Code de distribution interne :

(A) [-] Publication au JO
(B) [-] Aux Présidents et Membres
(C) [-] Aux Présidents
(D) [X] Pas de distribution

Liste des données pour la décision du 23 novembre 2023

N° du recours : T 0988/20 - 3.5.01

N° de la demande : 15714526.9

N° de la publication : 3132399

C.I.B. : G06Q20/02, G06Q20/32, G06Q20/34

Langue de la procédure : FR

Titre de l'invention :

PROCÉDÉ DE TRAITEMENT DE DONNÉES TRANSACTIONNELLES, DISPOSITIF ET PROGRAMME CORRESPONDANT

Demanderesse :

Banks and Acquirers International Holding

Référence :

Procédé de traitement de données transactionelles/BANKS AND ACQUIRERS INTERNATIONAL HOLDING

Normes juridiques appliquées :

CBE Art. 56

Mot-clé :

Activité inventive - émulation d'une carte de paiement virtuelle dans éspace sécurisé sur un serveur (oui - solution non évidente)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

N° du recours : T 0988/20 - 3.5.01

D E C I S I O N
de la Chambre de recours technique 3.5.01
du 23 novembre 2023

Requérante : (Demanderesse)	Banks and Acquirers International Holding 28-32 boulevard de Grenelle 75015 Paris (FR)
Mandataire :	Germain Maureau 12, rue Boileau 69006 Lyon (FR)
Décision attaquée :	**Décision de la division d'examen de l'Office européen des brevets postée le 5 décembre 2019 par laquelle la demande de brevet européen n° 15714526.9 a été rejetée conformément aux dispositions de l'article 97(2) CBE.**

Composition de la Chambre :

Président	W. Chandler
Membres :	N. Glaser
	L. Basterreix

Exposé des faits et conclusions

I. Le recours a été formé par la requérante contre la décision par laquelle la division d'examen a rejeté la demande de brevet européen n° 15714526.9.

II. La demande de brevet a été refusée sous forme d'une décision en l'état du dossier pour défaut d'activité inventive (article 56 CBE) et également pour défaut de clarté (article 84 CBE). Les raisons sont motivées dans les notifications de la division d'examen en date du 18 novembre 2019 (protocole d'une conversation téléphonique) et du 5 juin 2019 (convocation à une procédure orale).

III. La requérante demande que la décision de rejet de la demande soit révisée et qu'un brevet soit délivré sur la base des revendications déposées le 15 avril 2020, qui correspondent à celles qui ont été refusées par la division d'examen.

La requérante a soumis le document "What is a secure element?" (D9), extrait de l'internet, 15 avril 2020.

IV. La procédure orale devant la chambre s'est tenue le 23 novembre 2023 par visioconférence. A la fin de la procédure orale le président de la chambre a prononcé la décision.

V. La revendication 1 de la requête principale est rédigée ainsi :

"1. Procédé de traitement de données transactionnelles représentatives d'un paiement effectué par un

utilisateur à partir d'un terminal de communication (TC), procédé caractérisé en ce qu'il comprend :
- une étape de chargement (10) d'un terminal de paiement virtuel (vPos), au sein d'un premier espace mémoire sécurisé (SecSpacel) du terminal de communication (TC), ledit terminal virtuel (vPos) se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé du terminal de communication (TC) ;

- une étape de chargement (20), au sein d'un deuxième espace sécurisé (SecSpace2) situé sur un serveur (SrvVCB) connecté au terminal de communication (TC) par l'intermédiaire d'un réseau de communication (Ntwk), d'au moins une carte de paiement virtuelle (vCB), ladite carte de paiement virtuelle (vCB) étant instanciée par un module logiciel d'émulation (modEmul) mis en oeuvre sous la forme d'une exécution d'une machine virtuelle;

- une étape de traitement (30) par le terminal de paiement virtuel (vPos) d'une transaction de paiement, ladite étape de traitement comprenant :

- une étape d'échange de commandes ADPU entre ledit terminal de paiement virtuel (vPos) et ladite au moins une carte de paiement virtuelle (vCB) ;

- une étape de construction de ladite transaction de paiement selon les protocoles SEPA et/ou EMV, pour la mise en oeuvre dudit paiement."

Motifs de la décision

1. L'invention

1.1 L'invention se rapporte à un procédé de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication (TC), voir page 1, lignes 3 à 11.

1.2 De nombreuses solutions ont été proposées pour permettre à des utilisateurs d'effectuer des paiements à l'aide d'un terminal de communication (TC) tout en utilisant physiquement une carte de paiement. Les paiements en mode "card present" permettent un certain degré de sécurité car les données de la puce de la carte ou de la bande magnétique sont utilisées.

1.3 Mais un tel dispositif, connu de US2005/236480, se heurte à de nombreux problèmes, entre autres, il doit être adapté à un modèle de terminal particulier et il n'est pas adapté à une utilisation contemporaine des moyens de paiement, comme le paiement par web qui est plus universel. De plus, il est relativement aisé de subtiliser temporairement un tel dispositif, voir page 1, ligne 25, à page 2, ligne 14.

1.4 Il existe donc un besoin de fournir une technique qui permette de réaliser un paiement de type "card present" tout en étant adapté d'une part à des impératifs de passage à l'échelle, de sécurisation des données de la carte bancaire et des transactions, voir page 2, deuxième paragraphe.

1.5 Le principe général de la technique proposée par l'invention consiste à introduire, au sein du terminal de communication de l'utilisateur (TC), un terminal de

paiement virtuel (vPos). Ce terminal virtuel est mis en œuvre au sein d'un premier espace sécurisé du terminal de communication (TC) lequel espace sécurisé comprend une zone de mémorisation inviolable pouvant être mise en œuvre pour exécuter des transactions, et notamment des transactions de paiement à l'aide d'une carte de paiement virtuelle (vCB). Cette carte virtuelle est chargée dans un deuxième espace sécurisé (SecSpace2) dans un espace distant, présent sur un serveur auquel le terminal de communication est connecté.

2. Article 84 CBE

2.1 L'objection de clarté porte sur la revendication 5 que la division d'examen avait considérée être définie par le but à atteindre.

2.2 La requérante a argumenté que l'identification de l'espace sécurisé n'est pas un but à atteindre, mais au contraire l'action concrètement mise en œuvre par le terminal pour obtenir les informations utiles à l'établissement d'une communication ultérieure.

2.3 La Chambre est de l'avis que la revendication 5 est claire parce que l'étape d'identification de l'espace sécurisé, qui correspond à l'élément 21 de la figure 2 pointant vers un espace sécurisé sur un serveur et comprenant des cartes virtuelles, est suivie d'une étape de chargement 22 d'un module de communication, voir demande correspondante, page 8, lignes 22 à 28.

3. Article 56 CBE

3.1 La division d'examen a considéré que l'objet de la revendication 1 n'était pas inventif au regard d'une combinaison du POS virtuel connu de D8 (WO 2010/032216)

avec le serveur de cartes de paiement virtuelles connu de D7 (WO 2014/048990) car ceci permet de combiner les avantages des solutions de ces deux documents, voir point 2.4 de la décision.

3.2 D8 représente l'état de la technique le plus proche dans la mesure où ce document décrit un système de paiement qui permet d'effectuer des transactions de paiement au moyen d'un terminal de communication apte à mettre en oeuvre un terminal de paiement virtuel. Les cartes de paiement virtuelles sont stockées dans un espace mémoire sécurisé, mais toujours sur le terminal de communication, voir page 7, lignes 4 à 9, et non pas sur un serveur distant.

Quand une transaction doit être exécutée le serveur ("payment processing server") reçoit un paquet de données comprenant l'identification de la carte de paiement, l'identification du destinataire du paiement et un mot de passe unique ("one-time password"). Le paiement est autorisé si le mot de passe est correct. Le terminal de communication reçoit en retour un code d'autorisation que l'utilisateur communique au commerçant, voir page 8, ligne 21, à page 9, ligne 10. Le serveur ne fait pas de vérification du PIN car ceci a déjà été fait sur le terminal.

3.3 La Chambre est d'accord avec la division d'examen et la requérante que la revendication 1 se distingue de D8 par "*une étape de chargement (20), au sein d'un deuxième espace sécurisé (SecSpace2) situé sur un serveur (SrvVCB) connecté au terminal de communication (TC) par l'intermédiaire d'un réseau de communication (Ntwk), d'au moins une carte de paiement virtuelle (vCB), ladite carte de paiement virtuelle (vCB) étant instanciée par un module logiciel d'émulation (modEmul)*

mis en oeuvre sous la forme d'une exécution d'une machine virtuelle."

3.4 La mise en œuvre de cartes de paiement virtuelles au sein d'un serveur distant a pour effet de protéger une pluralité de cartes de paiement appartenant à une pluralité de titulaires, voir page 13, lignes 13 à 14 de la demande, d'une manière plus sécurisée que dans D8 où la perte de la carte mémoire amovible peut rendre impossible la mise en œuvre d'un paiement.

3.5 Le problème technique objectif peut donc être formulé ainsi: comment accroître la sécurisation de transactions effectuées au moyen de cartes de paiement virtuelles par de multiples utilisateurs potentiels.

3.6 La division d'examen a argumenté que l'élément sécurisé de D7, se trouvant sur un serveur, est une carte de type JavaCard et que les logiciels qui émulent la carte de paiement virtuelle s'exécutent sur une machine virtuelle dans cette carte, en citant Pascal Urien et al.: "*Towards a Secure Cloud of Secure Elements, Concepts and Experiments with NFC Mobiles*" (D1), Section B, The Applications Age, pour soutenir cet argument.

3.7 La Chambre n'est pas de l'avis que l'élément sécurisé de D7 est une Javacard. Le serveur de D7 prévoit un élément sécurisé pour chaque carte virtuelle du terminal de communication, voir D7, page 11, lignes 5 et suivantes, afin de stocker des données pour vérifier et autoriser une transaction entre le terminal de communication et le terminal de paiement, voir figure 4 de D7 et page 16, lignes 8 à 22. Mais nulle part dans D7 il n'est décrit que cet élément prend la forme d'une JavaCard. Ce n'est d'ailleurs pas nécessaire car l'émulation d'une carte de paiement sur le serveur

n'est pas requise. Les cartes de paiement virtuelles sont mises en œuvre seulement au niveau du terminal de communication. L'élément sécurisé prend plutôt la forme d'un microcontrôleur qui stocke des données et gère le cryptage, tel qu'il est décrit dans D9.

3.8 Une combinaison de D8 avec D7 n'amène pas à l'objet de la revendication 1 qui implique une activité inventive au regard d'une combinaison de D8 avec D7, mais aussi au regard d'une combinaison de D8 avec D1.

3.9 Le document D1 présente un historique des éléments sécurisés utilisés dans et par des cartes de paiement. Ces éléments sécurisés sont des microcontrôleurs sécurisés qui sont équipés d'un système d'exploitation qui soutient une machine virtuelle. Ils peuvent être organisés sous forme d'un "grid", voir page 170, colonne de gauche, troisième paragraphe.

La Figure 5 montre comment un terminal de communication ("NFC proxy") communique par un canal sécurisé avec le "grid" et via NFC avec un terminal POS. Les informations sont échangées sous la forme d'APDUs selon la norme ISO7816. Un élément sécurisé du "grid" stocke des applications EMV, voir page 170, colonne de gauche, lignes 3 à 7, et page 171, colonne de gauche, deuxième paragraphe, qui sont entre autres des applications de cryptage.

L'émulation d'une carte de paiement se fait par contre toujours sur le terminal de communication, voir page 171, colonne de gauche, lignes 1 à 5. Le "card emulation mode" de la page 169, colonne de gauche, deuxième paragraphe, fait aussi référence à l'émulation de la carte dans le contrôleur NCF de téléphone mobile.

3.10 Une combinaison de D8 avec D1 ammènerait à un système comprenant un serveur composé d'éléments sécurisés dont chacun stocke des applications EMV. Par contre, la configuration de ce système resterait différente de l'invention car le chargement d'une carte de paiement virtuelle et son instanciation se feraient toujours sur le terminal de communication. Les éléments sécurisés du "grid" de D1 sous la forme des micro-controlleurs sécurisés sont certes capables d'exécuter une machine virtuelle, mais il n'y aurait pas de motivation ni d'incitation pour la personne du métier à faire une telle modification qui représenterait une étape supplémentaire.

4. La revendication 1 implique donc une activité inventive conformément à l'article 56 CBE.

Dispositif

Par ces motifs, il est statué comme suit

1. La décision contestée est annulée.

2. L'affaire est renvoyée à la division d'examen afin de délivrer un brevet dans la version suivante:

- la description (pages 1-16) déposée pendant la procédure orale le 23 novembre 2023,

- les revendications 1 à 9 déposées le 15 avril 2020,

- et les dessins 1 à 4 (pages 1-3) déposés le 10 avril 2015.

Le Greffier : Le Président :

T. Buschek W. Chandler

Décision authentifiée électroniquement