentification du porteur 100 par renseignement d'un mot de passe ou par reconnaissance biométrique via le module de reconnaissance 50. Lorsque l'authentification du porteur 100 de la carte de paiement 1 est un succès, le module de

reconnaissance 50 opère une seconde authentification de la carte de paiement 1. Cette seconde authentification implique la lecture ou la capture du cryptogramme d'authentification 3 de la carte de paiement 1. De fait, cette double authentification conditionne la validation de l'opération sécurisée au fait que le porteur 100 détienne sa carte de paiement 1 lors de la validation de l'opération. En l'absence des données biométriques du porteur 100 ou du cryptogramme d'authentification 3, un pirate ne peut pas valider l'opération sécurisée. De plus, un niveau de sécurité supplémentaire est conféré par une carte de paiement 1 équipée d'un cryptogramme PAN 21.

L'invention concerne également un procédé d'authentification d'une carte de paiement 1 conforme de l'invention et du porteur 100 de cette carte de paiement 1. Cette authentification est réalisée afin de mener une opération sécurisée relative à des données personnelles du porteur 100 de la carte de paiement 1. Selon l'invention, ce procédé d'authentification peut être utilisé pour opérer une validation de paiement à distance et notamment d'un paiement à distance réalisé via un site internet. Néanmoins, le procédé selon l'invention peut également être utile pour effectuer une transaction financière, une opération sur un compte de fidélité, une signature numérique etc.

Comme illustré aux figures 5 et 6, le procédé d'authentification comprend une première étape d'authentification de la carte de paiement 1 et du porteur 100 de la carte paiement 1. Cette première étape d'authentification est nommée a). Lors de cette étape a), le porteur 100 renseigne les données sécuritaires 20, 21, 22, 23, 24, 200, 201, 203 de la carte de paiement 1. En pratique, l'étape a) peut aussi impliquer une authentification de l'identité du porteur 100 de la carte de paiement 1. Cette authentification est réalisée par connexion à un espace numérique sécurisé. La connexion implique le renseignement d'un identifiant accompagné d'un code d'accès et/ou d'une reconnaissance biométrique. La reconnaissance biométrique peut être digitale ou faciale. Cette fonctionnalité dépend des caractéristiques intégrées au terminal numérique 5 du porteur 100 de la carte de paiement 1.

Comme illustré aux figures 5 et 6, le procédé d'authentification comprend une étape de requête d'une opération sécurisée relative à des données personnelles du porteur 100 de la carte de paiement 1. L'étape de requête est notée b). Selon l'invention, la requête est effectuée auprès d'un espace numérique sécurisé 6 lié au compte bancaire de la carte de paiement 1. Ce compte bancaire est bien entendu ouvert auprès d'un organisme bancaire. Dans cet exemple, l'espace numérique sécurisé 6 est stocké sur un serveur distant géré par l'organisme bancaire. Comme décrit précédemment, l'espace numérique sécurisé 6 est accessible à distance au travers des moyens de télécommunication courant (internet, téléphonie mobile).

Le procédé d'authentification comporte une étape de vérification des données sécuritaires 20, 21, 22, 23, 24, 200, 201, 203 renseignées de la carte de paiement 1. Cette étape est notée c). L'étape de vérification c) est effectuée par comparaison des données sécuritaires 20, 21, 22, 23, 24, 200, 201, 203 renseignées avec des données de références stockées sur l'espace numérique sécurisé 6. Lorsque cette étape est un succès le procédé selon l'invention appelle une seconde authentification afin de valider l'opération relative à des données personnelles du porteur 100 de la carte de paiement 1.

A ces fins, le procédé d'authentification comporte une seconde étape d'authentification de la carte de paiement et du porteur de la carte paiement. Cette seconde étape d'authentification est notée d). Selon l'invention, la seconde étape d'authentification est opérée par reconnaissance du cryptogramme d'authentification 3 propriétaire de la carte de paiement 1.

Dans cet exemple, l'étape d) est réalisée au travers d'un module de reconnaissance 50 numérique disponible ou accessible par le terminal numérique 5 appartenant au porteur 100 de la carte de paiement 1. En pratique, la seconde étape d'authentification d), est opérée par une ouverture d'un canal de communication sécurisé entre l'espace numérique sécurisé 6 et le terminal numérique 5 du porteur 100 de la carte de paiement 1. Un tel canal de communication sécurisé peut utiliser un système PSP décrit précédemment. En pratique, l'espace numérique sécurisé 6 du compte bancaire appelle l'ouverture du module de reconnaissance 50 numérique sur le terminal numérique 5 du porteur 100 de la carte de paiement 1.

Comme illustré à la figure 3, à l'ouverture du module de reconnaissance 50, le procédé peut comprendre une opération d'authentification biométrique et/ou codifiée du porteur 100 de la carte de paiement 1. Dans cet exemple, une authentification biométrique par reconnaissance d'une empreinte digitale 51 est demandée. En cas de succès de l'authentification du porteur 100 de la carte de paiement 1, le module de reconnaissance 50 donne accès à une caméra du terminal numérique 5 pour permettre une capture numérique du cryptogramme d'authentification 3 propriétaire de la carte de paiement 1 (voir la figure 4). Ici, le module de reconnaissance 50 comprend un cadre 52 dans la carte de paiement 1 doit être placé au travers de l'écran du terminal numérique 5. Il est à noter que le module de reconnaissance 50 demande de scanner la carte de paiement 1.

La seconde étape d'authentification comprend une opération de comparaison du cryptogramme d'authentification 3 apposé sur la carte de paiement 1, avec une image numérique de référence du cryptogramme d'authentification. Cette image de référence est stockée dans l'espace numérique sécurisé 6 du compte bancaire. Lorsque l'image de

référence correspond au cryptogramme 3 apposé sur la carte de paiement, la seconde étape de d'authentification est considérée comme réussie.

En cas d'échec de la seconde étape d'authentification, l'opération sécurisée peut être avortée immédiatement, toutefois, le procédé peut permettre au porteur 100 de la carte de paiement de bénéficier d'un nombre déterminé d'essais de reconnaissance. Par exemple, il est possible de proposer trois essais de reconnaissance du cryptogramme d'authentification 3 avant que l'opération sécurisée ne soit interrompue par échec de la double authentification de la carte de paiement 1 et de l'identité de son porteur 100. En cas d'un premier échec, il est également possible de basculer vers des méthodes d'authentification plus classique tel que le système 3D sécure présenté en introduction de ce document.

Cependant en cas de succès de la seconde étape d'authentification d), le procédé d'authentification comprend une étape de finalisation de l'opération sécurisée relative aux données personnelles du porteur 100 de la carte de paiement 1. L'étape de finalisation est notée e). En pratique, l'étape de finalisation transmet les autorisations pour procéder à ladite opération sécurisée.

De manière additionnelle, le procédé d'authentification peut comporter une étape de géolocalisation du terminal numérique 5 du porteur 100 de la carte de paiement 1. La localisation du porteur 100 de la carte de paiement 1 peut donner une information quant à une tentative de fraude. En effet, si le terminal numérique 5 est localisé dans un Etat différent de celui dans lequel le compte bancaire a été ouvert, cela peut générer une alerte à l'attention du porteur 100. En pratique, le module de reconnaissance 50 est paramétré pour avoir accès aux données de localisation du terminal numérique 5. Alternativement, l'adresse IP du terminal de numérique 5 peut permettre de donner des informations sur la géolocalisation du porteur 100 de la carte de paiement 5.

En somme, cette géolocalisation a pour but de s'assurer que l'entrée des données sécuritaires 20, 21, 22, 23, 24, 200, 201, 203 de la carte de paiement 1 et la reconnaissance du cryptogramme d'authentification 3, en particulier du « QR code® » sont réalisées depuis le même endroit.

Selon un premier exemple de réalisation illustré à la figure 5, lorsque la première étape d'authentification a) est opérée à la suite d'une connexion à espace numérique sécurisé d'un portail en ligne 7 sécurisé distinct de l'espace numérique sécurisé 6, Cette possibilité est très courante, elle correspond à un achat réalisé par le porteur 100 de la carte de paiement 1 sur le portail en ligne 7 d'un site marchand. Selon cet exemple, le porteur 100 renseigne les données sécuritaires 20, 21, 22, 23, 24, 200, 201, 203 directement dans l'espace numérique sécurisé du portail en ligne 7.

L'étape de requête b) est réalisée au travers d'un canal de communication sécurisé qui est ouvert entre le portail en ligne 7 et l'espace numérique sécurisé 6. Ce canal peut être celui déjà utilisé entre un prestataire de service de paiement et une banque.

Dans cette situation, l'étape de finalisation e) s'opère également au travers de ce canal de communication sécurisé. Lorsque le portail en ligne 7 est un portail de paiement d'un site web marchand, l'étape de finalisation e) consiste à transmettre les autorisations de prélèvement entre l'organisme bancaire de la carte de paiement 1 et un organisme bancaire auquel est rattaché le portail de paiement. Le portail en ligne 7 peut également demander une signature numérique qui sera apportée au travers du procédé d'authentification de l'invention. Dans ce cas, l'étape de validation e) transmet une autorisation ou une signature numérique.

Selon un second exemple de réalisation du procédé illustré à la figure 6, la première étape d'authentification a) est opérée à la suite d'une connexion à l'espace numérique sécurisé 6 relié au compte bancaire de la carte de paiement 1. Selon cet exemple, le porteur 100 s'identifie auprès de l'espace numérique sécurisé 6. En pratique, le porteur 100 s'authentifie en renseignant son identité, via un identifiant. Cet identifiant est vérifié à l'aide d'un mot de passe et/ou par reconnaissance biométrique (digitale ou faciale).

Selon cet exemple, l'étape de requête b) est effectuée au sein de l'espace numérique sécurisé 6. Dans cette situation, l'étape de finalisation e) s'opère directement auprès de l'organisme bancaire, par exemple pour effectuer un mouvement bancaire interne, c'est-à-dire, entre deux comptes bancaires ouverts auprès du même organisme. Ces deux comptes bancaires peuvent appartenir au même porteur 100 ou à deux entités différentes. Alternativement, lorsqu'il s'agit d'une transaction financière entre deux organismes bancaires, l'étape de finalisation consiste à transférer les autorisations de prélèvement sur le compte bancaire du porteur 100 de la carte de paiement 1, vers un organisme bancaire bénéficiaire.

Revendications

[Revendication 1] Carte de paiement (1) comprenant une face recto (10) et une face verso (11), la carte de paiement (1) intègre aussi une puce électronique (12), la face recto (10) comprenant des données sécuritaires (2) qui incluent, au moins, un numéro PAN (20), une identité (22) du porteur de la carte de paiement (1) et une date limite de validité (23) de la carte de paiement (1), la face verso (11) possédant un cryptogramme CVV (24) généralement constitué de trois chiffres, caractérisée en ce qu'elle comporte sur une face (10, 11) au moins un cryptogramme d'authentification (3) comprenant un nombre de caractères compris entre 200 et 10 000, ce cryptogramme d'authentification (3) est unique et propriétaire de la carte de paiement (1), le cryptogramme d'authentification (3) étant apposé sur la carte de paiement (1), ce cryptogramme d'authentification (3) constitue un moyen d'identification de la carte de paiement (1) par reconnaissance optique, ce moyen d'identification étant lié à un compte bancaire auquel la carte de paiement (1) est liée.

[Revendication 2] Carte de paiement (1) selon la revendication 1, caractérisée en ce que le cryptogramme d'authentification (3) est un code matriciel constitué d'un nombre déterminé de modules noirs disposés dans un fond blanc de manière à former un motif unique, chaque module noir constituant un caractère du cryptogramme d'authentification (3).

[Revendication 3] Carte de paiement (1) selon l'une des revendications 1 ou 2, caractérisée en ce que le numéro PAN (20) est constitué de quatre séries de quatre chiffres, la carte de paiement (1) comprenant un cryptogramme PAN (21) substituant au moins une série de quatre chiffres du numéro PAN (20).

[Revendication 4] Carte de paiement (1) selon la revendication 3, caractérisée en ce que le cryptogramme PAN (21) comprend entre 16 et 100 caractères, de préférence, le cryptogramme PAN (21) comprend entre 36 et 64 caractères.

[Revendication 5] Carte de paiement (1) selon l'une des revendications 3 ou 4, caractérisée en ce que le cryptogramme PAN (21) est une grille de cardan.

[Revendication 6] Carte de paiement (1) selon l'une des revendications 1 à 5, caractérisée en ce que le cryptogramme CVV (24) est substitué par un cryptogramme possédant un nombre de caractères supérieur à trois.

[Revendication 7] Procédé d'authentification d'une carte de paiement (1) définie selon l'une des revendications 1 à 7, et du porteur (100) de cette carte de paiement (1), ceci en vue de réaliser une opération sécurisée relative à des données personnelles du porteur (100) de la carte de paiement (1), caractérisé en ce que le procédé d'authentification comprend au moins :

a) une première étape d'authentification de la carte de paiement (1) par renseignement des données sécuritaires (2, 20, 200, 201, 203, 22, 23) de la carte de paiement (1) et/ou une première authentification du porteur (100) de la carte paiement (1), le porteur (100) de la carte de paiement (1) renseignant son identité et/ou un identifiant ;

b) une étape de requête d'une opération sécurisée relative à des données personnelles du porteur (100) de la carte de paiement (1), la requête effectuée auprès d'un espace numérique sécurisé (6) lié au compte bancaire de la carte de paiement (1) ouvert auprès d'un organisme bancaire, l'espace numérique sécurisé (6) étant stocké sur un serveur distant géré l'organisme bancaire ;

c) une étape de vérification des données sécuritaires renseignées de la carte de paiement (1), cette étape étant effectuée par comparaison des données sécuritaires (2, 20, 200, 201, 203, 22, 23) renseignées avec des données de références stockées sur l'espace numérique sécurisé (6) ;

d) une seconde étape d'authentification de la carte de paiement (1) et du porteur (100) de la carte paiement (1), la seconde étape d'authentification étant opérée par reconnaissance du cryptogramme d'authentification (3) propriétaire de la carte de paiement (1), cette étape étant réalisée au travers d'un module de reconnaissance (50) numérique disponible ou accessible via un terminal numérique (5) appartenant au porteur (100) de la carte de paiement (1), et

e) une étape de finalisation de l'opération sécurisée relative aux données personnelles du porteur (100) de la carte de paiement (1).

[Revendication 8] Procédé d'authentification selon la revendication 7, caractérisé en ce que, la seconde étape d'authentification d), est opérée par une ouverture d'un canal de communication sécurisé entre l'espace numérique sécurisé (6) du compte bancaire et le terminal numérique (5) du porteur (100) de la carte de paiement (1), l'espace numérique sécurisé (6) du compte bancaire appelant alors l'ouverture du module de reconnaissance (50) numérique.

[Revendication 9] Procédé d'authentification selon l'une des revendications 7 ou 8, caractérisé en ce qu'il comporte, à l'ouverture du module de reconnaissance (50), une opération d'authentification biométrique et/ou codifiée du porteur (100) de la carte

de paiement (1), en cas de succès de l'authentification du porteur (100) de la carte de paiement (1), le module de reconnaissance donne accès à une caméra du terminal numérique (5) pour permettre une capture numérique du cryptogramme d'authentification (3) de la carte de paiement (1).

[Revendication 10] Procédé d'authentification selon l'une des revendications 7 à 9, caractérisé en ce qu'il comporte une comparaison du cryptogramme d'authentification (3) apposé sur la carte de paiement (1), avec une image numérique de référence du cryptogramme d'authentification (3) stockée dans l'espace numérique sécurisé (6) du compte bancaire.

[Revendication 11] Procédé d'authentification selon l'une des revendications 7 à 10, caractérisé en ce que, lorsque l'étape de connexion a) est opérée sur un portail en ligne (7) sécurisé distinct de l'espace numérique sécurisé (6), un canal de communication sécurisé est ouvert entre le portail en ligne (7) sécurisé et un espace numérique sécurisé (6) et relié au compte bancaire de la carte de paiement (1).

[Revendication 12] Procédé d'authentification selon l'une des revendications 7 à 11, caractérisé en ce qu'il comporte une étape de géolocalisation du terminal numérique (5) du porteur (100) de la carte de paiement (1).

[Revendication 13] Utilisation du procédé d'authentification défini selon l'une des revendications 7 à 12, pour opérer une validation de paiement à distance et notamment d'un paiement à distance réalisé via un site internet, le paiement à distance étant opéré au travers d'une carte de paiement (1) définie selon l'une des revendications 1 à 6.

Abrégé

Titre : Carte de paiement, procédé d'authentification et utilisation pour un paiement à distance

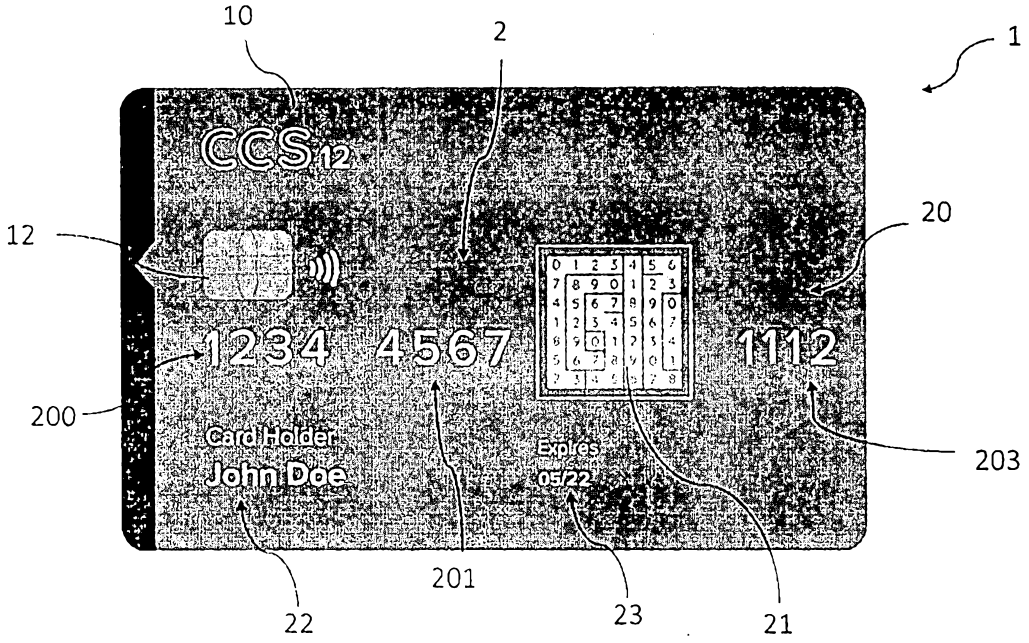
L'invention concerne une carte de paiement (1) qui comporte sur une face (10, 11) au moins un cryptogramme d'authentification (3) comprenant un nombre de caractères compris entre 200 et 10 000, ce cryptogramme d'authentification (3) est unique et propriétaire de la carte de paiement (1), le cryptogramme d'authentification (3) étant apposé sur la carte de paiement (1), ce cryptogramme d'authentification (3) constitue un moyen d'identification de la carte de paiement (1) par reconnaissance optique, ce moyen d'identification étant lié à un compte bancaire auquel la carte de paiement (1) est liée.

L'invention se rapporte aussi à un procédé d'authentification de la carte de paiement (1) et du porteur (100) de cette carte de paiement (1), ceci en vue de réaliser une opération sécurisée relative à des données personnelles du porteur (100) de la carte de paiement (1).

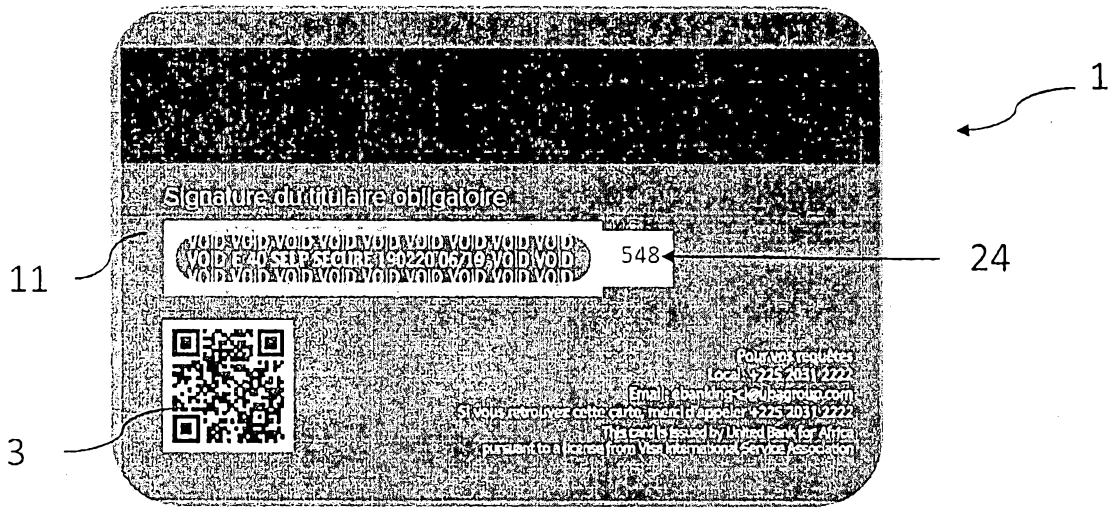
Enfin l'invention concerne une utilisation du procédé d'authentification pour effectuer un paiement à distance à l'aide de la carte de paiement (1).

Figure pour l'abrégé : Fig.6]

[Fig. 1]

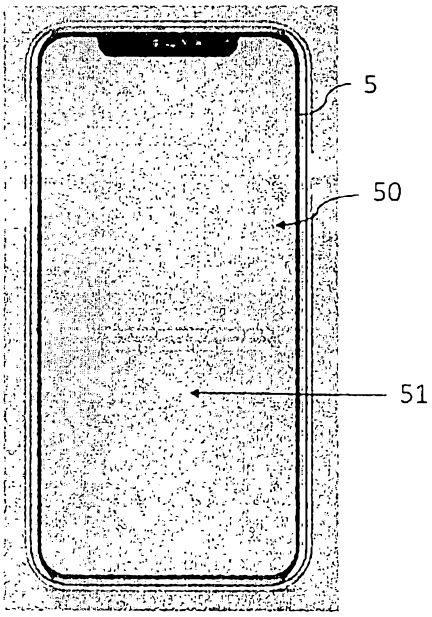


[Fig. 2]

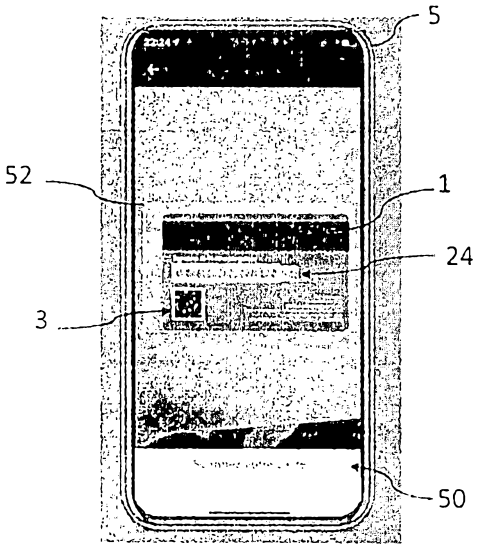


DUPLICATA

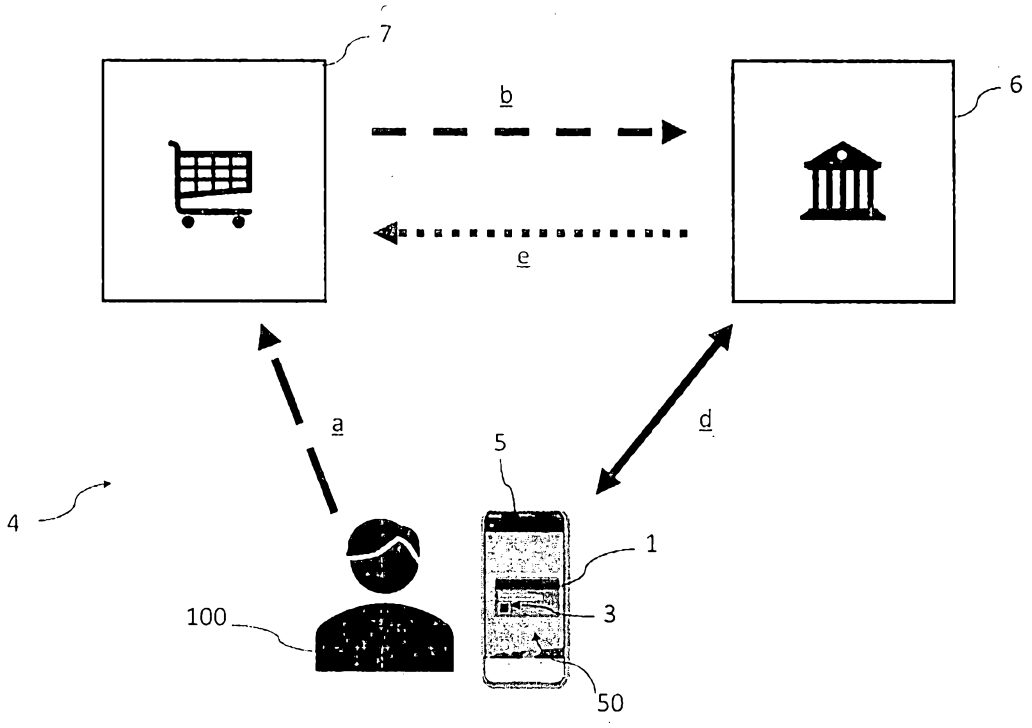
[Fig. 3]



[Fig. 4]



[Fig. 5]



[Fig. 6]