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 4 avril 2019

N° du recours : T 0236/16 - 3.5.05

N° de la demande : 07788889.9

N° de la publication : 2027667

C.I.B. : H04L9/32, H04N7/167

Langue de la procédure : FR

Titre de l'invention :
PROCEDES DE DIFFUSION ET DE RECEPTION D'UN PROGRAMME MULTIMEDIA EMBROUILLE, TETE DE RESEAU, TERMINAL, RECEPTEUR ET PROCESSEUR DE SECURITE POUR CES PROCEDES

Demandeur :
Viaccess

Référence :
Protection de contenu multimedia/VIACCESS

Normes juridiques appliquées :
RPCR Art. 13(1)
CBE Art. 56

Mot-clé :
Requête subsidiaire produite tardivement - recevable (oui)
Activité inventive - (oui)

Décisions citées :

Exergue :

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 0236/16 - 3.5.05

D E C I S I O N
de la Chambre de recours technique 3.5.05
du 4 avril 2019

Requérant : (Demandeur)	Viaccess Les Collines de l'Arche, Tour Opéra C 92057 Paris La Défense Cedex (FR)
Mandataire :	Lavoix 2, place d'Estienne d'Orves 75441 Paris Cedex 09 (FR)
Décision attaquée :	**Décision de la division d'examen de l'Office européen des brevets postée le 14 juillet 2015 par laquelle la demande de brevet européen n° 07788889.9 a été rejetée conformément aux dispositions de l'article 97(2) CBE.**

Composition de la Chambre :

Présidente	A. Ritzka
Membres :	P. Cretaine
	G. Weiss

Exposé des faits et conclusions

I. Le présent recours est formé par la demanderesse (requérante) de la demande de brevet européen n° 07788889.9 à l'encontre de la décision écrite postée le 14 juillet 2015 par la division d'examen rejetant la demande pour manque d'activité inventive (article 56 CBE), eu égard au contenu du document

D1: US 5 029 207

et des connaissances générales de l'homme du métier, telles qu'illustrées par le document

D4: Menezes et al.: "Handbook of Applied Cryptography", USA, 1er janvier 1997, pages 490 à 553.

II. L'acte de recours a été déposé le 1er septembre 2015 et la taxe de recours a été acquittée le même jour. Avec le mémoire exposant les motifs de recours, reçu le 16 novembre 2015, la requérante a demandé l'annulation de la décision attaquée et la délivrance d'un brevet sur la base de la requête principale sur laquelle la décision est fondée et qui a été redéposée avec le mémoire exposant les motifs du recours, ou sur la base des requêtes subsidiaires 1 à 3 déposées avec le mémoire exposant les motifs du recours. La requérante a aussi demandé la tenue d'une procédure orale, au cas où la chambre ne ferait pas droit à la requête principale ou à l'une des requêtes subsidiaires.

III. Une citation à une procédure orale a été envoyée le 21 janvier 2019. Dans une notification établie conformément à l'article 15(1) RPCR et envoyée le 24 janvier 2019, la chambre a communiqué, après un examen préliminaire, ses observations selon lesquelles l'objet

des revendications selon la requête principale ne semblait pas impliquer d'activité inventive eu égard à l'état de la technique antérieur tel que décrit dans la demande de la page 1, ligne 8 à la page 2, ligne 24, et aux connaissances générales de l'homme du métier telles qu'illustrées par le document D4. La chambre a aussi soulevé la question de la recevabilité, au vu de l'article 12(4) RPCR, des requêtes subsidiaires 1 à 3. Elle a de plus indiqué que les revendications selon ces requêtes subsidiaires 1 à 3 ne semblaient pas non plus impliquer d'activité inventive, eu égard à l'état de la technique antérieur mentionné ci-dessus et aux connaissances générales de l'homme du métier telle qu'illustrées par les documents D4 (pour les requêtes subsidiaires 1 à 3) et D5 (pour les requêtes subsidiaires 2 et 3), le document

D5: Menezes et al.: "Handbook of Applied Cryptography", 1997, US, pages 385 to 424,

étant introduit dans la procédure par la chambre elle-même selon l'article 114(1) CBE.

IV. Dans sa réponse en date du 4 mars 2019, la requérante a retiré la requête subsidiaire 1 et redéposé les revendications selon les requêtes subsidiaires 2 et 3 déposées avec le mémoire exposant les motifs des recours et redéposées, en tant que première et deuxième requêtes subsidiaires, et déposé des revendications selon une troisième requête subsidiaire.

V. La procédure orale s'est tenue le 4 avril 2019, au cours de laquelle la requérante a retiré la requête principale ainsi que les première et deuxième requêtes subsidiaires. La requérante a demandé l'annulation de la décision attaquée et la délivrance d'un brevet sur

la base des revendications selon la troisième requête subsidiaire déposée par lettre en date du 4 mars 2019, devenue requête principale.

VI. La revendication 1 selon l'unique requête s'énonce comme suit:

"Procédé de diffusion, par l'intermédiaire d'un réseau large bande, d'un programme multimédia embrouillé dans lequel :
- une information peut être acheminée vers une adresse multicast de sorte que seul un groupe de plusieurs terminaux correspondants à cette adresse multicast reçoit l'information tandis que d'autres terminaux connectés au même réseau ne reçoivent pas cette information, et
- une information peut être acheminée vers une adresse unicast de sorte que seul le terminal correspondant à cette adresse unicast reçoit l'information tandis que les autres terminaux connectés au même réseau ne la reçoivent pas,
et dans lequel une tête de réseau (4):
- embrouille (en 96 ; 250) le programme multimédia avec un mot de contrôle,
- chiffre (en 98 ; 252) le mot de contrôle afin d'obtenir un premier cryptogramme,
- chiffre (en 100 ; 256) le premier cryptogramme afin d'obtenir un second cryptogramme, le premier et le second chiffrements étant réalisés à l'aide de clés de chiffrement différentes choisies dans le groupe composé d'une clé d'exploitation (K_{proc}) et d'une clé de licence (K_{Term})
- multiplexe (en 104 ; 258) le second cryptogramme avec le programme multimédia embrouillé pour obtenir un contenu multiplexé,

- diffuse (en 108 ; 262) le contenu multiplexé vers une adresse multicast de diffusion afin d'établir une connexion point à multi-points entre la tête de réseau et plusieurs récepteurs du contenu multiplexé, et
- sur une liaison point à point établie (en 150) avec un terminal en utilisant l'adresse unicast de ce terminal, transmet la clé de licence individuellement à ce terminal par l'intermédiaire de cette liaison point à point,

caractérisé en ce que ladite clé d'exploitation est commune à tous les terminaux d'un opérateur et en ce que avant la transmission de la clé de licence :

- la tête de réseau procède à une étape d'authentification du terminal dans laquelle la tête de réseau:
- - détermine (en 160) une clé unique (K_{ecmu}) propre à identifier le terminal parmi l'ensemble des terminaux raccordés au réseau, à partir:
  - . de données préenregistrées connues de la tête de réseau et qui ne lui ont pas été transmises par le terminal,
  - et
  - . de données transmises (UA) par le terminal à la tête de réseau, les données préenregistrées et les données transmises étant chacune insuffisantes à elles seules pour permettre de déterminer la clé unique (K_{ecmu}) utilisée par ce terminal,
- - vérifie (en 196) que le terminal est apte à chiffrer ou à déchiffrer correctement des données avec la clé unique qu'elle a déterminée sans que pour cela la tête de réseau ait eu à transmettre au préalable les données préenregistrées ou la clé unique (K_{ecmu}) déterminée à ce terminal, la vérification comprenant:

▪ l'envoi, par la tête de réseau (en 168) d'un message ECM (Entitlement Control Message) au terminal dans lequel le champ destiné à contenir un cryptogramme d'un mot de contrôle contient un cryptogramme obtenu en chiffrant une donnée inconnue ($Alea_{Auth}$) du terminal à l'aide de la clé unique (K_{ecmu}) déterminée,

▪ puis la vérification (en 196) que la donnée inconnue du terminal a correctement été déchiffrée par ce terminal,

- et dans l'affirmative établit (en 198) que le terminal est authentifié, et
- si le terminal a été authentifié avec succès, la tête de réseau envoie (en 216) au terminal un message de transmission de licence contenant la clé de licence ou un cryptogramme de la clé de licence, par l'intermédiaire de la liaison point à point établie, et
- si le terminal n'est pas authentifié avec succès, la tête de réseau agit (en 200) de manière à empêcher le désembrouillage complet par ce terminal du programme multimédia embrouillé diffusé."

La requête comprend d'autres revendications indépendantes portant sur des procédés de réception correspondants (revendications 5 et 7), et des dispositifs de diffusion (revendication 9) et de réception (revendications 10 à 12) correspondants.

Motifs de la décision

1. Le recours est recevable (voir point II).

2. Recevabilité de la requête

La requête a été déposée en tant que requête

auxiliaire 3 en réponse à la communication émise par la chambre et est basée sur une combinaison des revendications de la requête principale déposée avec le mémoire exposant les motifs du recours. Étant donné que cette requête visait clairement et de façon plausible à surmonter l'objection de manque d'activité inventive soulevée par la chambre, celle-ci a exercé sa discrétion selon l'article 13(1) RPCR et décidé d'admettre la requête dans la procédure.

3. État de la technique le plus proche:

La chambre est convaincu par l'argument de la requérante que, le document D1 se rapportant à un système de diffusion de contenu multimédia par satellite, il n'envisage pas de liaison bi-directionnelle sur le canal de transmission de contenu entre la tête de réseau et un terminal de réception. En particulier, D1 ne permet pas à un terminal de coopérer avec la tête de réseau pour s'authentifier à partir de messages échangés sur une telle liaison bidirectionnelle.

La chambre considère donc que l'un quelconque des procédés existants tels que décrits par le demandeur lui-même de la page 1, ligne 8 à la page 2, ligne 24 de la description, représente un état de la technique plus proche de l'objet de la demande que le document D1.

Un tel procédé connu divulgue donc les caractéristiques suivantes d'un procédé de diffusion, par l'intermédiaire d'un réseau large bande, d'un programme multimédia embrouillé selon lesquelles:
- une information peut être acheminée vers une adresse multicast de sorte que seul un groupe de plusieurs terminaux correspondants à cette adresse multicast

reçoit l'information, tandis que d'autres terminaux connectés au même réseau ne reçoivent pas cette information, et
- une information peut être acheminée vers une adresse unicast de sorte que seul le terminal correspondant à cette adresse unicast reçoit l'information, tandis que les autres terminaux connectés au même réseau ne la reçoivent pas,
et selon lesquelles une tête de réseau:
- embrouille le programme multimédia avec un mot de contrôle,
- chiffre le mot de contrôle afin d'obtenir un premier cryptogramme,
- chiffre le premier cryptogramme afin d'obtenir un second cryptogramme, le premier et le second chiffrements étant réalisés à l'aide de clés de chiffrement différentes choisies dans le groupe composé d'une clé d'exploitation et d'une clé de licence,
- multiplexe le second cryptogramme avec le programme multimédia embrouillé pour obtenir un contenu multiplexé,
- diffuse le contenu multiplexé vers une adresse multicast de diffusion afin d'établir une connexion point à multi-points entre la tête de réseau et plusieurs récepteurs du contenu multiplexé, et
- sur une liaison point à point établie avec un terminal en utilisant l'adresse unicast de ce terminal, transmet la clé de licence individuellement à ce terminal par l'intermédiaire de cette liaison point à point.

Dans des procédés correspondants existants de réception, un terminal:
- écoute l'adresse multicast de diffusion et reçoit le contenu multiplexé,

- démultiplexe le contenu multiplexé reçu pour obtenir le second cryptogramme et le programme multimédia embrouillé,
- déchiffre le second cryptogramme afin d'obtenir le premier cryptogramme,
- déchiffre le premier cryptogramme afin d'obtenir le mot de contrôle, le premier et le second déchiffrements étant réalisés à l'aide de clés de chiffrement différentes choisies dans le groupe composé de la clé d'exploitation et de la clé de licence,
- la clé de licence étant transmise par l'intermédiaire d'une liaison point-à-point entre la tête de réseau et le terminal.

4. Activité inventive

Les différences entre l'objet de la revendication 1 et l'état de la technique le plus proche tel que défini au paragraphe 2 ci-dessus sont en substance les suivantes:
a) la clé d'exploitation est commune à tous les terminaux d'un opérateur,
b) avant la transmission de la clé de licence, la tête de réseau procède à une étape d'authentification du terminal dans laquelle la tête de réseau:
b1) détermine une clé unique (Figure 1: "K_{ECMU}") déjà connue du terminal et propre à l'identifier parmi l'ensemble des terminaux raccordés au réseau, à partir: de données préenregistrées (Figure 1: "$K_{rootEMCU}$") dans la tête de réseau et de données transmises par le terminal à la tête de réseau (Figure 1:"UA"), les données préenregistrées et les données transmises étant chacune insuffisantes à elles seules pour permettre de déterminer la clé unique ("K_{EMCU}") utilisée par ce terminal,
b2) vérifie que le terminal est apte à chiffrer ou à déchiffrer correctement des données avec cette clé

unique qu'elle a déterminée sans que pour cela la tête de réseau ait eu à transmettre au préalable les données préenregistrées ou la clé unique (Kecmu) déterminée à ce terminal, la vérification comprenant :
l'envoi, par la tête de réseau d'un message ECM (Entitlement Control Message) au terminal dans lequel le champ destiné à contenir un cryptogramme d'un mot de contrôle contient un cryptogramme obtenu en chiffrant une donnée inconnue (AleaAuth) du terminal à l'aide de la clé unique (Kecmu) déterminée,
puis la vérification que la donnée inconnue du terminal a correctement été déchiffrée par ce terminal,
et dans l'affirmative établit que le terminal est authentifié, et
d) si le terminal a été authentifié avec succès, la tête de réseau envoie au terminal un message de transmission de licence contenant la clé de licence ou un cryptogramme de la clé de licence, par l'intermédiaire de la liaison point à point établie, et
e) si le terminal n'est pas authentifié avec succès, la tête de réseau agit de manière à empêcher le désembrouillage complet par ce terminal du programme multimédia embrouillé diffusé.

Les effets techniques de ces différences sont les suivants:
- l'utilisation d'une même clé d'exploitation par plusieurs terminaux permet l'envoi d'une telle clé par transmission multicast, limitant ainsi la complexité du système,
- seul un terminal authentifié par la tête de réseau peut recevoir la clé de licence et donc être capable de désembrouiller le programme multimédia,
- le terminal est authentifié par un procédé cryptographique d'authentification de type "challenge-response" utilisant un défi d'authentification crypté

inconnu du terminal et une clé partagée entre la tête de réseau et le terminal,
- le défi d'authentification est envoyé sous forme encrypté par la tête de réseau au terminal dans le champ destiné à contenir un cryptogramme d'un mot de contrôle d'un message ECM conventionnel de transmission de licence (Entitlement Control Message selon la dénomination standardisée) sans avoir à utiliser un autre format de message.

Le problème technique objectif peut donc être formulé comme étant de limiter le risque de piratage des programmes multimédia embrouillés diffusés par l'intermédiaire d'un réseau, tout en limitant la complexité du système.

L'homme du métier est celui du domaine du contrôle d'accès aux contenus multimédia, un domaine technique qui fait largement appel à des procédés cryptographiques. On peut donc considérer qu'il a à sa disposition toute une variété de techniques cryptographiques bien connues, telles que celles décrites dans les documents D4 et D5 qui sont extraits d'un ouvrage faisant référence dans le domaine. En particulier, les procédés cryptographique utilisés dans la revendication 1 sont tous divulgués individuellement dans les documents D4 et D5:
- le paragraphe 13.5 de D4 divulgue la distribution d'une clé commune ("shared keys") à des entités préalablement authentifiées ("entities authentication"),
- le paragraphe 13.3.1 divulgue l'utilisation d'une clé commune à deux entités ("symmetric keys") pour la transmission d'une autre clé ("key-encrypting keys"),
- le paragraphe 12.4 de D4 divulgue la génération d'une même clé secrète dans deux entités à partir

d'informations fournies séparément par chacune des entités et de telle sorte que chacune des entités ne puisse pas déterminer la clé à partir de ses seules informations ("a key establishment technique in which a shared secret is derived by two parties as a function of information contributed by... each of these, ... such that no party can predetermine the resulting value"),
- le paragraphe 10.3.2 de D5 divulgue l'authentification d'une partie en testant sa connaissance d'une clé partagée ("require the claimant and the verifier to share a symmetric key"; "The claimant corroborates its identity by demonstrating knowledge of the shared key by encrypting a challenge... using the key").

On peut donc considérer que l'homme du métier pourrait utiliser une combinaison de ces techniques cryptographiques pour sécuriser la transmission de la clé de licence. Cependant, même ce faisant l'homme du métier n'arriverait pas à l'objet de la revendication. En effet, ni D4 ni D5 ne divulguent ou même suggèrent d'implémenter l'authentification du terminal en utilisant un message standardisé de type ECM pour transporter un cryptogramme du défi d'authentification. La requérante a fait valoir avec raison que cela permettait de réaliser un adressage individuel implicite du terminal sans rajouter de complexité supplémentaire dans le système de diffusion et sans avoir à développer une nouvelle structure de message pour l'authentification.

Au vu de ce qui précède, la chambre considère que l'objet de la revendication 1 implique une activité inventive (Article 56 CBE).

Les revendications indépendantes 5, 7 et 9 à 12 correspondent à la revendication 1 en termes de procédé de réception, de dispositif d'émission, ou de dispositif de réception, et satisfont donc aussi aux exigences de l'article 56 CBE.

Les revendications 2 à 4, 6 et 8 sont des revendications dépendantes et satisfont donc, en tant que telles, aux exigences de l'article 56 CBE.

Dispositif

Par ces motifs, il est statué comme suit

1. La décision attaquée est annulée.

2. L'affaire est renvoyée à l'instance du premier degré afin de délivrer un brevet dans la version suivante:
- description: pages 1 à 21 telles que déposées;
- revendications 1 à 12 de la troisième requête subsidiaire déposée par lettre en date du 4 mars 2019, devenue requête principale;
- dessins: feuilles 1/5 à 5/5 telles que déposées.

La Greffière : La Présidente :

K. Götz-Wein A. Ritzka

Décision authentifiée électroniquement