Unified Patent Court
Einheitliches Patentgericht
Juridiction unifiée du brevet

Division Locale de Paris

UPC_CFI_530/2025
&UPC-CFI-0002281/2025
&UPC-CFI-0002285/2025
& UPC-CFI-0000003/2026
& UPC-CFI-0002274/2025

Décision au fond
du Tribunal de première instance de la Juridiction Unifiée du Brevet, rendue le 17/11/2026

En-tête :

Le titulaire du brevet a la possibilité de modifier la description pour qu'elle soit en conformité avec la revendication modifiée (cf. R. 30.1 (a) RdP). En revanche, il n'est pas possible de modifier la description de telle sorte qu'elle change la signification du Brevet et de sa Revendication 1. Il est possible de limiter le périmètre de protection du Brevet, mais pas de donner une nouvelle signification au Brevet en modifiant aussi complètement la description. Ce serait d'ailleurs incompatible avec le principe de sécurité juridique pour les tiers.

Mots-clés :

R. 30.1 (a) RdP. Modification du brevet. Principe de sécurité juridique pour les tiers

DEMANDEUR

KEEEX SAS
5 rue de Lissandre
13013 - MARSEILLE - FR

Représenté par Thibaud LELONG, et autres représentants du Cabinet FIDAL, du Cabinet FIDAL INNOVATION et du Cabinet GERMAIN MAUREAU

DEFENDEURS

1) **ADOBE SYSTEMS SOFTWARE IRELAND LIMITED**
4-6 Riverwalk, Citywest Business Campus,
Saggart D24DCWO - Dublin 24 – IE

2) **ADOBE INC**
345 Park Avenue
CA 95110-2704 - San Jose – US

Représentés par Thomas CUCHE et autres représentants du cabinet

DTMV, du cabinet POWELL GILBERT et du cabinet PAUSTIAN & PARTNER

3) **OPEN AI OPCO LLC**
1455 3rd Street
CA 94158 - San Francisco - US

4) **OPEN AI IRELAND LTD**
117-126 Sheriff Street Upper, The Liffey Trust Centre, 1st Floor
D01 YC43 - Dublin 1 - IE

Représentés par David POR, et autres représentants du cabinet CLIFFORD CHANCE

5) **TRUEPIC INC.**
402 W. Broadway, Suite 400/PMB#5021
CA 92101 - San Diego - US

Représenté par Benjamin MAY, et autres représentants du cabinet JEANTET

6) **JOINT DEVELOPMENT FOUNDATION PROJECTS LLC**
548 Market Street PMB 57724
CA 94101-5401 - San Francisco - US

7) **COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY (C2PA)**
3500 South Dupont Highway Suite, AA101
DE 19901 - Dover - US

Représentés par Philipp Cepl, et autres représentants du cabinet Herbert Smith Freehills Kramer Paris LLP

BREVET LITIGIEUX

Numéro de brevet	*Titulaire(s)*
EP2949070	KEEEX SAS

COMPOSITION DE LA CHAMBRE -CHAMBRE PLENIERE :

Présidente et Juge-rapporteur	**Camille Lignieres**
Juge qualifiée sur le plan juridique	**Carine Gillet**
Juge qualifié sur le plan juridique	**Peter Tochtermann**
Juge qualifié sur le plan technique	**Alessandro Sanchini**

LANGUE DE LA PROCÉDURE : Français

DECISION

LES PARTIES EN PRÉSENCE

1. La société KEEEX SAS est une société française créée en 2014 par Laurent HENOCQUE qui est l'inventeur du brevet objet du présent litige. Le siège social de KEEEX est situé à Marseille. Cette société a le statut de PME (petite entreprise) et a pour objet le développement de programmes et de solutions informatiques. La société KEEEX est spécialisée dans les solutions de confiance et de sécurité numérique.
   KEEEX est titulaire du brevet européen EP 2 949 070 B1 (ci-après « EP 070 ») depuis sa cession définitive à son profit en date du 26 mars 2025 (pièce KEEEX A4), après en avoir été le licencié exclusif depuis 2014 (Mémoire en demande, page 12). Le tribunal relève que la contestation sur la titularité du brevet et donc la recevabilité de KEEEX dans son action en contrefaçon n'est plus soutenue à ce stade de la procédure par ADOBE.

2. Les sociétés ADOBE (Défenderesses 1 et 2) :

   La défenderesse 1) est une société de droit américain, la maison mère du groupe ADOBE fondé il y a plus de 40 ans, dont le siège social est situé en Californie, et qui est spécialisée dans les logiciels et autres outils numériques. ADOBE a notamment développé l'outil d'IA générative « ADOBE Firefly ».

   La défenderesse 2) est une société de droit irlandais appartenant au groupe ADOBE (Mémoire en défense ADOBE, page 16).

3. Les Défenderesses 3 à 4 OpenAI : (Mémoire en défense OpenAI, page 14)

   À titre préliminaire, il convient de noter que la société OpenAI LP a fait l'objet d'un retrait de l'action initiée à son encontre par ordonnance du 19/12/2025.

   Les défenderesses 3 et 4 sont des sociétés de droit américain faisant partie du groupe OpenAI, fondé en 2015, spécialisé dans la recherche et le développement de technologies d'intelligence artificielle (« IA »). L'activité principale du groupe OpenAI consiste à concevoir, entraîner et déployer des modèles d'IA avancés, tels que le modèle « ChatGPT ».

4. La société TRUEPIC (défenderesse 5), fondée en 2016, se présente comme une PME technologique américaine spécialisée dans la vérification et

l'authentification des images et vidéos numériques. Son siège social est situé à San Diego, Californie. (Mémoire en défense TRUEPIC, page 9)

5. Les défenderesses 6 et 7 :

   Joint Development Foundation Projects LLC (défendeur 6) est une société à responsabilité limitée spécifique (de type « Series » LLC) dont le siège social est situé à San Francisco (Californie). Le défendeur 6) a été principalement créé pour permettre la création d'entités dites « en série » afin de faciliter l'établissement de normes et de spécifications techniques et ainsi favoriser le développement d'activités par des tiers.

   Son unique membre est la C2PA (défendeur 7), une société à but non lucratif dont le siège social est situé dans l'État du Delaware.

6. Il n'est pas contesté qu'ADOBE, OpenAI et TRUEPIC sont engagés dans le développement de la technologie dite « C2PA ». Cette technologie est présentée par KEEEX comme « un moyen de développer un standard ouvert pour certifier l'authenticité et la provenance des contenus numériques (images, vidéos, documents). » (Récapitulatif des moyens de KEEEX, page 3)

FAITS ET PROCÉDURE

7. KEEEX a initié le 17 juin 2025 devant la Division Locale de Paris de la Juridiction Unifiée du Brevet (ci-après « JUB ») une action en contrefaçon du brevet EP 2 949 070 B1 (dit « EP 070 ») contre les sociétés ADOBE, OpenAI, TRUEPIC, JOINT DVT et C2PA.

8. Dans le cadre d'une objection préliminaire, les défendeurs ont contesté la compétence de la juridiction concernant les parts nationales du brevet en cause se situant hors du territoire des Etats membres contractants à l'AJUB, ce qui a donné lieu à une ordonnance de la cour d'appel de Luxembourg du 13/03/2026 décidant que « la juridiction n'est pas compétente pour statuer sur la contrefaçon alléguée des parties suisse, espagnole, britannique, irlandaise, norvégienne et polonaise du brevet EP 2 949 070 ». Il s'ensuit que le tribunal est saisi, dans le cadre de ce litige, des actes de contrefaçon allégués par KEEEX relatifs aux parts nationales du brevet dans les seuls États membres de l'AJUB désignés par le brevet et en vigueur sur lesdits territoires.

9. Les mémoires en défense avec demandes reconventionnelles en nullité du brevet ont été déposés en date des 30 et 31 décembre 2025.
   En date du 5 mars 2026, le demandeur a répliqué aux mémoires en défense et a demandé une modification conditionnelle du brevet avec 11 requêtes subsidiaires. KEEEX a déposé son dernier mémoire en date du 5 juin 2026, et les défendeurs en date du 6 juillet 2026.
   La procédure écrite a été clôturée le 27 août 2026 et la procédure de mise en état a été clôturée en date du 22 septembre dernier.

10. Le Juge Rapporteur a été saisi dans ce dossier par de multiples requêtes procédurales et a rendu des ordonnances, ayant elles-mêmes fait l'objet de nombreux recours en révision et/ou en appel.
Plusieurs réunions de mise en état en ligne ont été organisées pour se concerter avec les représentants des parties sur la mise en état de ce dossier et sur l'organisation de l'audience orale.

11. Les décisions procédurales, outre celle sur la compétence dans le cadre de l'objection préliminaire, qui ont un impact sur le périmètre du litige dont le panel est saisi, au stade de la décision finale à intervenir, sont les suivantes :

- l'abandon par KEEEX de sa demande initiale aux fins de voir statuer sur la fixation des dommages-intérêts dès la décision au fond au profit d'une décision sur ce point dans le cadre d'une procédure séparée ;
- la recevabilité de la demande de KEEEX en paiement d'une provision sur dommages-intérêts de 100 millions (préjudice matériel) et de 20 millions d'euros (préjudice moral) ;
- certaines parties du mémoire déposé par KEEEX le 5 juin 2026 ont été écartées des débats comme tardives ; et la demande de KEEEX pour une modification ultérieure de son brevet selon R. 30.2 RdP n'a pas été autorisée par le Juge Rapporteur (cf. ordonnance du 25 juin 2026 et sa confirmation par le panel le 29 juillet 2026) ;
- une garantie pour les frais de justice (R. 158 RdP) d'un montant total de 200 000 euros a été produite par le demandeur à la demande des défendeurs (ordonnance du 19 décembre 2025 définitive), puis une garantie supplémentaire de 100 000 euros à la demande d'ADOBE a été produite en date du 11 septembre 2026 (ordonnance du 20 juillet 2026 confirmée par le panel le 27 août 2026).

12. Enfin, il sera ajouté que le 17 juillet 2026, ADOBE a déposé dans le CMS pour information du Tribunal l'opinion préliminaire du Tribunal fédéral des brevets (Bundespatentgericht) sur la validité de la part allemande du brevet EP 070. Cette pièce a été admise au dossier par le Juge Rapporteur qui a invité les parties à produire leurs commentaires écrits sur cette nouvelle pièce du dossier. Cette opinion préliminaire concerne une action en nullité de la partie allemande du brevet invoqué qui a été déposée devant le Tribunal Fédéral des Brevets en Allemagne le 10 décembre 2025 par la société ADOBE Systems GmbH, laquelle n'est pas partie à la présente instance.

LES DEMANDES DES PARTIES

13. **KEEEX, demandeur au principal, sollicite, en substance :**

Sur l'action en contrefaçon :

Dire que les Défenderesses ont commis des actes de contrefaçon directe (article 25 AJUB) et indirecte (article 26 AJUB) de la revendication 1 du brevet EP 070 en :

- mettant à disposition des spécifications techniques C2PA ;
- mettant à disposition le logiciel C2PATOOL et les logiciels de vérification VERIFY et TRUEPIC ;
- mettant à disposition des fichiers vérifiables ;
- mettant à disposition les logiciels C2PATOOL, ADOBE FIREFLY et CHATGPT (OPENAI) permettant de produire des fichiers vérifiables ;

14. KEEEX reproche également aux défenderesses des actes de contrefaçon directe et indirecte des revendications 2, 4, 7, 8, 10, 11, 14, 16 et 18 du brevet EP 070 tel que délivré, ainsi que les revendications opposées dans la version modifiée du brevet en cause selon la requête principale et les requêtes subsidiaires. Il n'est pas opposé la revendication 15 du Brevet tel que délivré.

15. En conséquence, KEEEX demande au Tribunal qu'elle :

- Ordonne la cessation des actes de contrefaçon et que la mesure d'interdiction soit assortie d'une astreinte (Art. 63 AJUB)
- Ordonne l'allocation d'une provision à titre de dommages-intérêts *in solidum* par les défenderesses d'une somme de 100 millions d'euros (préjudice matériel) et la somme de 20 millions (préjudice moral)
- Ordonne la publication du dispositif de la décision à intervenir (Art. 80 AJUB)
- Condamne les défenderesses au paiement des frais de justice et frais exposés par le demandeur tant dans l'action principale que dans la demande reconventionnelle en nullité,
- Rejette les demandes de remboursement de frais à titre provisoire au titre de la règle 150.2 RdP, à hauteur de 1,25 million, formées par chacune d'entre elles ;
- Ordonne l'exécution immédiate (Art. 82 AJUB).

16. ***Sur la demande reconventionnelle en nullité :***

- le rejet de l'ensemble des demandes des Défenderesses tendant à dire irrecevables la modification du Brevet selon R. 30.1 RdP,
- le rejet des demandes en nullité des revendications contestées du brevet,
- le rejet des demandes tendant à voir subordonner l'exécution de toute injonction ou condamnation financière au versement d'une garantie par la société,
- le rejet de l'octroi d'un délai de grâce de 6 mois avant toute exécution,
- le rejet des demandes de remboursement provisoire des frais formées par chacune des Défenderesses au titre de la règle R 150.2 RdP.

17. **<u>Tous les défendeurs sollicitent en substance :</u>**

1) ***Concernant les demandes de modifications du brevet :***
JUGER irrecevables les modifications du Brevet conformément à la requête principale et aux requêtes subsidiaires demandées par la Demanderesse et en tout état de cause les REJETER ;

2) ***Concernant la demande reconventionnelle en nullité du brevet :***

A. À titre principal,
ANNULER dans leur intégralité les revendications 1, 2, 4, 7, 8, 10, 11, 14, 16 et 18 du Brevet (la revendication 15 n'étant concernée par la demande en annulation) tel qu'il a été délivré sur le territoire des États membres contractants de la JUB suivants : la France, l'Italie, l'Allemagne, l'Autriche, la Belgique, le Danemark, les Pays-Bas et la Suède ;

B. ANNULER dans leur intégralité les revendications opposées du brevet européen EP 2 949 070 B1 conformément à la requête principale et aux requêtes subsidiaires demandées par la Demanderesse, sur le territoire des États membres contractants de la JUB suivants : la France, l'Italie, l'Allemagne, l'Autriche, la Belgique, le Danemark, les Pays-Bas et la Suède.

C. En tout état de cause :
a. CONDAMNER la Demanderesse à payer tous les frais de la demande reconventionnelle en nullité ;
b. CONDAMNER la Demanderesse à rembourser, à titre provisoire (conformément à l'article 150.2 du Règlement de procédure), la somme de 1,25 million d'euros au titre des frais liés à la demande reconventionnelle en nullité.

18. ***3) Concernant la demande en contrefaçon :***

A. À titre principal,
a. DÉBOUTER la Demanderesse de sa demande en contrefaçon ;
b. DÉBOUTER la Demanderesse de sa demande en dommages et intérêts provisoires ;
c. DÉBOUTER la Demanderesse de l'ensemble de ses demandes, griefs et prétentions ;
d. CONDAMNER la Demanderesse à payer tous les frais de la demande en contrefaçon ;
e. CONDAMNER la Demanderesse à rembourser, à titre provisoire (règle 150.2 du RdP), la somme de 1.25 million d'euros au titre des frais pour la procédure en contrefaçon.6

B. A titre subsidiaire,
a. DÉBOUTER la Demanderesse de sa demande de condamnation in solidum des Défenderesses ;
b. SUBORDONNER l'exécution de toute décision faisant droit à une mesure d'injonction au versement par la Demanderesse d'une garantie d'un montant de 50 millions d'euros à payer à la Défenderesse 1) et à la Défenderesse 2) ;

c. ACCORDER un délai de grâce de six mois avant que toute injonction ne devienne exécutoire ;
d. DÉBOUTER la Demanderesse de sa demande visant à obtenir l'exécution immédiate de la décision, en tout état de cause ;
e. SUBORDONNER l'exécution de toute condamnation pécuniaire et/ou (provisoire) au titre de dommages et intérêts à la constitution d'un montant équivalent.

CONTEXTE DU LITIGE (avant contentieux)

19. KEEEX affirme avoir présenté en 2020 la solution divulguée dans le brevet EP 070 au New York Times, en présence de l'un des fondateurs de l'entité C2PA qui a par la suite développé le standard du même nom. Or, selon KEEEX, le standard C2PA reproduirait les enseignements de son brevet EP 070. Il est ainsi reproché par KEEEX aux sociétés JOINT DVP et C2PA d'avoir développé le standard C2PA, aux sociétés ADOBE, OpenAI, TRUEPIC d'en être les codéveloppeurs, et d'avoir diffusé ce standard de manière gratuite en Europe à travers leurs outils de vérification en ignorant les droits de son brevet EP 070, engendrant pour KEEEX l'impossibilité de monétiser sa technologie.

20. Ainsi, une lettre de mise en demeure circonstanciée de 35 pages a été adressée le 6 février 2025 par le conseil de KEEEX à ADOBE, à OpenAI et à TRUEPIC (objet : « Mise en demeure-contrefaçon de brevets EP 070 et US 10,218,714 ») affirmant que C2PA ainsi que ses sociétés membres portaient atteinte aux droits exclusifs conférés par EP 070 et US 10,218,714 en s'appuyant sur le procès-verbal de constat en ligne établi par un commissaire de justice (Me Legrain) en date du 15 janvier 2025 et des rapports techniques d'un expert (M. Aymar) aux fins de démontrer la similarité fonctionnelle entre les outils C2PA et les revendications du brevet EP 070. Les sociétés JOINT DVT et C2PA ont également reçu une mise en demeure, respectivement en date du 31 janvier 2025 et du 22 avril 2025 (Pièces KEEEX 9 à 14).

MOTIFS DE LA DÉCISION

21. **A titre liminaire, sur la juridiction internationale et la compétence de la Division Locale de Paris**

La juridiction internationale et la compétence interne ont été contestées par tous les défendeurs dans le cadre d'objections préliminaires fondées sur R. 19 RdP. Ces objections ont été rejetées par le Juge Rapporteur par ordonnance du 27 novembre 2025. Par une ordonnance rendue le 13 mars 2026, la Cour d'Appel de la JUB a infirmé l'ordonnance de première instance en décidant que la Juridiction n'était pas compétente pour statuer sur la contrefaçon alléguée des parties suisse, espagnole, britannique, irlandaise, norvégienne et polonaise du brevet EP 070.

22. Les autres points sur lesquels le Juge Rapporteur avait statué sur le fondement de R.19 RdP dans son ordonnance du 27 novembre 2025, notamment les objections

concernant la compétence interne de la Division Locale de Paris, ont été confirmés en appel (Extrait de l'ordonnance CoA du 13 mars 2026 en son § 45 : *« La compétence interne de la Division Locale de Paris pour connaître de l'affaire est en l'occurrence justifiée par l'accessibilité en France des logiciels de vérification de l'intégrité de contenus gratuitement mis à disposition sur Internet par les défenderesses. La société Truepic a au demeurant confirmé lors de l'audience qu'elle ne contestait pas, à l'occasion de l'appel, la décision relative à la compétence interne. Elle a, de la même manière, confirmé que sa demande de sursis à statuer était devenue sans objet par l'effet de la décision du 12 janvier 2026 ayant rejeté la demande de révision de l'ordonnance contestée. »*)

23. Il en résulte que la présente Division est compétente pour statuer sur ce litige concernant les parts du Brevet dans les seuls États contractants de l'Accord de la JUB, c'est-à-dire : la France, l'Italie, l'Allemagne, l'Autriche, la Belgique, le Danemark, les Pays-Bas et la Suède.

PRESENTATION DU BREVET EN CAUSE

24. Le brevet EP 070 s'intitule « procédé de vérification de l'intégrité d'un bloc de données numériques » [pièce 2.1 de KEEEX].
Le brevet est issu d'une demande internationale PCT/FR2014/050073 déposée le 15 janvier 2014 par l'Université Aix-Marseille et le CNRS (Centre National de la Recherche Scientifique) [pièce ADOBE, DTMV 3.3].
L'inventeur désigné est M. Laurent HENOCQUE.

25. La demande internationale, et donc le brevet EP 070, revendique la priorité d'une demande de brevet français FR 13 50549, déposée le 22 janvier 2013 et délivrée sous le numéro FR 3 001 313 le 12 février 2016.
La demande internationale a été publiée le 31 juillet 2014 sous le numéro WO 2014/114861.

26. Il n'est pas contesté que le Brevet est en vigueur au moment de la demande en contrefaçon de KEEEX dans les États membres contractants suivants : la France, l'Italie, l'Allemagne, l'Autriche, la Belgique, le Danemark, les Pays-Bas et la Suède.

27. EP 070 concerne de manière générale les procédés de vérification de l'intégrité et de l'authenticité de blocs de données numériques et d'accès à ces blocs de données, que ceux-ci soient distribués sur un réseau ou stockés sur un support de mémorisation ([0001] du Brevet).

28. Le Brevet mentionne les définitions de plusieurs termes ou expressions [0002], et notamment indique que « bloc de données » [0003] désigne tout fichier ou document numérique ou toute partie d'un tel fichier ou document, le terme fichier ne devant pas être compris comme limité à un fichier d'un système de gestion de fichiers.

29. Il est en outre défini l'expression « Empreinte numérique » au [0005] comme suit : « une donnée produite par une fonction permettant de garantir l'intégrité

du bloc de données, de sorte que si un bit du bloc de données est modifié, l'empreinte numérique sera modifiée. Cette fonction peut être une fonction de hachage, mais pas nécessairement. Une empreinte numérique est parfois nommée clé de hachage, somme de contrôle, empreinte, hash, résumé de message, condensé, condensat ou encore empreinte cryptographique ».

30. Enfin, l'expression « signature numérique » est définie au [006] ainsi : « une empreinte numérique chiffrée à l'aide d'une clé privée d'une paire de clés publique/privée et d'un programme cryptographique asymétrique tel que « pgp » (Pretty Good Privacy) ou son pendant libre « gpg » (Gnu Privacy Guard).
Une signature numérique permet de garantir l'intégrité d'un bloc de données et d'en authentifier le signataire, par analogie avec la signature manuscrite d'un document papier. A noter qu'une signature numérique ayant les propriétés d'une empreinte numérique peut être obtenue en appliquant un programme de chiffrement asymétrique directement au bloc de données. »

31. Dans l'art antérieur, il est connu, pour garantir l'intégrité d'un fichier, d'utiliser des fonctions de hachage telles que présentées dans la description du Brevet, du paragraphe [0009] au paragraphe [0025].

32. La description du Brevet relève que les solutions de l'art antérieur présentent l'inconvénient suivant [0027] :

- « *Actuellement, une empreinte ou une signature ne peut être insérée dans un bloc de données sans que sa valeur s'en trouve modifiée. Un bloc de données ne peut pas contenir ses propres empreintes ou signatures valides. Une empreinte ou signature (…) ne peut donc pas être utilisée à la fois comme élément d'identification ou d'authentification et comme critère de recherche d'un bloc de données indexé par les moteurs de recherche. (…) Rien ne permet de déterminer immédiatement le bloc de données susceptible de correspondre à cette signature. De plus, une fois un bloc de données trouvé, vérifier que ce bloc est conforme à la signature est une opération fastidieuse.* »

33. Le Brevet explique que ces difficultés proviennent de ce que « l'information nécessaire pour identifier ou authentifier un bloc de données doit rester extérieure à ce bloc ». Or, les informations situées à l'extérieur du bloc « peuvent être de ce fait corrompues par un tiers ou frauduleusement accessibles au moyen d'artifices » [0028].

34. Le brevet EP 070 indique qu'il existe un besoin de disposer d'une solution permettant « l'insertion d'une empreinte ou une signature dans un bloc de données de manière contrôlée et éventuellement non-destructive ». Il existe par ailleurs un besoin d'une méthode « capable de vérifier et/ou mettre à jour automatiquement cette empreinte ou signature ». [0029]

35. Le brevet EP 070 propose de pallier ces difficultés en divulguant un procédé de vérification de l'intégrité d'un bloc de données numériques comme il est exposé au paragraphe [0030]. Ce procédé tel que divulgué par le Brevet fonctionne en deux étapes :

- Dans un premier temps, une empreinte est calculée à partir d'un fichier initial puis insérée dans ce fichier afin de produire un fichier « vérifiable ».
- Dans un second temps, lorsqu'il s'agit de contrôler l'intégrité du fichier, le système recherche l'empreinte stockée dans le document, recalcule une nouvelle empreinte en excluant du calcul la zone contenant cette empreinte, puis compare les deux valeurs. Si elles correspondent, le fichier est considéré comme intact ; dans le cas contraire, il est considéré comme modifié. Divers modes de réalisation de ce procédé sont présentés du paragraphe [0031] au paragraphe [0044].

36. Le Brevet enseigne aussi divers modes de réalisation concernant un produit programme d'ordinateur comprenant des portions de fichier de programme enregistrées sur un support lisible par un ordinateur (cf. [0045] à [0050]).

37. Enfin, la description du Brevet présente les différentes figures du Brevet du paragraphe [051] au paragraphe [103].

38. Ainsi, la figure 1 représente des étapes d'un procédé comprenant, le cas échéant, une phase d'insertion (a), une phase de vérification (b) et une phase de mise à jour (c) d'une empreinte dans un bloc de données numérique dans un mode de réalisation : [0051]

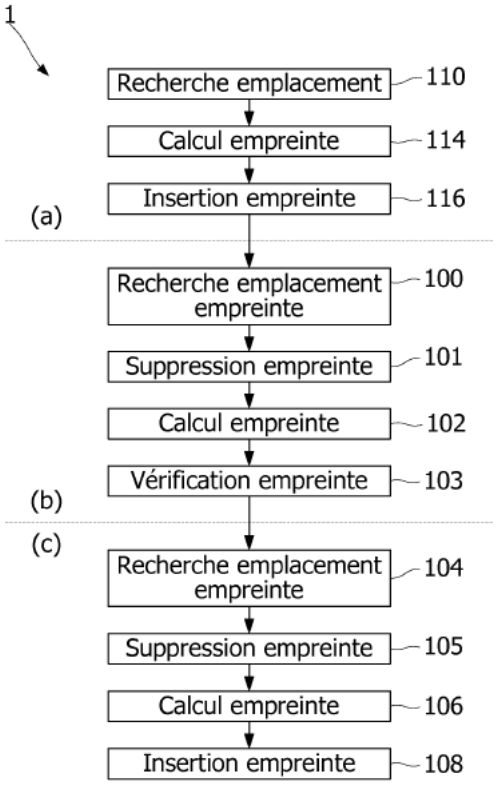


Fig. 1

39. La figure 3 du Brevet représente le bloc de données avant et pendant une vérification d'empreinte d'un bloc de données [0058] :

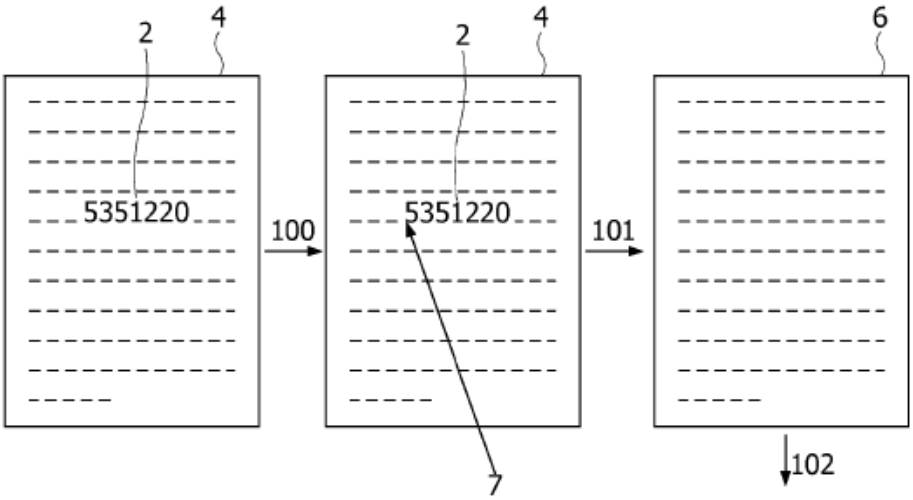


Fig. 3

40. Le Brevet comporte 20 revendications. Les revendications 1, 16 et 18 sont indépendantes. Les revendications 2 à 15 sont dépendantes de la revendication 1 (R1). La revendication 17 est dépendante de la revendication 16. Les revendications 19 et 20 sont dépendantes de la revendication 18. Seules les revendications 1, 2, 4, 7, 8, 10, 11, 14, 16 et 18 du Brevet tel que délivré sont opposées aux défenderesses au titre de la contrefaçon alléguée (cf. Mémoire en demande et récapitulatif des demandes de KEEEX du 7 septembre 2026).

41. Les revendications opposées dans le Brevet tel que délivré se lisent en langue française, comme suit :

« **1**. Procédé de vérification de l'intégrité d'un bloc de données numériques, le procédé comprenant des étapes consistant à :

rechercher, dans un premier bloc de données (4), une empreinte numérique d'identification du premier bloc de données (4), au moyen d'un premier repère (7),

si l'empreinte (2) d'identification du premier bloc de données est trouvée dans le premier bloc de données, calculer une empreinte numérique du premier bloc de données en appliquant une fonction de calcul d'empreinte au premier bloc de données, l'empreinte calculée du premier bloc de données ayant une valeur dépendant de chacun des bits du premier bloc de données en excluant les bits de l'empreinte d'identification (2) trouvée dans le premier bloc de données, et

vérifier l'empreinte d'identification trouvée dans le premier bloc de données en la comparant à l'empreinte calculée du premier bloc de données, une comparaison fausse révélant que le premier bloc de données a été modifié depuis que l'empreinte d'identification a été insérée dans le premier bloc de données,

ou que l'empreinte d'identification a été calculée en appliquant au premier bloc de données une autre fonction de calcul d'empreinte ».

42. **Les revendications 2, 4, 7, 8, 10, 11 et 14 qui sont dépendantes de R 1 sont libellées comme suit :**

2. Procédé selon la revendication 1, dans lequel le premier bloc de données comprend un lien de référence formé à partir d'une autre empreinte d'identification présente dans un second bloc de données, et ayant une valeur dépendant de chacun des bits du second bloc de données en excluant les bits de l'autre empreinte d'identification.

4. Procédé selon l'une des revendications 1 à 3, comprenant des étapes de génération d'un bloc de données vérifiable, consistant à :

rechercher un emplacement d'insertion d'empreinte dans un bloc de données initial (3), au moyen d'un troisième repère,

calculer une troisième empreinte numérique (2) du bloc de données vérifiable en appliquant la fonction calcul d'empreinte au bloc de données initial, la troisième empreinte calculée du bloc de données vérifiable ayant une valeur dépendant de chacun des bits du bloc de données initial, et

générer le bloc de données vérifiable en introduisant la troisième empreinte calculée du bloc de données vérifiable en tant qu'empreinte d'identification du bloc de données vérifiable, à l'emplacement d'insertion trouvé dans le bloc de données initial.

7. Procédé selon l'une des revendications 3 à 5, comprenant plusieurs étapes de calcul d'une empreinte d'un bloc de données et d'introduction de l'empreinte calculée dans le bloc de données en conservant les empreintes déjà insérées dans le bloc de données.

8. Procédé selon l'une des revendications 1 à 7, comprenant une étape de lecture d'une information utile à la localisation et/ou au calcul d'une empreinte d'identification (2), figurant dans un bloc de données (4) contenant l'empreinte d'identification.

10. Procédé selon l'une des revendications 1 à 9, dans lequel l'un des blocs de données comprend une métadonnée comprenant une partie variable exclue du calcul d'empreinte appliqué au bloc de données pour calculer l'empreinte d'identification du bloc de données.

11. Procédé selon la revendication 10, dans lequel l'empreinte d'identification du bloc de donnée se trouve dans la partie variable d'une métadonnée d'identification.

14. Procédé selon l'une des revendications 1 à 13, dans lequel l'introduction de chaque empreinte d'identification (2) dans un bloc de données (4) est effectuée en un emplacement dans le bloc de données, choisi pour ne pas modifier les conditions d'utilisation attendues du bloc de données (4) par un programme logiciel. »

43. **La revendication indépendante 16** est libellée comme suit :

16. Produit programme d'ordinateur comprenant des portions de fichier de programme enregistrées sur un support lisible par un ordinateur, pour mettre en œuvre les étapes du procédé selon l'une des revendications 1 à 15.

44. Enfin, **la revendication indépendante 18** est libellée comme suit :

18. Ensemble de fichiers enregistrés chacun sur un support lisible par un ordinateur, dans lequel chaque fichier contient une empreinte numérique d'identification du fichier, l'empreinte d'identification du fichier étant localisable dans le fichier au moyen d'un repère, l'empreinte d'identification du fichier ayant une valeur calculée en appliquant une fonction de calcul d'empreinte au fichier, la valeur de l'empreinte d'identification dépendant de chacun des bits du fichier en excluant les bits de l'empreinte d'identification du fichier, présente dans le fichier, l'intégrité de chaque fichier de l'ensemble de fichiers étant vérifiable à l'aide du procédé selon l'une des revendications 1 à 15, chaque fichier étant considéré comme un bloc de données »

INTERPRETATION ET CONSTRUCTION DES REVENDICATIONS

45. ***La personne du métier***

Les caractéristiques des revendications doivent être interprétées du point de vue de la personne du métier.

Cadre juridique

L'homme du métier est une entité fictive qui ne peut être assimilée à aucune personne réelle dans le domaine technique de l'invention. Le facteur déterminant n'est pas l'ensemble des connaissances et des compétences individuelles d'une personne, mais plutôt les connaissances générales d'usage, l'expérience moyenne et les aptitudes normales attendues dans le domaine technique concerné à la date de dépôt (UPC_CoA_768/2024, 30 avril 2025, Insulet Corporation c. EOFlow Co).

KEEEX propose la définition suivante : compte tenu du problème technique de la solution présentée et revendiquée, la personne du métier est un technicien spécialisé dans l'utilisation de systèmes de gestion électronique de documents numériques, de partage de données et de systèmes d'archivage. Il est concerné par les besoins d'indexation et marquage de contenus. En revanche, en tant que simple utilisateur d'algorithmes de hachage et de signature, il n'a pas besoin d'une connaissance approfondie en cryptographie (cf page 11 du récapitulatif de ses moyens).

Les défendeurs (mémoire en défense d'ADOBE, §24, ou celui d'OPENAI, page 5 du récapitulatif de ses moyens) proposent la définition suivante : la personne du métier doit être définie comme un ingénieur en informatique spécialisé dans la

sécurité des systèmes d'information, en particulier en cryptographie appliquée et en gestion de l'intégrité des données numériques, justifiant de plusieurs années d'expérience dans ce domaine.

46. Position du Tribunal :
Le Tribunal est convaincu que la définition proposée par les défendeurs est la plus pertinente, en ce que la lecture du Brevet nécessite la compréhension de concepts cryptographiques qui dépassent le cadre d'une simple utilisation d'algorithmes de hachage et de signatures numériques.

Il sera donc retenu la définition suivante : la personne du métier, en l'espèce, est un informaticien ou un ingénieur spécialisé en informatique qui a plusieurs années d'expérience professionnelle dans le domaine de la sécurité informatique et des procédés cryptographiques pour l'intégrité des données.

47. ***Les principes de l'interprétation***

Les principes applicables à l'interprétation des revendications ont été énoncés par la cour d'appel de la Juridiction Unifiée du Brevet dans son ordonnance rendue dans l'affaire UPC_CoA_335/2023, 26 février 2024, NanoString c. 10x Genomics, telle que rectifiée ; voir également cour d'appel, UPC_CoA_1/2024, 13 mai 2024, VusionGroup c. Hanshow ; UPC_CoA_768/2024, 30 avril 2025, Insulet c. EOFlow. Une revendication de brevet constitue non seulement le point de départ, mais aussi le fondement déterminant pour définir l'étendue de la protection conférée par un brevet européen, conformément à l'article 69 CBE, lu conjointement avec le protocole interprétatif de l'article 69 CBE. L'interprétation d'une revendication de brevet ne saurait se limiter au sens strict et littéral des termes employés. Au contraire, la description et les dessins doivent toujours être utilisés comme moyens d'explication pour interpréter la revendication, et non uniquement pour lever d'éventuelles ambiguïtés de celle-ci. Une revendication de brevet doit toujours être interprétée du point de vue de la personne du métier. Celle-ci interprète toujours les caractéristiques d'une revendication à la lumière de l'ensemble des revendications (UPC_CoA_1/2024, 13 mai 2024, VusionGroup c. Hanshow ; UPC_CoA_768/2024, 30 avril 2025, Insulet c. EOFlow ; UPC_CoA_646/2024, 25 novembre 2025, Meril c. Edwards). Ces principes d'interprétation d'une revendication de brevet s'appliquent tant à la question de la contrefaçon qu'à celle de la validité du brevet (NanoString c. 10x Genomics).

En appliquant ces principes, l'objectif est de combiner une protection adéquate pour le titulaire du brevet et une sécurité juridique suffisante pour les tiers.

48. **Concernant la revendication 1, les parties s'opposent sur l'interprétation des termes « signatures et empreintes numériques » :**

49. Selon KEEEX, l'empreinte d'identification ne peut pas être réalisée par une signature numérique, en s'appuyant sur les arguments suivants (cf. page 13 récapitulatif de ses moyens) :

Après le paragraphe [0006] du brevet EP'070, une signature numérique désigne une empreinte numérique chiffrée à l'aide d'une clé privée d'une paire de clés publique/privée et d'un programme cryptographique asymétrique.

Les termes empreinte et signature numérique désignent donc clairement des objets différents, la signature étant obtenue à partir d'une empreinte qui est transformée en signature par un programme cryptographique asymétrique et une clé privée d'un signataire.

Le paragraphe [0074] du Brevet tel que délivré présentait clairement un autre mode de réalisation (introduit par « Dans un deuxième mode de réalisation ») dans lequel l'empreinte est insérée dans le bloc de données sous la forme d'une signature numérique, ce qui ne signifie rien d'autre que la position de l'empreinte dans le bloc de données est occupée par une signature numérique.

Par ailleurs, dans toute la description, il n'existe aucune ambiguïté sur l'usage des termes « empreinte » et « signature ». A aucun moment, l'un de ces termes n'est utilisé pour l'autre et, lorsque ces deux objets sont concernés, ils sont tous les deux mentionnés sous la forme « empreinte et/ou signatures » (cf. paragraphes [0087], [0089] et [0095]). Par conséquent, les termes « empreinte » et « signature » désignent clairement des objets différents dans le Brevet EP 070.

Selon KEEEX, une signature est le résultat d'une opération cryptographique combinant un bloc de données (ou son empreinte) et un identifiant d'un signataire (la clé privée du signataire). Par conséquent, une signature n'identifie pas un bloc de données, mais un objet associant un bloc de données et un signataire qui est une entité totalement distincte du bloc de données. Il en résulte qu'un même bloc de données peut avoir une infinité de signataires et donc une infinité de signatures différentes. Une signature ne peut donc pas assurer une fonction d'identification d'un bloc de données au même titre qu'une empreinte d'identification du bloc de données, dont le calcul ne reçoit qu'une seule donnée d'entrée, à savoir le contenu du bloc de données. Enfin, KEEEX se réfère à l'attestation du Professeur Quisquater (sa pièce 37) selon laquelle : « La valeur d'une signature n'est pas du tout une (sorte) d'empreinte car elle est associée à un émetteur qui possède une clé secrète correspondante à son identité personnelle. Il s'agit donc d'une valeur dépendante du contexte, donc variable par définition. Il faudra bien s'assurer que ce contexte est correct. » (cf. livret d'audience -ou booklet- de KEEEX, au support des plaidoiries de l'audience orale, page 4).

50. <u>Selon les défendeurs, notamment ADOBE et OPENAI, le brevet EP 070 ne tient pas compte des différences entre l'empreinte numérique et la signature numérique</u> :

Les défendeurs regroupent ces deux concepts sous le terme plus général de « empreinte numérique ». Ce dernier est très large et englobe également les signatures numériques, comme exposées aux paragraphes [0006] et [0044] du Brevet (mémoire en défense d'Adobe, §13 et 14, page 19). Les défendeurs développent cette position dans toutes leurs écritures et la confirment à

l'audience orale lors de la présentation du Brevet par le représentant d'OpenAI. Ce dernier rappelle la définition donnée par le Brevet lui-même au [0005] et relève que dès le [0006] consacré aux définitions de termes du Brevet, il est mentionné expressément que « signature numérique désigne une « empreinte numérique » qui est chiffrée (…). Il en ressort qu'une signature est une sous-catégorie de l'empreinte numérique. Ceci est confirmé au [0062] du Brevet : « (…) le procédé 1 correspond à un procédé d'identification, de vérification et d'authentification d'un bloc de données au sein duquel une empreinte a été insérée de manière contrôlée (…) ». Ceci est également confirmé par divers modes de réalisation divulgués dans le Brevet, comme au paragraphe [0074] « l'empreinte 2 est insérée dans le bloc de données 4 sous forme d'une signature numérique (…), ce qui signifie que lorsqu'on utilise une empreinte chiffrée, il s'agit alors d'une « signature numérique ». Le paragraphe [0076] enseigne que « selon un mode de réalisation, une métadonnée de référence insérée dans le bloc de données, contient l'empreinte ou la signature d'un autre bloc de données afin d'établir un lien de référence (…) » et par d'autres modes de réalisation divulgués aux paragraphes 92, 93 ou 95, ainsi dans ce dernier, il est mentionné « que ce mode permet de traiter des blocs de données de multiples occurrences d'empreintes et/ou signatures (…). Enfin, la revendication 15 du Brevet est décisive car elle mentionne « un procédé selon l'une des revendications 1 à 14, dans lequel l'empreinte d'identification insérée dans un bloc de données est une signature numérique (…) ». Selon les défendeurs, les remarques de l'attestation du Professeur Quisquater à laquelle se réfère KEEEX (pièce 37 de KEEEX) ne seraient pas pertinentes dans le cadre de l'interprétation des termes du Brevet car elles sont mentionnées hors du contexte du brevet, or, ces termes doivent être interprétés dans le contexte du brevet.

51. Position du Tribunal :

Le Tribunal n'est pas convaincu par le raisonnement soutenu par le demandeur concernant une limitation de la revendication 1 aux seules empreintes de type « hash » (ou « hachage »). Au contraire, tout le Brevet enseigne que la revendication 1 couvre également les signatures numériques.

52. Certes, il est exact que la description distingue conceptuellement l'empreinte numérique de la signature numérique. Le paragraphe [0005] définit l'empreinte numérique comme une donnée permettant notamment de vérifier l'intégrité d'un bloc de données, tandis que le paragraphe [0006] présente la signature numérique comme une empreinte numérique chiffrée à l'aide d'une clé privée. Le brevet donc identifie deux objets techniques distincts et, d'un point de vue technique et cryptographique, une signature n'est pas identique à une simple valeur de hachage. De plus, le paragraphe [0006] confirme qu'une signature numérique permet de garantir l'intégrité d'un bloc de données, comme le permet une simple empreinte.

53. Cependant, la question n'est pas de savoir si un hash et une signature sont techniquement différents, mais d'évaluer comment la personne du métier

comprendrait l'expression revendiquée « empreinte numérique d'identification » dans le cadre de la revendication 1 du brevet en cause. Rien dans la revendication 1 n'exclut expressément les signatures numériques. La revendication ne mentionne ni fonction de hachage, ni hash, ni algorithme déterminé. Elle vise simplement une « empreinte numérique d'identification ». Si le déposant avait souhaité limiter la revendication aux seules empreintes non signées, il lui était parfaitement possible de le faire. Une telle limitation n'apparaît pas dans le texte revendiqué.

54. Cette lecture est confirmée par la description prise dans son ensemble. Le brevet ne présente jamais les signatures comme étrangères à l'invention. Au contraire, plusieurs passages de la description envisagent explicitement l'utilisation de signatures numériques dans le cadre du procédé revendiqué. Le paragraphe [0074] décrit précisément la situation dans laquelle l'empreinte d'identification est constituée par une signature numérique et explique comment la vérification est réalisée.

- [0074] *Dans un deuxième mode de réalisation du procédé 1, 1', l'empreinte 2 est insérée dans le bloc de données 4 sous la forme d'une signature numérique générée en chiffrant l'empreinte du bloc de données à l'aide d'une clé privée d'une paire de clés publique/privée. La vérification 102 de la signature numérique peut consister à déchiffrer la signature avec la clé publique de la paire de clés publique/privée, pour obtenir une empreinte déchiffrée du bloc de données, et à vérifier que l'empreinte déchiffrée correspond à celle calculée à partir du bloc de données modifié 6 dans lequel l'empreinte 2 a été supprimée à l'étape de suppression 101 ou de remplacement 101'. A noter que l'empreinte 2 peut également être une signature calculée en chiffrant non pas une empreinte du bloc de données, mais directement le bloc de données, avec la clé privée. Dans ce cas, la vérification de la signature peut être effectuée en déchiffrant la signature à l'aide de la clé publique correspondante et en comparant le bloc de données déchiffré ainsi obtenu avec le bloc de données modifié.*

55. Les paragraphes [0075], [0077], [0092] et [0093] traitent également de l'utilisation de signatures dans le fonctionnement de l'invention. Un lecteur objectif du brevet, comme l'est la personne du métier, comprend donc que le rédacteur considérait les signatures numériques comme faisant partie des réalisations couvertes par son enseignement.

56. L'existence de la revendication dépendante 15 apparaît encore plus significative :

- 15. *Procédé selon l'une des revendications 1 à 14, dans lequel l'empreinte d'identification (2) insérée dans un bloc de données est une signature numérique générée par un calcul cryptographique asymétrique utilisant une clé privée d'une paire de clés publique/privée, et la vérification d'empreinte (102) comprend une étape de déchiffrement de la signature numérique trouvée dans le bloc de données, avec la clé publique de la paire de clés publique/privée, la clé publique pouvant se trouver dans une métadonnée du bloc de données.*

57. Cette revendication prévoit explicitement que l'empreinte d'identification est une signature numérique, c'est-à-dire que la signature n'est pas, par exemple, ajoutée à l'empreinte : la signature est l'empreinte. Conformément aux principes ordinaires d'interprétation des revendications, une revendication dépendante ajoute normalement une limitation particulière à un objet déjà couvert par la revendication dont elle dépend. Si la revendication 1 excluait par principe les signatures numériques, la revendication 15 serait dépourvue de logique technique puisqu'elle introduirait un objet situé en dehors du champ de la revendication indépendante. L'interprétation la plus naturelle est, au contraire, que la revendication 1 couvre de manière générale les empreintes d'identification, parmi lesquelles figurent les signatures numériques, la revendication 15 se bornant à protéger explicitement cette réalisation particulière.

58. Le Tribunal n'est pas davantage convaincu par l'argument de KEEEX selon lequel la caractéristique 1.5 imposerait nécessairement une comparaison directe de deux « hash ». La revendication exige qu'une vérification soit effectuée en comparant l'empreinte trouvée à l'empreinte calculée, mais elle ne précise pas quelles opérations intermédiaires peuvent être nécessaires avant cette comparaison. Lorsqu'une signature numérique est utilisée, le procédé peut parfaitement comporter une étape préalable permettant d'obtenir l'empreinte sous-jacente à partir de la signature avant de procéder à la comparaison. Cette lecture est précisément celle qui est décrite dans les paragraphes [0074] et [0075].

59. Pour ces raisons, le Tribunal considère qu'il est conforme au texte des revendications, à la structure du brevet et à l'enseignement de la description de considérer que la revendication 1 couvre à la fois les empreintes non signées et les signatures numériques. Le fait que la description distingue ces deux notions ne conduit pas à exclure les signatures du champ de la revendication ; il conduit seulement à reconnaître qu'une signature constitue une forme particulière d'empreinte d'identification mise en œuvre dans certains modes de réalisation du brevet.

60. Le Tribunal relève en outre que KEEEX a cherché, dans le cadre de ses demandes de modification fondées sur la règle 30 RdP, à supprimer la revendication 15 ainsi qu'à modifier corrélativement plusieurs passages de la description, en particulier les paragraphes [0044] et [0074].

61. L'objectif affiché de ces modifications était de clarifier que l' « empreinte numérique d'identification » visée par le brevet ne doit pas être comprise comme une signature numérique, mais comme une empreinte de type hachage. KEEEX soutient ainsi que la revendication 15 et certains passages de la description entretiennent une confusion entre deux concepts techniques distincts et ne reflètent pas correctement ce qu'elle considère être l'enseignement véritable de l'invention. Ce dernier argument, qui n'a été avancé par KEEEX qu'au stade de sa réponse au mémoire en défense, n'est pas convaincant.

62. Le Tribunal relève en outre que, sur question du Juge Rapporteur, le demandeur a expressément indiqué que ses demandes de modification du brevet étaient conditionnelles au sens de R. 30.1 RdP (Communication via CMS du 24/06/2026). Cela signifie que le demandeur ne soutient sa demande de modification du brevet que si la version telle que délivrée est invalidée dans le cadre de ce litige. Ceci est confirmé dans le récapitulatif des demandes actualisées déposé par KEEEX, à la demande du Juge Rapporteur, dans le CMS en date du 7 septembre 2026, comme suit :

> **DECLARER** recevable la société KEEEX en tant que titulaire du Brevet européen EP 2 949 070 B1 ;
>
> **DECLARER** valable l'ensemble des revendications du Brevet européen EP 2 949 070 B1, **à défaut**,
>
> **FAIRE DROIT** à la requête principale de modification du Brevet européen EP 2 949 070 B1 concernant la suppression de la revendication 15, **à défaut**,
>
> **FAIRE DROIT** successivement aux requêtes subsidiaires, dans l'ordre dans lequel elles sont présentées (de la première requête à la onzième requête subsidiaire) ;
>
> **MODIFIER** le Brevet européen EP 2 949 070 B1 conformément aux requêtes retenues, afin de clarifier la portée du Brevet et de préserver sa validité ;

63. Par conséquent, KEEEX n'entendait pas abandonner le Brevet dans sa version telle que délivrée, mais a seulement sollicité une modification à titre subsidiaire dans le cas où la version initiale serait déclarée invalide par le Tribunal. Le Tribunal a donc interprété les termes discutés, au regard de la version telle que délivrée.

64. **L'expression « bloc de données numériques »**

Concernant le terme « Bloc de données numériques », la définition est donnée dans la description au [0003] du Brevet comme suit : « désigne tout fichier ou document numérique ou toute partie d'un tel fichier ou document, le terme fichier ne devant être compris comme limité à un fichier d'un système de gestion de fichiers ».

Rien dans la revendication 1.1 ne limite le bloc de données à un format particulier.

Il peut notamment s'agir d'un document PDF, d'une image, d'un fichier audio ou vidéo, d'un fichier XML, d'une archive ou plus généralement de tout ensemble de données numériques susceptible de contenir une empreinte d'identification.

65. **Conséquences de l'interprétation sur la construction des revendications**

La revendication 1 en langue française se lit, selon le découpage des caractéristiques proposé par ADOBE (Mémoire en demande, § 27) et non contesté par les autres parties, et que le Tribunal adopte comme suit :

- Procédé de vérification de l’intégrité d'un bloc de données numériques, le procédé comprenant des étapes consistant à :
- rechercher, dans un premier bloc de données (4), une empreinte numérique d'identification du premier bloc de données (4), au moyen d’un premier repère (7),
- si l’empreinte (2) d'identification du premier bloc de données est trouvée dans le premier bloc de données, calculer une empreinte numérique du premier bloc de données en appliquant une fonction de calcul d'empreinte au premier bloc de données,
- l’empreinte calculée du premier bloc de données ayant une valeur dépendant de chacun des bits du premier bloc de données en excluant les bits de l’empreinte d’identification (2) trouvée dans le premier bloc de données, et
- vérifier l’empreinte d'identification trouvée dans le premier bloc de données en la comparant à l’empreinte calculée du premier bloc de données, une comparaison fausse révélant que le premier bloc de données a été modifié depuis que l’empreinte d’identification a été insérée dans le premier bloc de données, ou que l’empreinte d’identification a été calculée en appliquant au premier bloc de données une autre fonction de calcul d’empreinte.

66. **<u>Caractéristique 1.1</u> :** ***Procédé de vérification de l’intégrité d'un bloc de données numériques, le procédé comprenant des étapes consistant à***

La caractéristique 1.1 constitue le préambule de la revendication et définit l'objet général de l'invention comme étant un procédé de vérification de l'intégrité d'un bloc de données numériques.

67. La personne du métier comprendrait que l'objectif du procédé (« vérification de l'intégrité ») est de déterminer si le contenu d'un bloc de données a été modifié depuis la création ou l'insertion de l'empreinte d'identification.

68. Le terme « intégrité » doit être compris dans son sens informatique habituel, c’est-à-dire, propriété selon laquelle les données n'ont pas été altérées ou modifiées.

69. Cette lecture est d'ailleurs cohérente avec la fin de la revendication 1.5, qui prévoit qu'une comparaison négative révèle que « le premier bloc de données a été modifié ». La finalité première du procédé est donc la vérification de l'intégrité du contenu (pas l'authentification d'un auteur, la preuve d'origine ou la certification d'un signataire, etc.).

70. En revanche, la revendication n'exige pas que la solution soit indépendante du format utilisé. Le bloc de données peut parfaitement avoir une structure propre à un format déterminé.

71. Comme indiqué dans l’interprétation des termes contestés, il est rappelé que l’expression « bloc de données » doit être comprise dans le contexte du brevet dans son sens large.

72. En résumé, la caractéristique 1.1 doit être comprise comme définissant un procédé destiné à déterminer si un bloc de données numériques, entendu comme tout fichier, document ou ensemble de données numériques, a conservé son intégrité, c'est-à-dire n'a pas été modifié.

73. **<u>Caractéristique 1.2</u> :** ***rechercher, dans un premier bloc de données (4), une empreinte numérique d'identification du premier bloc de données (4), au moyen d'un premier repère***

La caractéristique 1.2 exige qu'une empreinte numérique d'identification soit recherchée à l'intérieur même du bloc de données et que cette recherche soit effectuée au moyen d'un repère.

74. Cette étape intervient avant tout calcul d'empreinte. La personne du métier comprend donc que l'empreinte d'identification est déjà présente dans le bloc de données lorsqu'il commence la procédure de vérification, car le verbe « rechercher » implique une opération de localisation.

75. L'étape ne consiste pas simplement à lire une valeur dont l'emplacement serait connu à l'avance. Le procédé prévoit au contraire l'identification de l'emplacement de l'empreinte à partir d'un élément de repérage (« repère ») présent dans le bloc de données.

76. Le terme « repère » (« marker ») est un terme général, il n’est pas défini de façon particulière dans le Brevet.

77. La personne du métier comprend donc qu'une opération préalable est nécessaire afin de déterminer où se trouve l'empreinte d'identification qui devra ensuite être vérifiée, l'empreinte recherchée devant être présente à l'intérieur du bloc de données lui-même. Cette caractéristique distingue l'invention des systèmes de l’art antérieur dans lesquels l'empreinte est conservée dans une base de données externe ou dans un fichier séparé ou des systèmes dans lesquels l'empreinte est fournie par un tiers au moment de la vérification.

78. La personne du métier comprend qu'un repère est une information permettant de localiser l'empreinte dans le bloc de données, mais la revendication n'impose pas de forme particulière.

79. Selon la description, le repère peut donc être une chaîne de caractères, une balise (« tag »), un champ structuré, une indication de position ou toute autre information permettant d'accéder à l'emplacement de l'empreinte.

80. En revanche, le texte de la revendication exige un lien fonctionnel entre le repère et la localisation de l’empreinte : le repère doit permettre de retrouver l'empreinte recherchée.

81. La caractéristique 1.2 n'exige pas que le repère soit situé immédiatement à côté de l'empreinte, que le repère fasse partie de l'empreinte, que le repère ait une forme particulière ou que le repère soit indépendant du format du fichier.

82. En résumé, la caractéristique 1.2 doit être comprise comme exigeant qu'une empreinte numérique d'identification préalablement insérée dans le bloc de données soit localisée à l'intérieur de ce bloc au moyen d'une information de repérage permettant d'en déterminer l'emplacement. Le « premier repère » est une information servant à localiser l'empreinte d'identification, sans que la revendication impose une forme particulière de ce repère ni sa position exacte dans le bloc de données.

83. **<u>Caractéristique 1.3</u> :** ***si l'empreinte (2) d'identification du premier bloc de données est trouvée dans le premier bloc de données, calculer une empreinte numérique du premier bloc de données en appliquant une fonction de calcul d'empreinte au premier bloc de données,***

La caractéristique 1.3 décrit l'étape de recalcul de l'empreinte qui servira ensuite à la vérification. Après avoir localisé l'empreinte d'identification conformément à la caractéristique 1.2, le procédé calcule une nouvelle empreinte du bloc de données au moyen d'une fonction de calcul d'empreinte.

84. La formulation conditionnelle « si l'empreinte d'identification est trouvée » indique que le calcul prévu par la caractéristique 1.3 n'intervient que si l'étape de recherche de la caractéristique 1.2 a permis de localiser une empreinte d'identification dans le bloc de données.

85. La revendication décrit ainsi une succession logique d'étapes : recherche de l'empreinte ; localisation de l'empreinte ; calcul d'une nouvelle empreinte ; comparaison.

86. La revendication exige le calcul d'une nouvelle empreinte (« calculer une empreinte numérique du premier bloc de données »). La personne du métier comprend qu'il s'agit d'une valeur obtenue pendant la procédure de vérification afin de servir de référence pour la comparaison prévue à la caractéristique 1.5.

87. En indiquant « en appliquant une fonction de calcul d'empreinte », la revendication ne se limite pas expressément à une fonction spécifique ni à la nature de cette fonction.

88. La revendication ne mentionne qu'une « fonction de calcul d'empreinte » et, à ce stade, reste technologiquement ouverte. En résumé, la caractéristique 1.3 doit être comprise comme exigeant que, lorsqu'une empreinte d'identification a été localisée dans le bloc de données, une nouvelle empreinte du bloc de données soit calculée par application d'une fonction de calcul d'empreinte au bloc de données. Cette étape fournit la valeur de référence destinée à être utilisée lors de la vérification ultérieure prévue par la caractéristique 1.5. La revendication n'impose pas d'algorithme particulier ni ne limite expressément la fonction de calcul à une fonction de hachage déterminée. Ceci est confirmé au [0005] du Brevet indiquant expressément que « cette fonction peut être une fonction de hachage, mais pas nécessairement ».

89. **<u>Caractéristique 1.4</u> :** ***l'empreinte calculée du premier bloc de données ayant une valeur dépendant de chacun des bits du premier bloc de données en excluant les bits de l'empreinte d'identification (2) trouvée dans le premier bloc de données.***

    La caractéristique 1.4 précise la manière dont l'empreinte calculée de la caractéristique 1.3 doit être obtenue.

90. Elle exige que la valeur de l'empreinte calculée dépende de l'ensemble du contenu du bloc de données, à l'exception des bits correspondant à l'empreinte d'identification qui a été préalablement trouvée dans le bloc de données.

91. "l'empreinte calculée [...] ayant une valeur dépendant de chacun des bits du premier bloc de données » : la personne du métier comprend que l'empreinte doit être calculée à partir du contenu du bloc de données de telle sorte qu'une modification d'un bit pris en compte dans le calcul soit susceptible de modifier la valeur obtenue.

92. L'expression "dépendant de chacun des bits" ne signifie toutefois pas nécessairement qu'une relation mathématique doit prendre en compte "each and every bit". Elle exprime plutôt que le calcul porte sur l'ensemble des données prises en compte, "en excluant les bits de l'empreinte d'identification".

93. Cette dernière limitation est essentielle : la revendication impose que les bits constituant l'empreinte d'identification localisée à l'étape 1.2 ne participent pas au calcul de l'empreinte réalisée à l'étape 1.3.

94. La personne du métier comprend immédiatement la raison de cette exclusion : si l'empreinte d'identification était incluse dans le calcul, l'insertion de cette empreinte modifierait elle-même le contenu dont dépend l'empreinte calculée, ce qui empêcherait la comparaison ultérieure prévue à la caractéristique 1.5. La revendication résout donc le problème de l'auto-référence en excluant du calcul la zone contenant l'empreinte insérée.

95. La question la plus importante est de savoir ce qui est exactement exclu, c’est-à-dire la portée de l'exclusion.

96. Le texte de la revendication 1 vise expressément les bits de l'empreinte d'identification trouvée et, pris isolément, ce texte désigne uniquement les bits correspondant à l'empreinte elle-même. Il ne mentionne pas une zone plus large, des métadonnées associées, des champs annexes ou des structures contenant l'empreinte.

97. Pour mieux comprendre ce point, il convient de la lire à la lumière des revendications dépendantes 10 et 11, sans limiter la revendication 1, ainsi que de certains paragraphes de la description.

98. En effet, les revendications 10[1] et 11[2] prévoient explicitement des métadonnées comprenant une partie variable, laquelle peut être exclue du calcul et dans laquelle l'empreinte peut être stockée.

99. La personne du métier lisant l'ensemble du brevet comprend donc que l'exclusion n'est pas nécessairement limitée, dans tous les modes de réalisation, à la seule valeur binaire de l'empreinte. Les revendications 10 et 11 enseignent au contraire que des zones plus larges de données variables peuvent également être exclues du calcul.

100. La caractéristique 1.4 doit être interprétée en tenant compte, à la fois, de son texte, qui vise expressément l'exclusion des bits de l'empreinte d'identification, et de la description et des revendications dépendantes 10 et 11, qui montrent que le Brevet envisage également des modes de réalisation comportant des zones variables plus étendues.

101. La caractéristique 1.4 ne doit donc pas être interprétée comme imposant nécessairement une exclusion limitée à la seule chaîne représentant l'empreinte.

102. En résumé, la caractéristique 1.4 exige que l'empreinte calculée soit déterminée à partir du contenu du bloc de données tout en excluant du calcul les bits correspondant à l'empreinte d'identification précédemment localisée. Cette exclusion permet la vérification d'une empreinte insérée dans le bloc de données sans que sa présence n'affecte le résultat du calcul. Lue à la lumière de la description et des revendications 10 et 11, cette caractéristique n'exclut pas que des données variables associées à l'empreinte puissent également être exclues du calcul dans certains modes de réalisation du brevet. Au contraire, il n'y a aucun risque à prendre en compte d'autres données non variables dans le calcul, car celles-ci ne peuvent justement pas être modifiées et il n'y a – du fait de leur invariabilité - donc aucun risque que les données soient corrompues.

103. **Caractéristique 1.5 :** ***vérifier l'empreinte d'identification trouvée dans le premier bloc de données en la comparant à l'empreinte calculée du premier bloc de données, une comparaison fausse révélant que le premier bloc de données a été modifié depuis que l'empreinte d'identification a été insérée dans le premier bloc de données, ou que l'empreinte d'identification a été calculée en appliquant une autre fonction de calcul d'empreinte.***

La caractéristique 1.5 définit l'étape finale du procédé. Après avoir localisé l'empreinte d'identification (caractéristique 1.2) et calculé une nouvelle empreinte (caractéristiques 1.3 et 1.4), le système procède à une vérification en

[1] *10.1 Procédé selon l'une des revendications 1 à 9, dans lequel l'un des blocs de données comprend une méta-donnée*

10.2 comprenant une partie variable exclue du calcul d'empreinte appliqué au bloc de données pour calculer l'empreinte d'identification du bloc de données.

[2] *11. Procédé selon la revendication 10, dans lequel l'empreinte d'identification du bloc de donnée se trouve dans la partie variable d'une métadonnée d'identification.*

comparant les deux valeurs. Cette étape constitue le résultat du mécanisme de contrôle d'intégrité décrit par la revendication.

104. La revendication ne prévoit pas une vérification du document en général ni une vérification de l'auteur du document : ce qui est vérifié est spécifiquement l'empreinte d'identification trouvée dans le bloc de données.

105. La personne du métier comprend que la vérification porte sur la cohérence entre l'empreinte stockée dans le fichier et le contenu actuel du fichier.

106. Le terme central de cette caractéristique est le verbe « comparer ». Dans son sens ordinaire, « comparer » consiste à confronter deux valeurs afin de déterminer si elles correspondent ou non.

107. La revendication ne précise pas davantage la forme exacte de la comparaison, les opérations préparatoires éventuellement nécessaires ou l'algorithme utilisé pour effectuer cette comparaison. En revanche, le résultat attendu est clairement défini : il s'agit d'établir si l'empreinte trouvée correspond (est la même que) à l'empreinte recalculée.

108. La personne du métier lirait cette caractéristique comme exigeant simplement l'existence de deux valeurs :
l'empreinte trouvée dans le bloc de données ;
l'empreinte calculée lors de la vérification.
Ces deux valeurs sont ensuite confrontées afin de vérifier leur concordance.

109. En résumé, la caractéristique 1.5 exige qu'une vérification soit réalisée en confrontant l'empreinte d'identification trouvée dans le bloc de données à l'empreinte recalculée conformément aux caractéristiques 1.3 et 1.4, afin de déterminer si ces deux valeurs correspondent. Une différence entre les deux valeurs révèle soit une modification du bloc de données après l'insertion de l'empreinte d'identification, soit l'utilisation d'une fonction de calcul différente. La revendication exige l'existence d'une comparaison entre l'empreinte trouvée et l'empreinte calculée, sans définir expressément les opérations préparatoires éventuellement nécessaires avant cette comparaison.

VALIDITÉ DU BREVET

1) Revendication 1 (Brevet tel que délivré)

110. **Sur l'extension d'objet (art. 123.2 CBE)**

Cadre juridique :

Il y a extension de l'objet lorsque la revendication telle que délivrée s'étend au-delà du contenu de la demande telle que déposée. Pour déterminer s'il y a extension de l'objet, le Tribunal doit donc, en premier lieu, déterminer ce que la personne du métier, en faisant appel à ses connaissances générales et en se plaçant d'un point de vue objectif à la date de dépôt, déduirait directement et sans ambiguïté de l'ensemble de la demande telle que déposée. L'objet

implicitement divulgué, c'est-à-dire celui qui constitue une conséquence claire et non ambiguë de ce qui est expressément mentionné, doit également être considéré comme faisant partie de ce contenu (UPC_CoA_764/2024, 2 octobre 2025, expert klein GmbH c. Seoul Viosys Co).

111. Arguments des défendeurs :

Les défendeurs soutiennent que le brevet EP'070 délivré va au-delà du contenu de la demande telle qu'elle a été déposée, selon les arguments suivants :

- une sous-caractéristique de la caractéristique 1.5 de la revendication 1 (mentionnée à la fin de 1.5 et soulignée ci-dessous) n'a été intégrée dans la revendication 1 qu'au cours de l'examen du Brevet avant sa délivrance et n'était pas divulguée à l'origine. (cf. pièce DTMV 3.2) :
- « vérifier l'empreinte d'identification trouvée dans le premier bloc de données en la comparant à l'empreinte calculée du premier bloc de données, une comparaison fausse révélant que le premier bloc de données a été modifié depuis que l'empreinte d'identification a été insérée dans le premier bloc de données, ou que l'empreinte d'identification a été calculée en appliquant au premier bloc de données une autre fonction de calcul d'empreinte. »

112. Cette sous-caractéristique de la caractéristique 1.5 absente dans la demande initiale et ajoutée dans 1.5 constitue, selon les défendeurs, une extension de l'objet du brevet EP'070 au-delà du contenu de la demande telle qu'elle a été déposée.

113. Selon KEEEX, les deux caractéristiques ont été ajoutées pour préciser l'effet de la comparaison mentionnée qui porte sur l'empreinte d'identification trouvée dans le bloc de données et l'empreinte calculée sur ce bloc de données, à savoir:

« une comparaison fausse révélant que le premier bloc de données a été modifié depuis que l'empreinte d'identification a été insérée dans le premier bloc de données »,

« une comparaison fausse révélant que l'empreinte d'identification a été calculée en appliquant au premier bloc de données une autre fonction de calcul d'empreinte ».

114. KEEEX soutient que ces deux caractéristiques ne font qu'expliciter les possibilités pouvant conduire à une comparaison fausse. Il ne semble pas y en avoir d'autres. En effet, la logique élémentaire impose que pour vérifier un calcul, on le répète et on vérifie la cohérence des résultats. Si une divergence apparaît dans ces résultats, cela signifie que les deux calculs ne sont pas identiques. En outre, pour que deux calculs soient identiques, deux conditions doivent être respectées, à savoir que les données sur lesquelles portent ces calculs soient identiques (caractéristique 1), et que le mode opératoire appliqué par ces deux calculs soit le même (caractéristique 2).

115. Le paragraphe [0062] exprime d'une autre manière comment est réalisée la vérification revendiquée : « le procédé permet de retrouver par suppression de l'empreinte contenue dans le bloc de données, la valeur du bloc de données à partir de laquelle l'empreinte est supposée avoir été calculée, puis de vérifier si cette supposition est juste ou si elle est fausse par comparaison de l'empreinte supprimée à l'empreinte calculée ».

116. Cette vérification correspond exactement au cadre d'application de la logique élémentaire rappelée au paragraphe précédent puisqu'il s'agit de répéter un même calcul appliqué à une supposée même donnée et de comparer les résultats obtenus.

117. La caractéristique 1 apparaît presque littéralement à la fin du paragraphe [0062] : « Si la comparaison est fausse, le bloc de données 4 est corrompu ou a simplement été modifié ». Il peut être également affirmé que si le bloc de données a été corrompu, cela signifie qu'il a été modifié.

118. En ce qui concerne la caractéristique 2, les paragraphes [0071] et [0072] du Brevet EP 070 évoquent la condition sur le mode opératoire, puisqu'ils concernent l'enregistrement et la fourniture d'une information spécifiant le mode opératoire permettant d'assurer l'opération de vérification. En effet, le paragraphe [0071] indique que différents calculs ou algorithmes peuvent être mis en œuvre pour calculer l'empreinte et que l'empreinte peut être associée au nom de l'algorithme de calcul ayant servi à la génération de l'empreinte. Le paragraphe [0072] précise que lorsque l'empreinte 2 n'indique pas en elle-même le type de calcul ou d'algorithme de calcul ayant permis sa génération, cette information peut être fournie dans une métadonnée insérée dans le bloc de données.

119. Ainsi, selon le demandeur, les deux caractéristiques qui ont été ajoutées à la revendication 1 découlent directement et sans équivoque du texte tel que déposé du Brevet EP 070, des connaissances générales et de la logique élémentaire.

120. <u>Position du Tribunal :</u>

Il n'est pas contesté que l'ajout de la sous-caractéristique finale de 1.5 libellée comme suit : « *ou que l'empreinte d'identification a été calculée en appliquant une autre fonction de calcul d'empreinte* » a été introduit pendant la phase de la délivrance. Il s'agit d'un ajout illicite pour les raisons invoquées en défense, en ce qu'il induit un élargissement du périmètre de protection par rapport à la demande telle que déposée. En effet, la demande telle que déposée ne divulguait pas qu'une comparaison fausse puisse, en elle-même, révéler l'emploi d'une fonction de calcul différente. La revendication 1 s'étend donc au-delà du contenu de la demande telle que déposée.

121. Il s'en déduit que la revendication 1 du Brevet tel que délivré est nulle sur le fondement de l'art. 123(2) de la Convention de Munich (CBE).

122. Cependant, le Tribunal relève que la requête subsidiaire n° 11 (RS 11) en modification du Brevet proposée par KEEEX (pièce KEEEX 29.11) a traité cette

défaillance en supprimant l'ajout de la sous-caractéristique contestée. En effet, RS 11 se lit comme suit :

REVENDICATIONS

1. Procédé de vérification de l'intégrité d'un bloc de données numériques, le procédé comprenant des étapes consistant à :

rechercher, dans un premier bloc de données (4), une empreinte numérique d'identification du premier bloc de données (4), au moyen d'un premier repère (7),

si l'empreinte (2) d'identification du premier bloc de données est trouvée dans le premier bloc de données, calculer une empreinte numérique du premier bloc de données en appliquant une fonction de calcul d'empreinte au premier bloc de données, l'empreinte calculée du premier bloc de données ayant une valeur dépendant de chacun des bits du premier bloc de données en excluant les bits de l'empreinte d'identification (2) trouvée dans le premier bloc de données, et

vérifier l'empreinte d'identification trouvée dans le premier bloc de données en la comparant à l'empreinte calculée du premier bloc de données, une comparaison fausse révélant que le premier bloc de données a été modifié depuis que l'empreinte d'identification a été insérée dans le premier bloc de données~~, ou que l'empreinte d'identification a été calculée en appliquant au premier bloc de données une autre fonction de calcul d'empreinte~~.

123. Surabondamment, le Tribunal se propose d'examiner la validité du Brevet tel que délivré au regard de la nouveauté (art. 54 CBE).

124. Les défendeurs ont opposé divers documents, notamment celui intitulé « KANAI » (ou « D5 », selon les écritures d'ADOBE).

125. **Sur la nouveauté (art. 54.1 CBE)**

126. Cadre juridique :

Conformément à l'article 54(1) CBE, une invention est considérée comme nouvelle si elle n'est pas comprise dans l'état de la technique. Un enseignement technique n'est pas compris dans l'état de la technique s'il se distingue, par au moins une de ses caractéristiques connues, de ce qui est déjà connu dans l'état de la technique. Seul est considéré comme antériorisé par un document de l'état de la technique ce que la personne du métier, en faisant appel à ses connaissances générales à la date de dépôt ou de priorité pertinente, déduirait directement et sans ambiguïté de ce seul document (cf. UPC_CoA_182/2024, 25 septembre 2024, Mammut c. Ortovox ; UPC_CoA_382/2024, 14 février 2025, Abbott c. Sibio).

127. Au regard de KANAI :

Présentation du document d'art antérieur dit « KANAI »

Il s'agit d'une demande de brevet US 2005/0166044 A1 publiée le 28 juin 2005 et intitulée « Digital measurement apparatus and image measurement apparatus ». (cf pièce DMTV 4.5, D5) dont l'abstract indique: « *digital measurement apparatus measures a physical measurement object, provides a digital Signature of public-key cryptography to measured data of a thus-measured physical quantity, and manages the measured data. The apparatus generates at least a pair of a public*

key and a private key, to be used for the digital signature of the public key cryptography, through a key generating algorithm ».

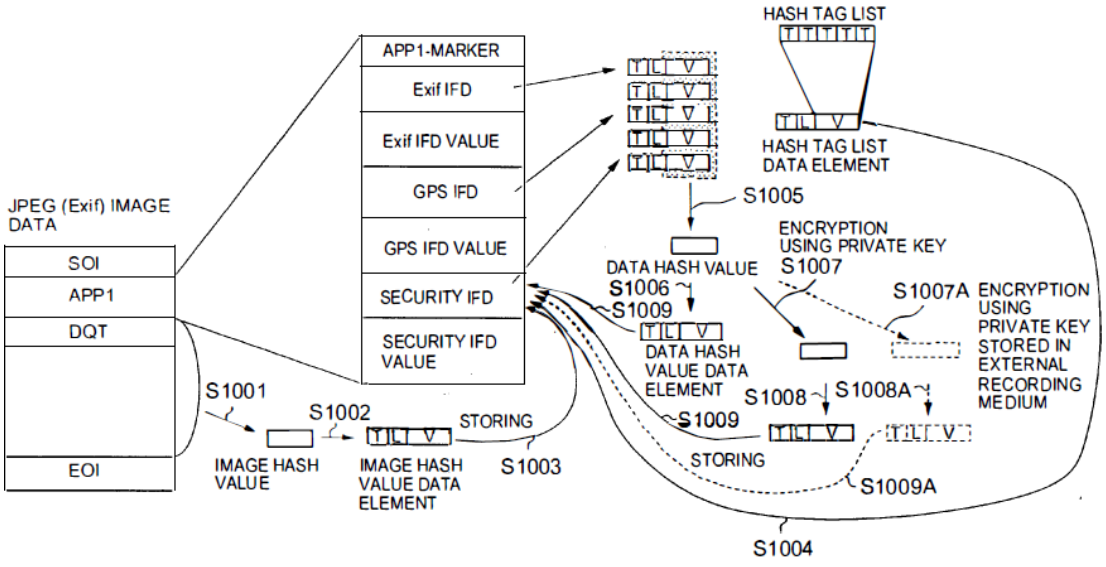
Ce document concerne un système destiné à garantir l'intégrité et l'authenticité de données de mesure numériques, notamment des images produites par des appareils tels que des appareils photo numériques, des scanners ou des équipements médicaux. L'invention vise à remédier aux inconvénients des systèmes dans lesquels la signature numérique est stockée dans un fichier séparé du fichier de données, ce qui peut conduire à une dissociation entre les deux.

128. L'idée centrale de KANAI consiste à intégrer directement dans le fichier les valeurs de hachage et les signatures numériques nécessaires à la vérification. Le système calcule tout d'abord un hachage des données à protéger, en particulier du contenu principal de l'image. Cette valeur de hachage est ensuite enregistrée dans une structure de données spécifique intégrée au fichier. Une seconde valeur de hachage peut être calculée à partir de plusieurs éléments considérés comme importants pour la crédibilité du document, tels que la date de création, l'identité de l'utilisateur, diverses métadonnées ou encore la première valeur de hachage. Cette seconde valeur est ensuite chiffrée au moyen d'une clé privée pour générer une signature numérique.

129. Dans le cas particulier du format JPEG/Exif, KANAI prévoit la création d'une zone de métadonnées de sécurité (« Security IFD ») au sein du fichier image. Cette zone contient notamment une valeur de hachage de l'image (« Image Hash Value »), une liste des éléments protégés (« Hash Tag List »), une valeur de hachage globale (« Data Hash Value ») ainsi qu'une ou plusieurs signatures numériques. L'ensemble de ces informations est enregistré directement dans le fichier image**.**

130. Dans sa Figure 10, le document KANAI illustre la manière dont les informations de sécurité sont intégrées dans un fichier image au format JPEG/Exif :

FIG.10



131. La figure 10 montre que le fichier image contient, outre les données d'image proprement dites, une structure spécifique dénommée Security IFD (Security Image File Directory), destinée à recevoir les informations utilisées pour la protection de l'intégrité du fichier. Cette structure est intégrée directement dans le fichier JPEG/Exif au sein du segment APP1.

132. Le procédé commence par le calcul d'une première valeur de hachage appelée Image Hash Value, obtenue à partir du flux de données principal de l'image. Cette valeur est enregistrée dans un élément de données spécifique dénommé Image Hash Value Data Element. La figure montre ensuite la création d'une Hash Tag List, c'est-à-dire une liste identifiant les éléments du fichier qui doivent être pris en compte pour les vérifications ultérieures.

133. À partir des éléments désignés dans cette liste, le système calcule une seconde valeur de hachage appelée Data Hash Value. Cette valeur est ensuite stockée dans un Data Hash Value Data Element. Le Data Hash Value est ensuite chiffré au moyen d'une clé privée afin de produire une Data Signature, laquelle est également enregistrée dans la structure Security IFD.

134. La figure met ainsi en évidence que le fichier contient simultanément une valeur de hachage autonome (Image Hash Value), une valeur de hachage globale (Data Hash Value) et une signature numérique (Data Signature), l'ensemble de ces informations étant regroupé dans une structure de métadonnées intégrée au fichier lui-même.

135. Cette figure revêt une importance particulière car elle montre explicitement l'insertion dans le fichier d'une valeur de hachage représentant le contenu protégé, indépendamment de la signature numérique.
Ainsi, il apparaît que KANAI divulgue déjà un mécanisme impliquant une valeur de hachage intégrée au fichier, stockée dans une zone dédiée, puis utilisée lors de la procédure de vérification de l'intégrité. Les paragraphes [0049] à [0057] décrivent la génération et le stockage de ces valeurs, tandis que les paragraphes [0062] et [0063] exposent leur lecture, leur recalcul et leur comparaison lors de la vérification.

136. Ce document attache une importance particulière à la question de l'insertion de la signature dans le fichier. Il explique que l'ajout d'une signature modifie le contenu du fichier et pourrait donc affecter le calcul de l'empreinte. Pour résoudre cette difficulté, KANAI prévoit notamment la réservation préalable d'un espace destiné à recevoir la signature ou certaines données de sécurité, espace qui est ignoré ou traité de manière spécifique lors du calcul des valeurs de hachage.

137. **Selon ADOBE :** (cf. pages 23 à 26 du récapitulatif des moyens)

ADOBE appuie sa démonstration sur certains paragraphes de la description de la demande KANAI qui sont les suivants :

- [0063] *First, the value in the value portion of the data signature data element is read from the JPEG (Exif) image data. Then, the thus-obtained data Signature is decrypted using the public key of the digital camera. Thereby, the data hash value is obtained. (…) Then, it is determined whether the thus-obtained data hash value agrees (…)*
- *The protected image data Stream is read … and is compressed through the hash algorithm (SHA-1, MD5, or the like). Thus, the hash value is calculated. (…) When they do not agree with one another, it is determined that the image data was altered in some way. (…)*

Traduction libre en français :

- [0063] Tout d'abord, la valeur contenue dans la partie valeur de l'élément de données de signature est lue à partir des données d'image JPEG (Exif). Ensuite, la signature ainsi obtenue est déchiffrée à l'aide de la clé publique de l'appareil photo numérique. On obtient ainsi la valeur de hachage des données. (…) Ensuite, il est déterminé si la valeur de hachage ainsi obtenue correspond (...)
- Le flux de données d'image protégé est lu ... et compressé à l'aide de l'algorithme de hachage (SHA-1, MD5 ou similaire). La valeur de hachage est ainsi calculée. (...) Lorsqu'elles ne correspondent pas, il est déterminé que les données d'image ont été modifiées d'une manière ou d'une autre. (…)

138. ADOBE soutient que l'emplacement basé sur un « marqueur » de l'empreinte numérique d'identification intégrée est divulgué via un indicateur d'étiquette/type :

- [0056] *A TLV data element is produced (in a step S1008) using a tag number (written in the tag portion "T") indicating that this TLV data element is of the data signature. This TLV data element includes the data signature in the value portion thereof. The thus-produced TLV data element is called a data Signature data element.*

Traduction libre en français :

- [0056] Un élément de données TLV est produit (à l'étape S1008) à l'aide d'un numéro d'étiquette (écrit dans la partie étiquette « T ») indiquant que cet élément de données TLV est de la signature de données. Cet élément de données TLV comprend la signature de données dans sa partie valeur. L'élément de données TLV ainsi produit est appelé élément de données Signature de données.

139. En conséquence, ADOBE relève que US'044 – KANAI – D5 divulgue également la génération d'un bloc de données vérifiable en réservant/identifiant d'abord un emplacement d'insertion dans le bloc de données initial, puis en intégrant la signature/empreinte calculée à cet emplacement :

- [0038] *(…) an area for embedding the digital signature is previously secured in the file of image data, this area is previously filled with predetermined values, a hash value of the entire data is calculated, the digital signature is produced, and then, the produced digital signature is embedded in the previously secured area.*

Traduction libre en français :

- [0038] (…) une zone destinée à intégrer la signature numérique est préalablement réservée dans le fichier de données d'image, cette zone est préalablement remplie avec des valeurs prédéterminées, une valeur de hachage de l'ensemble des données est calculée, la signature numérique est produite, puis la signature numérique produite est intégrée dans la zone préalablement réservée.

140. Selon ADOBE, KANAI antériorise la revendication 1, y compris selon l'interprétation indûment restrictive de la Demanderesse qui réduit l'« empreinte d'identification » à un hachage brut, non chiffré. Dans son second mode de réalisation, KANAI calcule une « valeur de hachage d'image » au moyen d'un algorithme tel que SHA-1 ou MD5, l'insère dans le fichier JPEG/Exif au sein d'un élément de données TLV spécifiquement balisé, puis la vérifie en la comparant à une valeur de hachage nouvellement calculée sur le flux de données d'image protégé. KANAI distingue cette valeur de hachage d'image de la « valeur de hachage de données » et de la « signature de données » de niveau supérieur. La présence de ces mécanismes supplémentaires ne retire donc rien à la divulgation complète du sous-processus de hachage brut. [Sources : Mémoire n° 1, § 4.2.2.1.5, pp. 77–81, par. 149–159. Mémoire n° 2, § 3.6, pp. 71–80, par. 257–306. Mémoire n° 3, § 2.4.6, pp. 50–52, par. 140–145.]

141. ADOBE relève en outre que la propre analyse de KANAI par la Demanderesse confirme l'essentiel de cette correspondance : elle reconnaît que la valeur de hachage « peut être recherchée et trouvée à l'aide d'un repère dans le bloc de données SOI-EOI » et que cette recherche sert à obtenir la valeur destinée à être comparée. Ses objections se concentrent ainsi sur l'exclusion des bits de l'empreinte trouvée (caractéristique 1.4). [Sources : Mémoire n° 2, § 3.6, pp. 71–80, par. 257–306. Mémoire n° 3, § 2.4.6, pp. 50–51, par. 140–142. Objection de la Demanderesse : Réplique du 5 juin 2026, § III.4.4.1.5.]

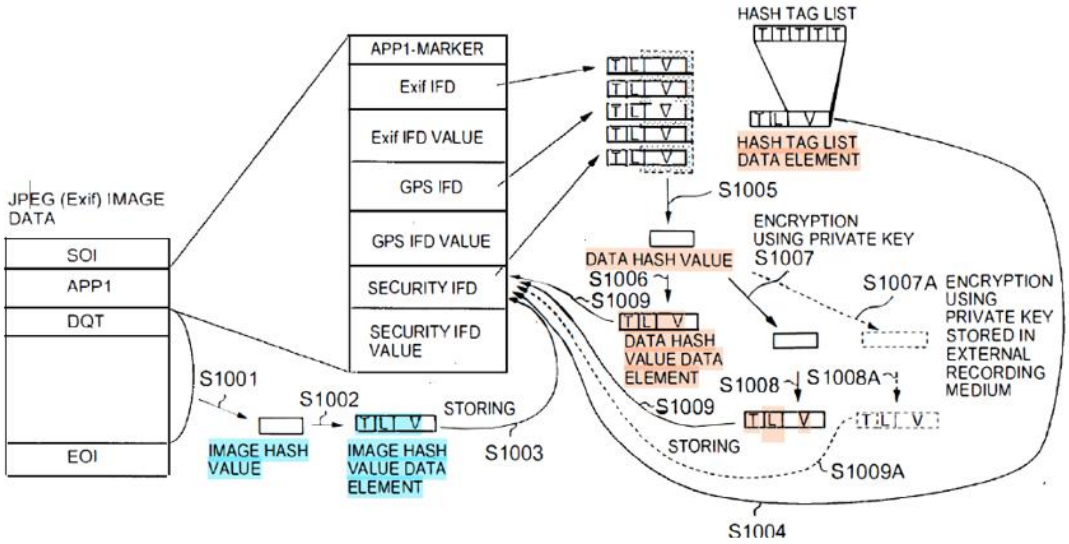
142. **<u>Selon OPENAI :</u>** (cf. § 74 à 84, pages 27 récapitulatif de ses moyens)

Le document KANAI, qui porte notamment sur des appareils photo numériques, explique qu'il était connu dans l'art antérieur d'utiliser une clé privée stockée dans l'appareil pour calculer une signature numérique de la photo, la signature étant ensuite stockée dans un support, aux côtés de la photo, et la clé publique correspondante permettant de vérifier la photo. Or, le fichier de l'image et la signature étant séparés (cf. para. [0005] et [0006]), il pouvait arriver que la relation entre ces deux éléments ne soit pas assurée, ce qui correspond là encore au même problème que celui du Brevet.

143. OpenAI fait référence au second mode de réalisation décrit au regard du format d'image Exif (voir Fig. 9) qui définit différentes zones : (i) une zone s'étendant du début de la zone nommée DQT jusqu'à la fin de la zone précédant la zone EOI ; il s'agit de la zone où sont stockées les informations utiles à protéger ; (ii) une zone APP qui comprend certaines métadonnées, dont notamment une zone « security IFD », qui consiste en une collection de tags pour décrire les informations de

sécurité, ainsi que les zones Exif IFD et GPS IFD qui comprennent des informations utilisées pour améliorer la crédibilité des données, par exemple, les conditions et le lieu de prise de la photo.(cf. US 044, para. [0047])

144. Selon les défenderesses, le procédé de génération et de signature d'une image selon le format Exif est illustré à la Fig. 10 de D5 (KANAI) qui est annotée par OPENAI comme suit :



---

145. Selon OPENAI, au vu de ce mode de réalisation illustré par la Fig. 10 de KANAI, US 044 décrit la génération d'un bloc de données d'une image (encadré en rouge) qui comporte des données à protéger (encadré en bleu), et pour lesquelles un hash (surligné en bleu) est calculé et inséré dans un élément TLV (surligné en orange) comprenant un tag « T ». Cet élément TLV est inséré dans la zone « security IFD » (encadrée en orange), elle-même comprise dans la zone APP1 (encadrée en vert), elle-même comprise dans le bloc de données (en rouge). La vérification consiste à extraire le hash de l'élément TLV, calculer un hash des données à protéger, et comparer les deux valeurs de hash. (§ 79 récapitulatif des moyens d'OPENAI)

146. **<u>Réponse de KEEEX contestant le défaut de nouveauté au regard de KANAI :</u>** (cf. pages 25 et 26 récapitulatif des moyens de KEEEX)

KEEEX présente tout d'abord une <u>réponse générale</u> aux attaques sur la validité de son Brevet. Dans son mémoire en réplique au mémoire en défense, pour chacune des antériorités qui lui est opposée, KEEEX soutient que les documents invoqués reposent tous sur des systèmes de signature numérique et non sur des empreintes d'identification au sens du brevet. Selon le demandeur, ces références utilisent des signatures destinées à authentifier un auteur ou un document, alors que son invention repose sur un mécanisme distinct permettant d'insérer dans un fichier un identifiant calculé sur son propre contenu et de vérifier ce contenu au moyen d'un simple recalcul. L'argument central de la réplique au mémoire en défense repose sur le fait que les antériorités invoquées ne divulguent ni l'utilisation d'une véritable empreinte d'identification intégrée

au document ni la comparaison directe revendiquée par le brevet, de sorte que la nouveauté et l'activité inventive demeurent préservées

147. ***Plus particulièrement, concernant la validité au regard du document KANAI,*** KEEEX réplique que KANAI est un système complexe de sécurité reposant sur une architecture spécifique au format JPEG/Exif, sur des structures de métadonnées dédiées et sur des mécanismes de signature numérique. Selon le demandeur, ce document ne divulgue pas le mécanisme générique de recherche d'une empreinte d'identification au moyen d'un repère puis de vérification par recalcul et comparaison tel qu'il serait revendiqué par le brevet EP070.

148. KEEEX expose que, dans la comparaison entre l'objet de la revendication 1 et le document D5, les Défenderesses ignorent certaines caractéristiques de la revendication 1. Si bien que la conclusion d'absence de nouveauté à laquelle elles aboutissent ne peut qu'être contestée.

149. a) Empreinte d'identification

En effet, les Défenderesses ne tiennent pas compte de la fonction d'identification de l'empreinte revendiquée, laquelle est pourtant essentielle à la résolution du problème technique soulevé dans le Brevet.

Le document D5 décrit une valeur de hachage calculée sur des données image situées entre des étiquettes DQT et EOI d'un fichier JPEG et insérée dans un bloc APP1 entre des étiquettes SOI et DQT du fichier JPEG, lequel est délimité par les étiquettes SOI et EOI.

En réalité, le document D5 ne précise nulle part qu'il faut attribuer à cette valeur de hachage la fonction d'identifiant du fichier JPEG. Plus généralement, le document D5 n'aborde pas le problème de l'identification du fichier JPEG. Il est donc implicite que le fichier JPEG généré comme indiqué dans le document D5 reçoive un identifiant classique comme un nom de fichier dans le système d'exploitation Windows ou OSX.

150. b) Recherche d'une empreinte d'identification à l'aide d'un repère

Les Défenderesses relèvent que la valeur de hachage est insérée dans un champ TLV formé d'une étiquette, d'une longueur et d'une valeur correspondant à la valeur de hachage.

Même si une étiquette est associée à la valeur de hachage, le document D5 n'indique nulle part comment la valeur de hachage est trouvée dans le fichier, et encore moins que l'étiquette associée à la valeur de hachage est utilisée pour retrouver celle-ci dans le fichier JPEG, ni même que cette étiquette peut être utilisée à cet effet.

151. c) Calcul d'empreinte avec exclusion de l'empreinte d'identification trouvée

Cette caractéristique est importante car elle contribue avec l'étape de recherche au moyen d'un repère, à rendre le procédé de vérification revendiqué universel, ou plus précisément, indépendant d'un éventuel format ou structure prédéfinis du bloc de données.

Cette caractéristique de la revendication n'a pas non plus été prise en compte par les Défenderesses dans leur appréciation de la pertinence du document D5. En effet, elles ont fait valoir que cette caractéristique de la revendication 1 était divulguée par le document D5 du simple fait que la zone de données d'image DQT-EOI sur laquelle porte le calcul de la valeur de hachage ne comporte pas la valeur de hachage.

Or, le document D5 ne prévoit pas de déterminer la zone de calcul d'empreinte à partir du résultat de la recherche d'empreinte dans le bloc de données. En réalité, cette zone de calcul est prédéfinie avant toute insertion d'empreinte ou de signature dans le bloc de données :

- « *Specifically, the information starting from the DQT marker and ending before the EOI marker is required to be protected.* » (Paragraphe 0047)

152. Ainsi, les étiquettes DQT et EOI qui délimitent l'étendue de la zone d'image à protéger par une empreinte et une signature préexistent à une éventuelle recherche d'empreinte. La détermination de cette zone d'image ne requiert donc nullement de connaître la position de l'empreinte dans le bloc de données, ou de procéder à une recherche préalable de l'empreinte dans le bloc de données.

153. Au contraire, le procédé de vérification tel que formulé par la revendication 1 impose de procéder à la recherche de l'empreinte d'identification avant de pouvoir calculer l'empreinte, du fait que le calcul d'empreinte est effectué en excluant les bits de l'empreinte d'identification trouvée.

154. En outre, contrairement à l'objet de la revendication 1, le calcul de la valeur de hachage des données d'image ne peut pas procéder par exclusion de la valeur de hachage, puisque la zone du calcul de cette valeur de hachage est spécifiée positivement entre deux étiquettes prédéfinies DQT, EOI. Il ne s'agirait donc pas d'un mécanisme fondé sur l'exclusion de l'empreinte localisée, ni plus généralement sur l'exclusion de certaines données, mais d'un mécanisme fondé sur la sélection préalable d'une portion déterminée du fichier devant être prise en compte pour le calcul.

155. **Réponses aux critiques de KEEEX :** (cf. en particulier, les arguments en réponse de OPENAI aux § 85 à 89 récapitulatif de ses moyens)

OpenAI répond que KEEEX procède à une lecture excessivement complexe du document KANAI en s'appuyant sur l'ensemble de ses modes de réalisation et sur tous les mécanismes de sécurité qu'il décrit, alors que l'analyse de nouveauté des défenderesses se concentre uniquement sur le second mode de réalisation et, plus précisément, sur la seule « valeur de hachage de l'image » (*Image Hash Value*). Selon OpenAI, cet élément constitue à lui seul une empreinte intégrée dans le fichier, localisable au moyen d'un repère, recalculée sur les données protégées puis comparée à la valeur stockée lors de la vérification. OpenAI soutient également que l'exclusion, lors du calcul, d'éléments supplémentaires autres que l'empreinte elle-même ne permet pas de distinguer la revendication 1, dès lors que les revendications 10 et 11 du brevet envisagent elles-mêmes

l'exclusion de portions plus larges du fichier. Enfin, OpenAI considère que le repère revendiqué est divulgué par les étiquettes (*tags*) et structures utilisées dans KANAI, lesquelles permettent de localiser l'empreinte dans le fichier. Les autres mécanismes décrits dans KANAI, notamment les signatures numériques ou les structures destinées à protéger d'autres données, sont présentés comme indépendants du sous-processus de vérification reposant sur la seule « Image Hash Value », lequel reproduirait déjà les caractéristiques essentielles de la revendication 1

156. Position du Tribunal :

Le Tribunal n'est pas convaincu par les arguments de KEEEX et considère que la Revendication 1 est divulguée en ce que la personne du métier, en faisant appel à ses connaissances générales à la date de dépôt du Brevet, aurait déduit directement et sans ambiguïté du seul document KANAI l'enseignement de chacune des caractéristiques, comme suit :

157. **Caractéristique 1.1** : Le document KANAI divulgue un procédé destiné à vérifier l'intégrité de données numériques, en particulier d'images enregistrées au format JPEG/Exif. Lors de la vérification, une valeur de hachage précédemment enregistrée dans le fichier est comparée à une nouvelle valeur calculée à partir des données d'image. Une discordance entre ces valeurs révèle une altération des données protégées. La photographie numérique constitue ainsi un « bloc de données numériques » au sens de la revendication 1.

158. Le Tribunal n'est pas convaincu par l'argument de la Demanderesse selon lequel le document ne relèverait pas du champ de la revendication au motif qu'il serait limité à un format particulier. Comme indiqué précédemment dans l'analyse de la construction des revendications, la revendication 1 n'exige ni universalité particulière ni indépendance à l'égard du format du fichier traité. Il suffit que le document divulgue, pour le fichier considéré, le procédé de vérification revendiqué.

159. **Caractéristique 1.2** : KANAI divulgue une « valeur de hachage de l'image » (*Image Hash Value*) stockée dans le fichier Exif au sein de la structure de sécurité (*Security IFD*). Cette valeur constitue une empreinte numérique au sens de la revendication.

160. Le Tribunal relève également que la structure TLV utilisée dans KANAI comporte une partie « T » (*Tag*), une partie « L » (*Length*) et une partie « V » (*Value*). La partie « T » permet d'identifier l'élément de données contenant la valeur de hachage de l'image et donc de localiser cette valeur dans le fichier. Elle remplit ainsi la fonction du « premier repère » au sens de la revendication 1.2.

161. Le Tribunal ne partage pas l'analyse de la Demanderesse selon laquelle le repère revendiqué exigerait nécessairement une recherche textuelle ou un marqueur indépendant de la structure logique du fichier. Le brevet définit le repère de

manière fonctionnelle, comme un moyen permettant de localiser l'empreinte. Une localisation fondée sur une balise de données répond à cette exigence.

162. **Caractéristique 1.3** : Une fois la valeur de hachage localisée, KANAI enseigne le recalcul d'une nouvelle valeur de hachage à partir des données d'image protégées. Le document prévoit explicitement l'application d'un algorithme de hachage tel que SHA-1 ou MD5 au flux de données d'image afin d'obtenir une valeur destinée à la vérification.

163. Le Tribunal considère que cette opération correspond au calcul d'une empreinte numérique du bloc de données au moyen d'une fonction de calcul d'empreinte, tel que requis par la caractéristique 1.3.

164. Le Tribunal n'est pas convaincu par l'argument selon lequel KANAI ne concernerait que des signatures numériques. Le document distingue clairement la « valeur de hachage de l'image », la « valeur de hachage des données » et la « signature des données ». L'existence d'une couche supplémentaire de signature ne fait pas disparaître la divulgation autonome de la valeur de hachage de l'image.

165. **Caractéristique 1.4** : La valeur de hachage de l'image est stockée dans l'IFD de sécurité intégré au fichier JPEG/Exif. En revanche, lors du recalcul de la valeur de hachage, seules les données d'image comprises entre les marqueurs DQT et EOI sont soumises à l'algorithme de hachage.

166. Il en résulte que la zone contenant la valeur de hachage enregistrée n'est pas prise en compte lors du calcul de l'empreinte recalculée. Les bits correspondant à l'empreinte enregistrée ne contribuent donc pas au résultat obtenu. Le fait que les données du champ DQT soient prises en compte à l'étape 1001, comme le montre la figure 10 de KANAI, est sans conséquence, car ce champ ne contient que des données invariables qui déterminent en partie la structure de l'image JPEG, comme l'ont fait valoir les défendeurs lors de l'audience sans être contredits.

167. Le Tribunal n'est pas convaincu par l'argument de la Demanderesse selon lequel KANAI définirait ce qui doit être inclus dans le calcul alors que la revendication définirait ce qui doit en être exclu. La caractéristique 1.4 n'impose pas une méthode particulière permettant d'exclure l'empreinte d'identification du calcul. Elle exige seulement que la valeur de l'empreinte recalculée soit obtenue sans tenir compte des bits correspondant à l'empreinte stockée. D'un point de vue fonctionnel, une donnée située en dehors de la portion de données soumise à la fonction de hachage est effectivement exclue du calcul, peu importe que cette exclusion résulte d'une suppression active ou de la définition préalable de la région à traiter.

168. Le Tribunal n'est pas davantage convaincu par l'argument selon lequel la revendication exigerait nécessairement la prise en compte de tous les bits du bloc de données autres que ceux de l'empreinte. Comme indiqué lors de l'interprétation de la revendication, l'expression « dépendant de chacun des bits»

signifie que l'empreinte dépend de l'ensemble des données retenues pour le calcul et non qu'aucune autre donnée ne puisse être exclue. Une telle interprétation serait d'ailleurs difficilement conciliable avec les revendications dépendantes 10 et 11, lesquelles prévoient explicitement qu'une métadonnée peut comprendre une partie variable exclue du calcul de l'empreinte et que l'empreinte elle-même peut être située dans cette partie variable.

169. Dès lors, même si KANAI détermine positivement la zone du fichier soumise au calcul de hachage, tandis que la revendication 1 décrit l'opération en termes d'exclusion de l'empreinte localisée, les deux approches répondent au même objectif technique, à savoir éviter que les données de vérification stockées dans le fichier n'affectent le résultat du calcul utilisé pour la vérification. Le Tribunal considère ainsi que l'homme du métier lirait au minimum dans KANAI l'enseignement, sinon littéral, du moins directement et sans ambiguïté, d'un calcul d'empreinte effectué à l'exclusion de la zone contenant l'empreinte d'identification.

170. Dans les deux cas, l'objectif est de calculer une empreinte représentative de la charge utile protégée (payload) du fichier, en excluant les données de vérification et, le cas échéant, d'autres données prédéfinies qui ne doivent pas influer sur le résultat du calcul, afin de permettre la détection d'une modification du contenu effectivement protégé.

171. En conséquence, la caractéristique 1.4 est divulguée par KANAI.

172. **Caractéristique 1.5** : KANAI enseigne ensuite la comparaison entre la valeur de hachage précédemment lue dans le fichier et la valeur de hachage nouvellement calculée. Le document indique expressément qu'une différence entre ces deux valeurs révèle une altération des données d'image.

173. Le Tribunal considère que cette séquence de lecture, de recalcul et de comparaison correspond à la vérification revendiquée par la caractéristique 1.5.

174. La circonstance que KANAI prévoie également d'autres mécanismes de vérification n'est pas pertinente. La revendication 1 est rédigée de manière ouverte et n'exclut pas l'existence d'étapes supplémentaires. Il suffit que le document divulgue le mécanisme de comparaison revendiqué, ce qui est le cas.

175. **Conclusion :**

Le Tribunal considère qu'aucune des objections soulevées par la Demanderesse ne permet de distinguer l'objet revendiqué du document KANAI. Ce document divulgue directement et sans ambiguïté chacune des caractéristiques 1.1 à 1.5 de la revendication 1.

La revendication 1 du brevet tel que délivré est dès lors dépourvue de nouveauté au regard du document KANAI.

2) <u>Validité des revendications dépendantes de Revendication 1 opposées par KEEEX (2, 4, 7, 8, 10, 11 et 14)</u>

176. <u>Cadre juridique :</u>

La Cour d'appel a jugé (UPC_CoA_473/2025, UPC_CoA_474/2025, UPC_CoA_873/2025 et UPC_CoA_881/2026, 13 juillet 2026, Fujifilm c. Kodak) que le titulaire du brevet n'est pas tenu de présenter une demande de modification au titre de la règle 30 du règlement de procédure aux seules fins de défendre des revendications dépendantes telles que délivrées ou des combinaisons de revendications déjà couvertes par le brevet tel que délivré. Toutefois, lorsque la nullité de plusieurs revendications ou de l'ensemble des revendications est demandée, le titulaire du brevet doit préciser, de manière suffisamment motivée, quelles revendications dépendantes il estime valables dans l'hypothèse où la revendication indépendante serait déclarée nulle. S'il se prévaut d'une combinaison particulière de revendications dépendantes, cette combinaison doit également être identifiée avec suffisamment de précision (points 2, 3 et 5 du sommaire).

177. <u>Dans le cas présent :</u>

KEEEX n'a pas précisé dans ses mémoires quelles sont les revendications dépendantes qu'il considère comme valides au cas où la revendication 1 serait déclarée nulle, et a encore moins motivé cette affirmation. Ce n'est que lors de l'audience orale que le représentant du demandeur a déclaré que la revendication 2 pourrait être valable même dans le cas où la revendication 1 serait invalidée, mais le représentant d'ADOBE a, à bon droit, fait remarquer que cette argumentation ne figurait pas dans les écritures et devait donc être écartée des débats comme tardive.

178. C'est au titulaire du titre qu'il incombe de démontrer que les revendications dépendantes pourraient être valides alors même que la revendication principale est déclarée nulle. En l'espèce, le Tribunal constate que KEEEX n'a pas précisé dans ses écritures, de manière suffisamment motivée, quelles revendications dépendantes il estime valables dans l'hypothèse où la revendication indépendante serait déclarée nulle.

179. Il s'ensuit que du fait de l'invalidation de la revendication 1 (pour les motifs de l'extension de l'objet illicite et du défaut de nouveauté), les revendications dépendantes critiquées n° 2, 4, 7, 8, 10, 11 et 14 seront déclarées également invalides.

3) <u>Autres revendications indépendantes (16 et 18)</u>

Les revendications indépendantes 16 et 18 sont construites en miroir avec le procédé de la revendication 1 et souffrent donc des mêmes motifs d'invalidité, d'extension de l'objet et surabondamment de défaut de nouveauté au vu de KANAI pour les mêmes motifs.

4) Les requêtes subsidiaires en modification conditionnelle du Brevet

180. KEEEX propose en réponse à la demande reconventionnelle en révocation de son brevet, 11 requêtes subsidiaires en modification sur le fondement de R. 30.1 RdP, telles que présentées dans ses pièces KEEEX 29.1 à 29.11. Le demandeur a établi un tableau dans son mémoire du 5 mars 2026 résumant les requêtes subsidiaires présentées comme suit :

2.11. Tableau récapitulatif des requêtes

Requête	Descriptif résumé[1]
Principale	Suppression de la revendication 15 incompatible avec la revendication 1
Première requête subsidiaire	Requête principale + La fonction de calcul d'empreinte est une fonction de hachage
Deuxième requête subsidiaire	Première requête subsidiaire + information = fonction de hachage
Troisième requête subsidiaire	Première requête subsidiaire + signature
Quatrième requête subsidiaire	Requête principale + navigateur
Cinquième-neuvième requêtes subsidiaires	Requête principale, première-quatrième requêtes subsidiaires, respectivement + retrait de l'alternative dans la revendication 1
Dixième requête subsidiaire	Brevet tel que délivré
Onzième requête subsidiaire	Brevet tel que délivré + retrait de l'alternative dans la revendication 1

[1] Ce tableau a pour simple objectif de donner une vue synthétique de l'organisation des requêtes, mais ne peut se substituer à la présentation individuelle détaillée de chaque requête.

181. Au cours de l'audience orale, le panel a demandé des précisions afin de vérifier si les requêtes subsidiaires devaient être considérées comme un ensemble complet et fermé ou si KEEEX souhaitait laisser ouverte la possibilité que l'une quelconque des revendications principales et dépendantes figurant dans les ensembles de revendications présentés dans les requêtes subsidiaires respectives puisse être recombinées et doivent – en tant que requête subsidiaire supplémentaire – être recombinées selon n'importe laquelle de ces recombinaisons théoriquement possibles (cf. question du juge Tochtermann à 2 :28 du procès-verbal audio de l'audience). Les défendeurs ont répondu, que tout au long de la procédure, les requêtes subsidiaires ont été présentées par KEEEX comme un ensemble complet et fermé de revendications, sans suggérer ni justifier des combinaisons possibles. (cf. réponse de Me Por à 3 :33 du procès-verbal audio de l'audience). Dans sa réplique orale, KEEEX n'a pas contredit les défendeurs dans cette interprétation de leurs demandes en modification. (cf. réponse de M. Bourgeois à 3:45 du procès-verbal audio de l'audience).

182. Concernant RS 1 à RS 9 : Les requêtes en modification du Brevet n° 1 à 9 proposées par KEEEX, sur le fondement de R. 30.1 RoP, comportent la suppression de la revendication 15, laquelle n'est pas comprise dans les attaques en nullité formées par les défendeurs.

183. Tout d'abord, sur le plan procédural, le Tribunal rappelle que le périmètre du litige est défini par les parties ; or, la validité de la revendication 15 n'était pas critiquée par les défendeurs. Par conséquent, comme cela est soutenu à bon droit par les défendeurs, il n'est pas permis au titulaire du Brevet de modifier ou de supprimer cette revendication non opposée.

184. En outre, sur le plan substantiel, le titulaire du brevet a la possibilité de modifier la description pour qu'elle soit en conformité avec la revendication modifiée (cf. R. 30.1 (a) RdP). En revanche, il n'est pas possible de modifier la description de telle sorte qu'elle change la signification du Brevet et de sa Revendication 1. Il est possible de limiter le périmètre du Brevet, mais pas de donner une nouvelle signification au Brevet en modifiant aussi complètement la description. Ce serait d'ailleurs incompatible avec le principe de sécurité juridique pour les tiers. En l'espèce, l'argument de KEEEX pour justifier la suppression de la revendication 15 et des parties de la description au support est que celles-ci seraient incompatibles avec la revendication 1. Or, il a été démontré dans la partie de la présente décision consacrée à l'interprétation et à la construction des revendications que tout le Brevet enseigne au contraire que la revendication 1 couvre également les signatures numériques, comme le confirme la revendication 15, qui n'apparaît donc pas incompatible, mais ne fait qu'en préciser la portée. Par la suppression de la revendication 15 et de toutes les parties de la description qui viennent en support, le titulaire du Brevet tente donc de modifier la portée et la signification de son brevet, de manière a posteriori pour échapper à l'antériorisation par D5, ce qui n'est pas admissible.

185. Le panel en conclut que les requêtes RS 1 à RS 9 en modification du brevet ne sont pas admissibles, tant sur le plan procédural que sur le plan substantiel.

186. Il est rappelé que KEEEX a abandonné la requête 10 (SR 10), qui n'avait d'ailleurs aucune utilité puisqu'elle reprenait à l'identique le brevet tel que délivré dont la validité a déjà été examinée plus haut (cf. l'ordonnance après conférence de la mise en état du 22 septembre 2026) et que la modification ultérieure sur R. 30.2 RdP n'a pas été autorisée par le panel (cf. ordonnance du 25 juin 2026 et sa confirmation par le panel le 29 juillet 2026).

187. Concernant SR 11, cette dernière ne propose ni la modification de la description ni la suppression de la revendication 15 du brevet. SR 11 ne souffre donc pas des critiques opposées par les défendeurs concernant l'inadmissibilité de RS1 à RS9. Elle consiste, comme cela a déjà été présenté, en la suppression de la dernière partie de la caractéristique 1.5.

188. Les défendeurs reprochent à RS 11 son inadmissibilité au motif de l'extension de la portée de la protection sur le fondement de l'Art. 123(3) CBE.

189. Position du Tribunal sur l'inadmissibilité de RS 11 au vu de l'Art. 123(3) CBE :

190. La requête subsidiaire 11 (RS11) correspond, pour l'essentiel, au brevet tel que délivré, à ceci près que la revendication 1 a été modifiée par la suppression de la seconde branche de l'alternative figurant à la fin de la caractéristique 1.5, à savoir les termes « ou que l'empreinte d'identification a été calculée en appliquant une

autre fonction de calcul d'empreinte ». Cette modification vise à répondre à l'objection d'extension de l'objet soulevée à l'encontre du brevet tel que délivré, au motif que cette alternative ne trouverait pas de fondement direct et non ambigu dans la demande telle que déposée. La requête subsidiaire 11 conserve en revanche l'ensemble des autres caractéristiques de la revendication 1 ainsi que l'économie générale du brevet tel que délivré, y compris les modes de réalisation mettant en œuvre des signatures numériques.

191. Le Tribunal doit toutefois encore examiner si la suppression de cette caractéristique est conforme aux exigences de l'article 123(3) CBE. En effet, même lorsqu'une modification vise à remédier à une éventuelle extension de l'objet au sens de l'article 123(2) CBE, elle ne peut être admise si elle a pour effet d'étendre la protection conférée par le brevet après sa délivrance. Il convient dès lors de déterminer si la suppression de l'alternative relative à l'utilisation d'une autre fonction de calcul d'empreinte modifie la portée de la revendication 1 telle que délivrée et conduit à accorder au titulaire une protection plus étendue que celle résultant du texte du brevet délivré.

192. Selon ADOBE, l'élément que le requérant cherche à supprimer a été introduit dans le jeu de revendications du 13 mars 2020, ce qui a convaincu la division d'examen d'accorder un brevet. Le demandeur a fait valoir que, puisque les deux variantes étaient revendiquées conjointement dans le cadre de la fausse comparaison, une comparaison correcte impliquerait que le bloc de données n'ait pas été modifié et que les fonctions de hachage utilisées soient identiques. Par conséquent, en supprimant l'une des variantes, cette dernière n'est plus requise par la revendication. Par conséquent, la cinquième requête subsidiaire viole l'article 123(3) de la CBE en cherchant à étendre l'étendue de la protection.

193. ADOBE soutient que la suppression de la seconde branche de l'alternative figurant à la caractéristique 1.5 n'est pas admissible au regard de l'article 123(3) CBE. Selon ADOBE, cette alternative a été introduite au cours de la procédure d'examen et a contribué à la délivrance du brevet. ADOBE fait valoir que, dans la revendication telle que délivrée, une comparaison correcte entre l'empreinte trouvée et l'empreinte calculée implique non seulement que le bloc de données n'a pas été modifié, mais également que la même fonction de calcul d'empreinte a été utilisée. La suppression de l'alternative relative à l'utilisation d'une autre fonction de calcul d'empreinte aurait pour conséquence de supprimer cette condition de la revendication et conduirait ainsi, selon ADOBE, à une extension de la protection conférée par le brevet délivré en violation de l'article 123(3) CBE.

194. Le Tribunal n'est pas convaincu que la suppression de la seconde branche de l'alternative figurant à la caractéristique 1.5 conduise nécessairement à une extension de la protection au sens de l'article 123(3) CBE. En effet, la modification concerne les conséquences attribuées à une comparaison négative et n'affecte pas, à première vue, les étapes techniques du procédé revendiqué. Il n'apparaît donc pas immédiatement que des actes qui ne relevaient pas du champ de la revendication telle que délivrée tomberaient désormais dans son champ.

195. Il n'est toutefois pas nécessaire pour le Tribunal de trancher définitivement cette question parce que, quoi qu'il en soit, RS 11 ne résout pas le problème du défaut de nouveauté du Brevet.

196. Position du Tribunal sur la validité de RS 11 :

197. Le document de l'art antérieur KANAI opposé par les défendeurs antériorise le Brevet modifié dans RS 11, pour les mêmes motifs que ceux exposés à propos de la version du brevet telle que délivrée. RS 11 n'est donc en outre pas valide pour défaut de nouveauté au vu du document de l'art antérieur KANAI.

198. Conclusion sur la validité du Brevet :

Les modifications proposées par le titulaire du brevet ne sont pas admissibles ; elles ne peuvent donc pas remédier aux défauts de brevetabilité des revendications du brevet EP 070 qui sont opposées, lesquelles sont invalides soit par extension de l'objet, soit par défaut de nouveauté au vu du document KANAI.

LA CONTREFAÇON :

199. Dépourvues de fondement, toutes les demandes de KEEEX au titre de l'action en contrefaçon doivent être rejetées, ainsi que toutes ses demandes subséquentes.

200. Il n'est donc pas nécessaire de statuer sur la matérialité et la responsabilité concernant la contrefaçon invoquée par KEEEX.

LES FRAIS DE JUSTICE (article 69 AJUB) :

201. Concernant la répartition des frais de justice entre les parties, KEEEX, partie qui succombe, doit être condamnée à payer tous les frais de la présente affaire (action en contrefaçon et demande reconventionnelle en révocation).

202. Concernant l'octroi d'une provision, chacun des 4 groupes de défendeurs demande le paiement d'une provision sur les frais à hauteur de 1,25 million d'euros au titre des frais liés à la demande en contrefaçon et la même somme pour les frais de la demande reconventionnelle en nullité.

203. Position du Tribunal :

Il convient de considérer les éléments suivants :

-le plafond pour le montant global des frais recouvrables est en l'espèce de 2 millions d'euros,

- la provision recommandée par la Cour d'Appel est de 50 % du total des frais recouvrables estimés.

En outre, pour fixer des frais raisonnables et proportionnés, il doit être pris en compte deux critères spécifiques de ce litige (reconnus par la Cour d'Appel dans l'ordonnance rendue dans cette affaire en date du 30 avril 2026) qui sont : la synergie des défenses et le statut de petite entreprise de KEEEX. Ces deux

caractéristiques particulières du présent litige justifient une pondération par rapport au plafond recommandé par la Décision du Comité administratif (Décision relative aux Lignes directrices relatives aux frais de procédure et au plafond des frais recouvrables du 24 avril 2023, modifiée le 4 novembre 2025).

204. Au vu de ces éléments, il convient d'allouer une somme totale à titre de provision de 300 000 euros, somme déjà produite comme garantie par KEEEX, c'est-à-dire 75 000 euros à chacun des groupes de défendeurs.

PAR CES MOTIFS,

Le Tribunal de première instance de la JUB :

1. Ordonne que soient déclarées invalides toutes les revendications opposées du brevet EP2949070 (le « Brevet » ou « EP 070 »), dans sa forme délivrée, et déclare toutes les requêtes en modification non admissibles,

2. Par conséquent, annule dans leur intégralité les revendications 1, 2, 4, 7, 8, 10, 11, 14, 16 et 18 du Brevet tel qu'il a été délivré sur le territoire des États membres contractants de la JUB suivants : la France, l'Italie, l'Allemagne, l'Autriche, la Belgique, le Danemark, les Pays-Bas et la Suède,

3. Ordonne que le greffe envoie une copie de cette décision à l'Office européen des brevets et à l'office national des brevets de tout État membre contractant concerné, conformément à l'article 65, paragraphe 5, de l'AJUB, et ce après l'expiration du délai de recours devant la Cour d'appel,

4. Rejette toutes les demandes de KEEEX en matière de contrefaçon fondées sur le brevet EP 070,

5. Ordonne que la totalité des frais de justice de la présente affaire (pour l'action en contrefaçon et la demande reconventionnelle en nullité) soit à la charge de KEEEX, partie qui succombe,

6. Condamne KEEEX à payer une provision au titre des frais de justice d'une somme totale de 300 000 euros à tous les défendeurs comme suit : 75 000 euros à chacun des quatre groupes de défendeurs ADOBE, OPENAI, TRUEPIC et JOINT DVT/C2PA, et ce, dans le délai de 30 jours à compter de la notification de la présente décision.

7. Fixe la valeur du présent litige à plus de 50 000 000 d'euros pour chacune des actions (la contrefaçon et la demande reconventionnelle en nullité).

Rendue à Paris, le 17 novembre 2026.

Camille Lignières, juge président et juge-rapporteur

Camille Lignières
Date : 2026.11.17 11:25:49 +01'00'

Carine Gillet, juge qualifié sur le plan juridique

Carine Gillet 2026.11.17 10:54:06 +01'00'

Peter Tochtermann, juge qualifié sur le plan juridique

Peter Michael Dr. Tochtermann Digital unterschrieben von Peter Michael Dr. Tochtermann Datum: 2026.11.17 09:56:51 +01'00'

Alessandro Sanchini, juge qualifié sur le plan technique

ALESSANDRO SANCHINI Firmato digitalmente da ALESSANDRO SANCHINI Data: 2026.11.16 17:26:16 +01'00'

Marielle Brasseur, greffier de la Division Locale de Paris

Digitally signed Marielle BRASSEUR 2026-11-17 11:41:42 +0100

Unified Patent Court Einheitliches Patentgericht Juridiction unifiée du brevet

Informations relatives au recours

Toute partie dont les conclusions ont été rejetées, en tout ou en partie, peut former un recours contre la présente décision devant la Cour d'appel, dans un délai de deux mois à compter de la date de sa notification (art. 73, paragraphe 1, de l'AJUB, Règles 220.1(a) et 224.1(a) du Règlement de procédure de la JUB.

Informations relatives à l'exécution (art. 82 de l'AJUB, art. 37, paragraphe 2, de l'AJUB, règles 118.8, 158.2, 354 et 355.4 du RdP)

Une copie certifiée conforme de la décision exécutoire sera délivrée par le greffier adjoint à la demande de la partie chargée de l'exécution, règle 69 du Règlement de procédure

DETAILS DE LA DECISION

UPC nº : UPC_CFI_530/2025

et UPC-CFI-0002281/2025 - UPC-CFI-0002285/2025 - UPC-CFI-0000003/2026

UPC-CFI-0002274/2025

Type d'action : Action en contrefaçon et demandes reconventionnelles en nullité

Date de la décision : 17 novembre 2026