ROYAUME DU MAROC
---
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

# (12) BREVET D'INVENTION

(11) N° de publication :
**MA 38282 B1**

(51) Cl. internationale :
**H04L 9/00; G09C 5/00**

(43) Date de publication :
**30.12.2016**

(21) N° Dépôt :
**38282**

(22) Date de Dépôt :
**16.12.2013**

(86) Données relatives à la demande internationale selon le PCT:
N° Dépôt international Date D'entrée en phase nationale
**PCT/EP2013/076725 16.07.2015**

(71) Demandeur(s) :
**PHILIP MORRIS PRODUCTS S.A, Quai Jeanrenaud 3 CH-2000- Neuchâtel (SE)**

(72) Inventeur(s) :
**CHANEZ PATRICK ; FRADET ERWAN**

(74) Mandataire :
**SABA & CO**

(54) Titre : **PROCEDE ET APPAREIL PERMETTANT DE MARQUER DES ARTICLES MANUFACTURES AU MOYEN D'UNE CARACTERISTIQUE PHYSIQUE**

(57) Abrégé : L'invention concerne un procédé permettant de marquer un article manufacturé, ledit procédé consistant à : créer un identifiant de produit unique pour un article manufacturé ; créer une ou plusieurs clés de chiffrement ; générer une clé secrète au moyen de l'identifiant de produit unique et de la ou des clés de chiffrement ; générer une valeur de bruit de système en exécutant une fonction de hachage sur la clé secrète et l'identifiant de produit unique ; générer une clé physique à partir d'une propriété physique mesurée de l'article manufacturé ; générer une valeur de bruit physique en exécutant une fonction de hachage sur la clé physique et l'identifiant de produit unique ; générer un identifiant sécurisé dérivé de la valeur de bruit de système et de la valeur de bruit physique ou intégrant celles-ci ; et placer une marque sur l'article manufacturé, la marque comprenant l'identifiant sécurisé ou un identifiant dérivé de l'identifiant sécurisé. L'invention concerne également des procédés permettant d'authentifier des articles marqués conformément au procédé décrit.

## الملخص

يتم وصف طريقة تعليم عنصر مصنع، حيث تشتمل على: إنشاء معرف منتج فريد لعنصر مصنع؛ وإنشاء واحد أو أكثر من مفاتيح التشفير؛ وإنشاء مفتاح سرى باستخدام معرف المنتج الفريد والواحد أو أكثر من مفاتيح التشفير؛ وتوليد قيمة تشفير نظام بإجراء دالة تجزئة على المفتاح السري ومعرف المنتج الفريد؛ وتوليد مفتاح فيزيائي من خاصية فيزيائية مقاسة للعنصر المصنع؛ وتوليد قيمة تشويش فيزيائية بإجراء دالةتجزئة على المفتاح الفيزيائي ومعرف المنتج الفريد؛ وتوليد معرف آمن مشتق من أو يضم قيمة تشويش النظام وقيمة التشويش الفيزيائية؛ ووضع علامة على العنصر المصنع، تشتمل العلامة على المعرف الآمن أو معرف مشتق من المعرف الآمن. يتم أيضًا وصف طرق للمصادقة على عناصر معلمة وفقًا للطريقة الموصوفة.

الشكل3

(TRENTE DEUX PAGES)

PHILIP MORRIS PRODUCTS S.A.
P. P. SABA & CO., Casablanca

## الوصف التفصيلي

**المجال التقني:-**

يتعلق ذلك الاختراع بطرق تعليم العناصر المصنعة والجهاز المخصص لذلك. تحديدًا، يتعلق ذلك الاختراع بتعليم بضائع معلبة.

**الخلفية التقنية:-**

تشكل السلع المزيفة والمهربة مشكلة عامة بالنسبة للعملاء، والمصنعين، والسلطات الحكومية. يتم بشكل غير قانوني بيع السلع المزيفة، وهى سلع غير مصرح بإنتاجها وعادة ما تكون ذات جودة رديئة، في جميع أنحاء العالم. تعد هذه السلع ضارة بالنسبة للعميل حيث أنها قد تكون ذات جودة رديئة وهو ما قد يمثل خطورة (يمثل ذلك أهمية بالتحديد لمنتجات مثل الأدوية أو السلع الاستهلاكية الأخرى). تعد السلع المزيفة ضارة بالنسبة للمصنعين حيث أنهم قد يعانون من فقدان السمعة، وزيادة المنافسة من مصنعين غير شرعيين يقومون بإنتاج منتجاتهم، وانتهاك الحقوق الشرعية الأخرى. تعتبر السلع المهربة، التي تمثل بضائع مصنعة بغرض التهرب من الضرائب أو اللوائح الحكومية، مشكلة كبيرة للمصنعين والسلطات الحكومية. يتم تحويل هذه السلع واستيرادها والمتاجرة فيها بشكل غير شرعي، حيث تتسبب في خسائر جسيمة لعائدات السلطات الحكومية بسبب التحصيل غير المناسب للرسوم الجمركية والضرائب.

من المفيد التمتع بالقدرة على المصادقة على العناصر المصنعة باستخدام علامات فريدة على العناصر بدون الحاجة إلى تخزين كل علامة فريدة في المكان الذي يُراد فيه المصادقة على العناصر. من المفضل أيضًا التمتع بالقدرة على اكتشاف العناصر المزيفة، أو العناصر التي تم لها نسخ علامة فريدة لمنتج مصدق عليه، بدون الحاجة إلى تخزين سجل تصديق لكل علامة فريدة.

**الكشف عن الإختراع:-**

في أحد جوانب الكشف، يتم توفير طريقة تعليم العنصر المصنع، حيث تشتمل على:

إنشاء معرف منتج فريد للعنصر المصنع؛

إنشاء واحد أو أكثر من مفاتيح التشفير؛

توليد مفتاح سرى باستخدام معرف المنتج الفريد وواحد أو أكثر من مفاتيح التشفير؛

توليد مفتاح فيزيائي من خاصية فيزيائية مقاسة للعنصر المصنع؛

توليد معرف آمن مشتق من، أو يضم، المفتاح السري والمفتاح الفيزيائي؛ و

وضع علامة على العنصر المصنع، وتشتمل العلامة على المعرف الآمن أو معرف مشتق من المعرف الآمن.

قد ينضم المعرف الآمن معرف المنتج الفريد.

على نحو مفضل، تتضمن الطريقة أيضًا خطوة توليد قيمة تشويش النظام باستخدام المفتاح السري ومعرف المنتج الفريد، حيث يتم اشتقاق المعرف الآمن من، أو يحتوي على، قيمة تشويش النظام. على نحو مفضل، تشتمل خطوة توليد قيمة تشويش النظام على إجراء دالة تجزئة على المفتاح السري ومعرف المنتج الفريد.

على نحو مفضل، تتضمن الطريقة أيضًا توليد قيمة تشويش فيزيائية باستخدام المفتاح الفيزيائي ومعرف المنتج الفريد، حيث يتم اشتقاق المعرف الآمن من، أو يضم، قيمة تشويش النظام. على نحو مفضل، تشتمل خطوة توليد قيمة التشويش الفيزيائية على إجراء دالة تجزئة على المفتاح الفيزيائي ومعرف المنتج الفريد.

كما هو مستخدم هنا، "معرف المنتج الفريد" تعنى المعرف الذي يقوم بتحديد العنصر المصنع بشكل فريد. يتم إعطاء كل عنصر مصنع معرف منتج فريد مختلف. معرف المنتج الفريد هو عادةً سلسلة أو قيمة رقمية أو أبجدية رقمية.

كما هو مستخدم هنا، تعني كلمة "تشفير" عملية تحويل المعلومات باستخدام خوارزمية، لجعل هذه المعلومات غير قابلة للقراءة لأي شخص ماعدا الأشخاص الذين يمتلكون معرفة خاصة بصيغة مفتاح تشفير. فك التشفير هو عملية معكوسة. بعد "مفتاح التشفير" معلومة يتم استخدامها مع خوارزمية التشفير الحسابية لتشفير أو لفك تشفير معلومات. يعد مفتاح التشفير عادةً سلسلة أو قيمة رقمية أو أبجدية رقمية.

كما هو مستخدم هنا، يتم استخدام المصطلح "مفتاح سرى" لوصف مفتاح مستخدم في دالة تجزئة بمفتاح يتم توليدها باستخدام معرف منتج فريد وواحد أو أكثر من المفاتيح الإضافية أو البيانات. في الوقت الذي يتم فيه التوليد، لا يُعرف المفتاح السري من قبل أي طرف ماعدا الطرف الذي قام بإنشاء المفتاح السري. لا يقتصر المصطلح "مفتاح سرى" في هذا السياق على مفتاح خاص في سياق مخطط التشفير غير التماثلي.

كما هو مستخدم هنا، تعد "دالة التجزئة" هي الدالة التي تخطط بيانات مدخلة إلى خرج بمقاس ثابت (عادةً أصغر من البيانات المدخلة) وتسمى قيمة التجزئة. تقوم دالة التجزئة عادةً باستبدال أو تحويل، أو استبدال وتحويل، المعلومات لإنشاء قيمة التجزئة أو قيمة التشويش. على نحو مفضل، تعد دالة التجزئة دالة تجزئة تشفيرية. تنتج دالة التجزئة التشفيرية بصمة أو تدقيق مجموع للبيانات المدخلة. يمكن افتراض تماثل البيانات لو تم استخدام نفس دالة التجزئة التشفيرية حيث تقومان بتوليد نفس قيمة التجزئة. على نحو مميز، تعد دالة التجزئة دالة تجزئة أحادية الاتجاه، والتي تعنى أنه من المستحيل حسابيًا اشتقاق البيانات المدخلة من قيمة التجزئة. يمكن استخدام هذه الخواص في عملية المصادقة، كما سيتم وصفه فيما يلي. يمكن عمل مفتاح لدالة تجزئة عن طريق ضم مفتاح سرى ورسالة مدخلة لإنشاء قيمة تجزئة أو تشويش بمفتاح.

كما هو مستخدم هنا، يعني المصطلح "قيمة التشويش" قيمة تجزئة، أو قيمة تجزئة بمفتاح، أو قيمة أو سلسلة رموز مشتقة مباشرة من قيمة تجزئة ومفتاح سرى.

قد تكون الخاصية الفيزيائية المقاسة للعنصر المصنع أي خاصية فيزيائية مقاسة وقد تكون على أساس الكتلة، أو الحجم، أو الشكل، أو نسيج السطح أو النقش، أو اللون، أو التركيبة الكيميائية أو الاستجابة لمنبه، مثل الاستجابة لمنبه كهربي، أو مغناطيسي أو بصري. يتم على نحو مفضل اختيار الخاصية الفيزيائية المقاسة وقياسها بدقة حتى تكون فريدة على الأرجح لكل عنصر مصنع، أو حتى تكون مختلفة عن الخاصية الفيزيائية المقاسة لأي عنصرين مصنعين. توفر الخاصية الفيزيائية المقاسة على نحو مفضل توقيع فيزيائي للعنصر المصنع. في تجسم مفضل، تعد الخاصية الفيزيائية المقاسة صورة لجزء من تعبئة العنصر المصنع.

قد يكون المعرف الآمن أي نوع من المعرفات لكنه يكون على نحو مفضل سلسلة أو قيمة رقمية أو أبجدية رقمية. قد يكون العلامة أيضاً سلسلة من الرموز أو الأعداد أو قد تكون تمثيلاً تصويريًا مثل رمز شريطي أحادى أو ثنائي الأبعاد.

في أحد التجسيدات، تشتمل خطوة توليد معرف آمن على توليد معرف أول بواسطة تشفير معرف المنتج الفريد مع قيمة تشويش النظام وتوليد المعرف الآمن بواسطة تشفير المعرف الأول مع قيمة التشويش الفيزيائية.

في هذا التجسيد، قد تشتمل الطريقة أيضًا على المصادقة على العنصر المصنع في مركز تحقق، تشتمل خطوة المصادقة على: تحديد العلامة على العنصر؛ وفك تشفير العلامة لاشتقاق المعرف الأول وقيمة التشويش الفيزيائية؛ وفك تشفير المعرف الأول لاشتقاق معرف المنتج الفريد وقيمة تشويش النظام؛ وتوليد مفتاح فيزيائي جديد من خاصية فيزيائية مقاسة للعنصر المصنع؛ وتوليد نسخة جديدة من قيمة التشويش الفيزيائية بأداء دالة تجزئة على المفتاح الفيزيائي الجديد ومعرف المنتج الفريد المشتق؛ ومقارنة النسخة الجديدة لقيمة التشويش الفيزيائية مع قيمة التشويش الفيزيائية المشتقة؛ وتوفير بيان عما إذا كانت قيمة التشويش المشتقة مماثلة للنسخة الجديدة لقيمة التشويش الفيزيائية أو ذات صلة بها.

قد تشمل خطوة المقارنة اشتقاق نتيجة ارتباط وتشتمل خطوة تقديم إشارة على تقديم إشارة عما إذا كانت درجة الارتباط أكبر من قيمة العتبة.

في هذا التجسيد، قد تشتمل خطوة المصادقة أيضًا على: توليد نسخة جديدة للمفتاح السري من معرف المنتج الفريد وواحد أو أكثر من مفاتيح التشفير؛ وتوليد نسخة جديدة من قيمة تشويش النظام بأداء دالة تجزئة على النسخة الجديدة للمفتاح السري ومعرف المنتج الفريد؛ ومقارنة النسخة الجديدة لقيمة تشويش النظام مع قيمة تشويش النظام المشتقة؛ وتوفير بيان عما إذا كانت النسخة الجديدة لقيمة تشويش النظام وقيمة تشويش النظام المشتقة متماثلتان.

في تجسيد آخر، تشتمل خطوة توليد المعرف الآمن على توليد معرف آمن أول بتشفير معرف المنتج الفريد مع قيمة تشويش النظام؛ وتوليد معرف آمن ثانٍ بتشفير معرف المنتج الفريد مع معرف قيمة التشويش الفيزيائية؛ ووضع علامة على العنصر المصنع،

تشتمل العلامة على المعرفين الآمنين الأول والثاني أو معرف أو معرفات مشتقة من المعرفين الآمنين الأول والثاني.

في هذا التجسيد، قد تشتمل الطريقة أيضًا على المصادقة على العنصر المصنع في مركز تحقق، وتشتمل خطوة المصادقة على: تحديد العلامة على العنصر؛ وفك تشفير العلامة لاشتقاق معرف المنتج الفريد، وقيمة تشويش النظام وقيمة التشويش الفيزيائية؛ وتوليد نسخة جديدة من المفتاح السري من معرف المنتج الفريد والواحد أو أكثر من مفاتيح التشفير؛ وتوليد نسخة جديدة لقيمة تشويش النظام بإجراء دالة تجزئة على النسخة الجديدة للمفتاح السري ومعرف المنتج الفريد؛ ومقارنة النسخة الجديدة لقيمة تشويش النظام مع قيمة تشويش النظام المشتقة؛ وتوليد مفتاح فيزيائي جديد من خاصية فيزيائية مقاسة للعنصر المصنع؛ وتوليد نسخة جديدة من قيمة التشويش الفيزيائية بإجراء دالة تجزئة على المفتاح الفيزيائي الجديد ومعرف المنتج الفريد المشتق؛ ومقارنة النسخة الجديدة لقيمة التشويش الفيزيائية مع قيمة التشويش الفيزيائية المشتقة؛ وتوفير إشارة عما إذا كانت النسخة الجديدة لقيمة تشويش النظام مماثلة لقيمة تشويش النظام المشتقة والنسخة الجديدة لقيمة التشويش الفيزيائية مماثلة لقيمة التشويش الفيزيائية المشتقة أو ذات علاقة بها.

في أي من التجسيدين، قد تشتمل خطوة توليد المعرف الآمن الأول على تشفير معرف المنتج الفريد وقيمة تشويش النظام باستخدام مفتاح مولد الرموز، حيث تشتمل خطوة توليد المعرف الآمن الثاني على ضم المعرف الآمن الأول وقيمة التشويش الفيزيائية مع معرف مولد الرموز، وحيث يمكن اشتقاق مفتاح مولد الرموز أو الحصول عليه من جدول بحث في مركز التحقق باستخدام معرف مولد الرموز.

في أي من التجسيدين، قد تشتمل الطريقة أيضًا على خطوة تخزين الواحد أو أكثر من مفاتيح التشفير في مركز تحقق. قد يشتمل الواحد أو أكثر من مفاتيح التشفير على مفتاح استاتيكي ومفتاح ديناميكي، وحيث يتم إنشاء مفتاح ديناميكي جديد لكل دفعة من العناصر المصنعة حيث أنه يتم استخدام نفس المفتاح الاستاتيكي لدفعات كثيرة من العناصر المصنعة

قد يتضمن معرف المنتج الفريد معلومات تحدد دفعة العناصر التي ينتمي إليها العنصر.

يوفر الاختراع إمكانية المصادقة عليهما من خلال المعلومات من المصنع، أي مفاتيح التشفير المتنوعة، وكذلك الخاصية الفيزيائية للعنصر. يوفر ذلك طبقتين من المصادقة، ويتيح اكتشاف تقليد المعرفات على العناصر الأصلية، لكنها ليست في حاجة إلى مساحة تخزين كبيرة لرموز المصادقة.

في جانب آخر من جوانب الاختراع، يتم توفير جهاز لتعليم العنصر المصنع، وهو يشتمل على:

مولد مفاتيح مهيأ لتوليد مفاتيح تشفير؛

مولد رموز مهيأ لتوليد معرف منتج فريد لكل عنصر مصنع؛

مولد مفاتيح فيزيائي مهيأ لتوليد مفاتيح فيزيائية من خاصية فيزيائية مقاسة لكل عنصر مصنع؛

وسيلة معالجة مهيأة لـ :

توليد مفتاح سرى لكل عنصر مصنع باستخدام معرف المنتج الفريد وواحد أو أكثر من مفاتيح التشفير؛

توليد معرف آمن مشتق من أو يضم المفتاح السري والمفتاح الفيزيائي؛

وجهاز تعليم لتعليم كل عنصر مصنع بالمعرف الآمن أو معرف مشتق من المعرف الآمن.

على نحو مفضل، تتم تهيئة المعالج لتوليد قيمة تشويش نظام لكل عنصر مصنع باستخدام المفتاح السري ومعرف منتج فريد، حيث يتم اشتقاق المعرف الآمن من قيمة تشويش النظام أو يحتوي عليها. على نحو مفضل، تتم تهيئة المعالج لتوليد قيمة تشويش النظام لكل عنصر مصنع بإجراء دالة تجزئة على المفتاح السري ومعرف المنتج الفريد.

على نحو مفضل، تتم تهيئة المعالج لتوليد قيمة تشويش فيزيائية لكل عنصر مصنع باستخدام المفتاح الفيزيائي ومعرف المنتج الفريد، حيث يتم اشتقاق المعرف الآمن من قيمة التشويش الفيزيائية أو يحتوي عليها. على نحو مفضل، تتم تهيئة المعالج لتوليد قيمة

التشويش الفيزيائية لكل عنصر مصنع بإجراء دالة تجزئة على المفتاح الفيزيائي ومعرف المنتج الفريد.

في أحد التجسيدات، تتم تهيئة وسيلة المعالجة من أجل: توليد معرف أول لكل عنصر مصنع بتشفير معرف المنتج الفريد مع المفتاح السري أو قيمة تشويش النظام؛ وتوليد المعرف الآمن لكل عنصر مصنع بتشفير المعرف الأول مع قيمة التشويش الفيزيائية.

في تجسيد آخر، تتم تهيئة وسيلة المعالجة من أجل: توليد معرف آمن أول لكل عنصر مصنع بتشفير معرف المنتج الفريد مع المفتاح السري أو قيمة تشويش النظام وتوليد معرف آمن ثانٍ لكل عنصر مصنع بتشفير معرف المنتج الفريد مع المفتاح الفيزيائي أو قيمة التشويش الفيزيائية؛ وتتم تهيئة جهاز التعليم لتعليم كل عنصر مصنع بالمعرف الآمن الأول والمعرف الآمن الثاني أو معرف أو معرفات مشتقة من المعرفين الآمنين الأول والثاني.

قد يكون العنصر المصنع حاوية تحتوى على منتج تبغ. من أمثلة منتجات التبغ، السجائر، والتبغ السائب، والسيجار، والخراطيش أو عبوات أنظمة التدخين المسخنة كهربيًا أو أنظمة السجائر الإلكترونية الأخرى.

يتيح الاختراع المصادقة على العناصر المصنعة بدون الحاجة إلى تخزين كميات كبيرة من المعلومات. يمثل ذلك أهمية لأي أنظمة عملية مناسبة للمصادقة على عناصر منتجة بكميات كبيرة. علاوة على ذلك، يعمل استخدام مفتاح فيزيائي مع معرف منتج فريد (UPI) على زيادة الأمان ويجعل إنتاج السلع المزيفة أو المهربة أكثر صعوبة. توفر إضافة مفتاح فيزيائي نظامًا يمكنه اكتشاف التقليد ومن الصعب نسخه. حتى لو امتلك المزيف المعرفة لأداة محددة مستخدمة لتوليد المفاتيح الفيزيائية، تجعل التوليفة من المفتاح الفيزيائي مع معرف المنتج الفريد عملية التزييف مستحيلة تقريبًا. يتيح الاختراع أيضًا تنفيذ المصادقة عبر الإنترنت، أي عبر الاتصال بمركز تحقق عبر شبكة اتصالات على أساس قيمة تشويش النظام، وكذلك إتاحة تنفيذ المصادقة بدون اتصال على أساس قيمة التشويش الفيزيائية. التعليم المطلوب على كل عنصر هو واحد أو أكثر من الرموز ببساطة وبذلك

يضيف تكلفة قليلة جدًا لكل عنصر مقارنة ببعض الحلول الأخرى، والتي تعتمد على ملصقات تعليم يصعب إعادة إنتاجها فنيًا.

**شرح مختصر للرسومات:-**

سيتم وصف تجسيدات الاختراع وسيُسلط المزيد من الضوء على الاختراع، على سبيل المثال وليس الحصر، بالإشارة إلى الرسومات المرفقة التي فيها:

يمثل الشكل1رسمًا تخطيطيًا لنظام التعليم وفقًا لأحد تجسيدات الاختراع؛

يوضح الشكل2كيف يتم اشتقاق قيمة تشويش النظام وقيمة التشويش فيزيائية؛

يمثل الشكل3مخططًا انسيابيًا يبين طريقة تعليم أحد تجسيدات الاختراع، والتي قد يتم تنفيذها على النظام بالشكل1؛

يمثل الشكل4مخططًا انسيابيًا يبين طريقة مصادقة لتجسيد الاختراع المبين في الشكل3، حيث يتم تنفيذها على النظام في الشكل1؛

يمثل الشكل5مخططًا انسيابيًا يبين طريقة تعليم تجسيد آخر للاختراع، حيث يتم تنفيذها على النظام في الشكل1؛ و

يمثل الشكل6مخططًا انسيابيًا يبين طريقة مصادقة تجسيد الاختراع المبين في الشكل5، حيث يتم تنفيذها على النظام في الشكل1.

**وسائل تنفيذ الإختراع:-**

يمكن استخدام علامات فريدة على العناصر المصنعة لتتبع العناصر. على سبيل المثال، قد يتم ربط طلب العميل بملصق أو ملصقات التعريف لحالة أو حالات شحن معينة تحتوي على بضائع مطلوبة. تعنى "البضائع" في هذا السياق عناصر مصنعة أو غيرها من السلع لغرض التوزيع أو البيع للعملاء. يتيح ذلك للعميل، والمُصنع والوسطاء تتبع موقع البضاعة المطلوبة. قد يتم تحقيق ذلك باستخدام الماسحات الضوئية لمسح المعرفات والاتصال بمركز التحقق. بدلاً من ذلك، يمكن قراءة المعرفات من قبل شخص، حيث يمكنه الاتصال يدويًا مع مركز التحقق. قد يتم أيضًا استخدام المعرفات من قبل العملاء، والسلطات الوطنية وغيرها من الأطراف، للتحقق من أن عنصر محدد يحتوى على منتجات أصلية. على سبيل المثال، قد يستخدم طرف ما ماسحة ضوئية لقراءة المعرف على علبة

شحن (أو يمكن قراءة المعرف من قبل الشخص، كما هو مناقش أعلاه). قد يتم إرسال تفاصيل المعرف إلى مركز التحقق. ثم يمكن قيام مركز التحقق بالبحث أو بالأحرى معالجة تفاصيل المعرف، وتحديد تفاصيل إنتاج علبة الشحن وإرسال هذه التفاصيل إلى الماسح الضوئي، ما يؤدى إلى إتاحة قيام الطرف بالتحقق من أن علبة الشحن، والمنتجات الموجودة بداخله أصلية. في حالة عدم تعرف قاعدة البيانات المركزية على المعرف، فقد يفترض الطرف أن السلع المذكورة مزيفة. قد يتم استخدام المعرفات أيضًا لاقتفاء أثر العناصر. على سبيل المثال، إذا احتاج المصنع استدعاء المنتجات من عدد محدد من علب شحن، فمن الممكن اقتفاء أثر علب الشحن هذه باستخدام معرفاتها.

يمثل الشكل1رسمًا تخطيطيًا لنظام تعليم وفقًا لأحد تجسيدات الاختراع. في هذا التجسيد، يشتمل النظام101على واحد أو أكثر من مراكز الإنتاج103، 105، 107لإنتاج عناصر مصنعة109. قد يشتمل كل مركز إنتاج على خط أو مرفق إنتاج الذي قد يكون خط تصنيع وتغليف سجائر. على نحو مفضل، يتم تنفيذ الإنتاج في دفعات، ويجرى تخصيص كل دفعة لإنتاج عدد محدد من العناصر المصنعة الفردية. إذا كان هنالك اثنان أو أكثر من مراكز الإنتاج، فقد توجد فعليًا في نفس مواقع التصنيع أو مواقع مختلفة. في هذا التجسيد، يتضمن النظام مراكز إنتاج103، 105، 107، إلا أنه قد يتم في الحقيقة تنفيذ الاختراع في أي نقطة استيراد، أو نقطة توزيع، نقطة مشترٍ، أو تاجر جملة أو أي نقطة أخرى في سلسلة الإمداد.

يتضمن كل مركز إنتاج مولد رموز111لتوليد رموز للعناصر المصنعة109. على نحو مفضل، يعد مولد الرموز111حاسوبًا مستقلاً بذاته بالكامل أو وحدة تحكم دقيقة مخصصة لمركز إنتاج محدد. يتضمن كل مركز إنتاج أيضًا مولد مفتاح فيزيائي112يقيس أو يقوم بترميز خاصية فيزيائية لكل عنصر مصنع وتحويل ذلك إلى مفتاح فيزيائي207. يستخدم مولد الرموز111مفاتيح فيزيائية لتوليد رموز لتعليم العناصر.

في هذا التجسيد، يعد مولد المفاتيح الفيزيائية من النوع الموصوف في البراءةWO2007/071788. تتم إضاءة جزء من التغليف لكل عنصر ويتم التقاط صورة للجزء المضيء بواسطة حساس صور رقمي. يتم اختيار جزء التغليف لبنيته الدقيقة

المختلطة المستقرة فيما يتعلق بالوقت. تتميز مواد مثل الورق والكرتون ببنية دقيقة مختلطة يمكن استخدامها بمثابة "بصمة" للعنصر. يتم تحويل صورة البنية الدقيقة من جزء العنصر إلى مفتاح فيزيائي أو توقيع، كما هو موصوف في البراءةWO2007/071788، فيشكل قيمة أو مصفوفة أبجدية رقمي. مولد المفاتيح الفيزيائية لهذا النوع متوفر من Signoptic Technologies, Savoie Technolac ,5 allée Lac d'Aiguebelette BP340 5 ,73375-F ,LE BOURGET-DU-France ,LAC. مع ذلك، قد يتم استخدام أي نوع من مولدات المفاتيح الفيزيائية وقد يتم الاعتماد على خواص فيزيائية أخرى للعنصر مثل الكتلة أو الشكل، أو قد يعتمد حتى على خواص كيميائية أو بيولوجية للعنصر.

في هذا التجسيد، يتضمن كل مركز إنتاج أيضًا جهاز تعليم113التعليم الرموز المتولدة على العناصر المصنعة109. قد يشتمل جهاز التعليم113على أي وسائل تعليم مناسبة، على سبيل المثال وليس الحصر، طابعة نفث مستمر للحبر، أو طابعة نفث حبر عند الطلب، أو طابعة هولوجرافية، أو طابعة ليزر، أو أي طابعة أخرى أو جهاز تعليم يتيح الطباعة أو التعليم للرموز المتولدة على العناصر المصنعة الفردية. قد تكون طباعة أو تعليم الرموز المتولدة على كل عنصر، أو على الغلاف الخارجي، أو على الملصقات أو على أي طريقة ملائمة أخرى. في أحد التجسيدات، تتم طباعة الرموز المتولدة على ملصقات أو علامات لاصقة لوضعها على العناصر المصنعة، على نحو مفضل لا تقبل الإزالة. في أحد التجسيدات، تتم طباعة الرموز المتولدة بشعاع ليزر على طبقة من مادة حساسة لليزر على العنصر المصنع أو على غلاف العنصر. تتيح هذه الطريقة طباعة الرمز من خلال طبقة الغلاف شفافة.

يشتمل النظام101أيضًا على مركز تحقق114يتضمن مولد مفاتيح115التوليد المفاتيح209، 211للاستخدام في التعليم والمصادقة على العناصر المصنعة وخادم مركزي117. في هذا التجسيد، يمكن أن يقوم مولد الرموز111بالاتصال بمركز التحقق114من خلال اتصال آمن بالإنترنت119وخادم121في مركز الإنتاج، أو بأي وسائل اتصال بيانات أخرى. بدلاً من ذلك، قد يقوم مولد المفاتيح111بالاتصال مع مركز التحقق عن طريق بوابة تصنيع مخصصة لواحد أو أكثر من مراكز الإنتاج.

يقوم مولد المفاتيح115بتوليد مفتاح تشفير، يُشار إليه هنا بمفتاح استاتيكي. يقوم مولد المفاتيح115بتوليد نسخة غير مشفرة من المفتاح الاستاتيكي ونسخة مشفرة من المفتاح الاستاتيكي. النسخة غير المشفرة من المفتاح الاستاتيكي، يُشار إليها هنا بالمفتاح الاستاتيكي النشط209، مبينة بخط حدودى متصل في الشكل1. النسخة المشفرة للمفتاح الاستاتيكي، يُشار إليها هنا بالمفتاح الاستاتيكي غير النشط211، مبين بخط حدودي منقط في الشكل1. يتم توليد المفتاح الاستاتيكي النشط209، أي النسخة غير المشفرة للمفتاح الاستاتيكى، في مولد المفاتيح115وبهذا يمكنه الوصول إليه من الخادم المركزي117. يقوم مولد المفاتيح115بإرسال المفتاح الاستاتيكي غير النشط211إلى مولد الرموز111في مركز الإنتاج103، 105، 107.

قد يتم إرسال المفتاح الاستاتيكي غير النشط211من مولد المفاتيح115إلى مولد الرموز111بدعم البيانات غير المتلاشية، على سبيل المثالRom-CD، أوRom-DVDأو قرص صلب قابل للإزالة. يتم نقل دعم البيانات فيزيائيًا إلى مولد الرموز111في مركز الإنتاج103، 105، 107. بدلاً من ذلك، قد يتم إرسال المفتاح الاستاتيكى غير النشط211من مولد المفاتيح115إلى مولد الرموز111عن طريق توصيل شبكة آمن، على سبيل المثال أحد الشبكات التي تشمل تشفيرًا. قد يكون ذلك عند الطلب من مولد الرموز111. يضمن هذا موثوقية، وسرية وسلامة المفتاح الاستاتيكي.

يقوم مولد المفاتيح115أيضًا بتوليد رمز تنشيط213، والذى يشتمل على المفتاح أو رمز لفك تشفير المفتاح الاستاتيكي غير النشط211لتكوين مفتاح استاتيكي نشط209. رمز التنشيط هذا213يمكن الوصول إليه من الخادم المركزي117. على نحو مفضل، يتم تخزين المفتاح الاستاتيكي النشط209ورمز التنشيط213معًا، مع تحديد مركز الإنتاج103، 105، 107الذي يتم له التخصيص.

في أحد التجسيدات، يشتمل المفتاح الاستاتيكي على عدد من الأجزاء. قد يكون الجزء الأولى مجموعة من رموز سرية، على سبيل المثال مصفوفة قاسية. قد تكون المصفوفة القاسية، على سبيل المثال، سلسلة طويلة من أرقام عشوائية أو عشوائية زائفة. قد يتضمن عدد الأجزاء أيضًا محددًا فريدًا للمفتاح الاستاتيكي، ورمزًا متسلسلاً يحدد كيفية ضم

المفتاح الاستاتيكي مع مفتاح ديناميكي (مناقش أدناه)، وشهادة تشفيرية رقمية مرتبطة بمعرف فريد للمفتاح الاستاتيكي وسياسة أو رخصة المفتاح الاستاتيكي التي تحتوي على الشهادة التشفيرية الرقمية المتولدة أعلاه.

على نحو مفضل، يتم تشفير المفتاح الاستاتيكي غير النشط، بعبارة أخرى النسخة المشفرة من المفتاح الاستاتيكي، وبالتحديد مجموعة الرموز السرية، باستخدام شفرة قوية. من أمثلة التشفير المناسب، التشفير الكتلي (معيار تشفير بيانات) الثلاثي أو التشفير الثلاثي/التشفير الكتلي ريجندايل. يُطبق كلٌ منها خوارزمية شفرة معيار تشفير البيانات ثلاث مرات على كل كتلة بيانات ويمثل معيار تشفير البيانات الثلاثي/ريجندايل تباين صغير ل معيار تشفير البيانات الثلاثي الذي يتم تطويره من قبلIBM. في تلك الحالة، يشتمل معيار تشفير البيانات الثلاثي أو مفتاح معيار تشفير البيانات الثلاثي/ريجندايل على رمز تنشيط213. بالتالي، في تجسيد مفضل، يتم فك تشفير المفتاح الاستاتيكي النشط209، ويتم تشفير المفتاح غير النشط211باستخدام معيار تشفير البيانات الثلاثي أو مفتاح معيار تشفير البيانات الثلاثي/ريجندايل، ويشتمل رمز التنشيط213على معيار تشفير البيانات الثلاثي ذلك أو مفتاح معيار تشفير البيانات الثلاثي/ريجندايل.

في الخطوة التالية203، يتم تسجيل المفتاح الاستاتيكي غير النشط211المستقبل من مولد الرموز111. يتم ذلك من خلال مولد الرموز111الذي يرسل إلى مركز التحقق114معلومات215عن المفتاح الاستاتيكي المستقبل وأي معلومات آلية ذات الصلة (غير موضحة). يتم على نحو مفضل إرسال ذلك عن طريق وصلة إنترنت آمنة119، كما هو مبين في الشكل1، إلا أنه قد يتم إرساله بواسطة قناة أخرى مناسبة. يقوم مركز التحقق114بإعادة رمز التنشيط213إلى مولد الرموز111. يتيح رمز التنشيط213تنشيط المفتاح الاستاتيكي غير النشط211، وهذا مبين تخطيطيًا في217. يتم على نحو مفضل أيضًا إرسال رمز التنشيط213عبر وصلة إنترنت آمنة119، كما هو مبين في الشكل1. يتم على نحو مفضل ترتيب إجراء التسجيل بحيث لا يتم على الإطلاق نقل المفتاح الاستاتيكي النشط209عبر الإنترنت.

قد يأخذ إجراء التسجيل شكل آلية استبدال زوج المفاتيح العام/الخاص التقليدي. قد يستخدم ذلك زوج مفتاح لاتماثلي مع شهادة تشفير رقمية تشكل جزءًا من المفتاح الاستاتيكي، كما هو مناقش أعلاه. في تلك الحالة، قد يكون المفتاح العام لزوج المفاتيح اللاتماثلي في شكل مفتاح صادر من طرف ثالث، على سبيل المثال، سلطة حكومية. قد تشتمل المعلومات215حول المفتاح الاستاتيكي المستقبل الذي يتم إرساله من مولد الرموز111إلى مركز التحقيق114، على المعرف الفريد للمفتاح الاستاتيكي الذي يشكل جزءًا من المفتاح الاستاتيكي، كما هو مناقش أعلاه. قد تشتمل المعلومات الآلية ذات الصلة (غير مبينة) التي يتم أيضًا إرسالها من مولد الرموز111إلى مركز التحقق114، على معرف فريد أو شهادة لمولد الرموز111أو مركز الإنتاج. قد يتضمن ذلك المعرف الفريد معلومات حول مكان وهوية مولد الرموز أو مركز الإنتاج، والذى تمت المصادقة عليه مسبقًا للإنتاج. على نحو مفضل، يتم تشفير المعرف الفريد للمفتاح الاستاتيكي ومولد الرموز أو معرف مركز الإنتاج، باستخدام المفتاح العام لزوج المفاتيح اللاتماثلي مع شهادة المفتاح الاستاتيكي.

بمجرد استقبال مركز التحقق114للمعرف الفريد للمفتاح الاستاتيكي المشفر ومولد الرموز أو معرف مركز الإنتاج، يستطيع مركز التحقق114فك التشفير باستخدام المفتاح الخاص لزوج المفاتيح اللاتماثلي مع شهادة المفتاح الاستاتيكي. وبعد ذلك، قديقوم مركز التحقق بالتأكد من أن المعرف الفريد للمفتاح الاستاتيكي ومولد الرموز أو مركز الإنتاج صالح. ثم، يقوم مركز التحقق114بإعادة إرسال رمز التشفير213إلى مولد الرموز111. كما هو مذكور بالفعل، على نحو مفضل، يكون رمز التنشيط213في شكل معيار تشفير بيانات ثلاثي أو شفرة معيار تشفير بيانات ثلاثي/ريجندايل. يقوم مركز التحقق بتشفير رمز التنشيط (على سبيل المثال معيار تشفير البيانات الثلاثي أو شفرة معيار تشفير البيانات الثلاثي/شفرة ريجندايل) مع المفتاح العام لزوج المفاتيح اللاتماثلي المرتبط بشهادة المفتاح الاستاتيكي. تيح ذلك فك تشفير رمز التنشيط (على سبيل المثال معيار تشفير البيانات الثلاثي أو شفرة معيار تشفير البيانات الثلاثي/شفرة ريجندايل) بواسطة مولد الرموز باستخدام المفتاح الخاص لزوج المفاتيح اللاتماثلي المرتبط بشهادة المفتاح الاستاتيكي. ثم، يمكن تنشيط المفتاح الاستاتيكي

غير النشط211باستخدام رمز التنشيط الذي تم فك تشفيره213لتكوين المفتاح الاستاتيكي النشط209.

بمجرد تنشيط المفتاح الاستاتيكي غير النشط211في مولد الرموز111، يصبح مركز الإنتاج قادرًا على تصنيع العناصر وإنتاج رموز للعناصر المصنعة في مولد الرموز111.

يقوم مولد الرموز111بتوليد مفتاح جديد، هنا يُشار إليه بالمفتاح الديناميكى219، لكل دفعة من العناصر المصنعة. من المفضل أن يكون المفتاح الديناميكي219رمزًا سريًا عشوائيًا، مثل رقم عشوائي. يستخدم مولد الرموز المفتاح الديناميكي219لدفعة ما، مع المفتاح الاستاتيكي النشط209، لتوليد مفتاح سرى223. يمثل المفتاح السري223الـnالمستخدم مع المفاتيح الفيزيائية ومعرف المنتج الفريد (UPI) لكل عنصر لتوليد رموز221 (على سبيل المثال، رموز أبجدية – رقمية) تُعلم العناصر المصنعة في تلك الدفعة بها. في هذا التجسيد، يشتمل معرف المنتج الفريد لكل عنصر على تفاصيل إنتاج تحدد وقت الإنتاج مع قيمة العداد التراكمي لتمييز العناصر المنتجة خلال فترة زمنية واحدة بنفس مركز الإنتاج.

يستخدم مولد الرموز دالة تجزئة تشفيرية على مجموعة من معرف المنتج الفريد مع المفتاح السري ومجموعة من معرف المنتج الفريد مع المفتاح الفيزيائي. يعمل ذلك على إنشاء بصمات رقمية، يُشار إليه هنا بـ "قيم تشويش"، للعنصر، ويتم استخدام قيم التشويش هذه لتوليد الرموز221التي يتم وضعها على البنود بواسطة جهاز التعليم113. بالإضافة إلى دوال التجزئة المستخدمة على نحو شائع، فإن مجموعة متنوعة من التقنيات متاحة لتوليد قيم التجزئة أو قيم التشويش، التي تتضمن، على سبيل المثال وليس الحصر: تحويل، استبدال، استبدال مجدول وفهرسة.

يوضح الشكل2طريقة توليد قيم التشويش التي ينفذها مولد الرموز111. للقيام بتوليد قيمة تشويش النظام225، يتم أولاً اشتقاق المفتاح السري من المفتاح الاستاتيكي النشط209، والمفتاح الديناميكي219ومعرف المنتج الفريد221. المفتاح الديناميكي219والمفتاح الاستاتيكي النشط209معروفان فقط لمركز التحقق114ولمولد

الرموز111. في الخطوة 301، يتم استخدام المفتاح الديناميكي ومعرف المنتج الفريد لاستخراج المفتاح السري من المصفوفة القاسية الموجود في المفتاح الاستاتيكي، وفقًا لرمز متسلسل داخل المفتاح الاستاتيكي. ثم يتم تجزئة المفتاح السري223ومعرف المنتج الفريد221في الخطوة 303لإنتاج تشويش النظام للعنصر. للقيام بتوليد قيمة التشويش الفيزيائية227، يتم تجزئة المفتاح الفيزيائي207مع معرف المنتج الفريد221في الخطوة 305. قد تكون دالة التجزئة المستخدمة لتوليد قيمة تشويش النظام هي نفسها دالة التجزئة المستخدمة لتوليد قيمة التشويش الفيزيائية أو مختلفة عنها.

يوضح الشكل3طريقة لاستخدام قيمة تشويش النظام وقيمة التشويش الفيزيائية لتوليد معرف آمن لكل عنصر وفقاً للتجسيد الأول للاختراع. في الخطوة 311يتم ضم قيمة تشويش النظام225ومعرف المنتج الفريد221. في الخطوة 313يتم تشفير قيمة تشويش النظام ومعرف المنتج الفريد المجتمعين بواسطة مفتاح تعتيم مولد الرموز (231 (CGOKلإنتاج معرف أول241. يعد مفتاح تعتيم مولد الرموز مخصصًا لمولد الرموز ويتم تحميله مسبقاً على مولد الرموز. ثم، يتم ضم المعرف الأول241مع قيمة التشويش الفيزيائية227ومعرف مولد رموز233. سيسمح معرف مولد الرموز (233 (CGIDبالحصول على مفتاح تعتيم مولد الرموز أثناء المصادقة. ثم، يتم تشفير المعرف الأول، وقيمة التشويش الفيزيائية ومفتاح تعتيم مولد الرموز باستخدام مفتاح شامل235في الخطوة 317لإنتاج المعرف الآمن251. المفتاح الشامل235مشترك لجميع مراكز الإنتاج، وقد يكون جزءًا من زوج المفاتيح التماثلي أو اللاتماثلي المعروف لمركز التحقق. ثم، يتم تعليم المعرف الآمن251على العنصر في الخطوة 319بواسطة جهاز التعليم113.

يحتفظ مولد الرموز111أو مركز الإنتاج103، 105، 107بعدد الرموز التي يتم تعليم العناصر المصنعة بها. بالإضافة إلى ذلك، يقوم مولد الرموز111بإرسال المفتاح الديناميكي219لكل دفعة، مع معلومات حول الدفعة (ليست مبينة)، إلى مركز التحقق114. قد يتم القيام بذلك من خلال وصلة إنترنت آمنة119. قد تتضمن المعلومات حول الدفعة معلومات مختلفة، على سبيل المثال وليس الحصر العلامة التجارية، والسوق المستهدفة أو جهة الوصول المستهدفة. لا يلزم إرسال المفاتيح الديناميكية219إلى مركز التحقق114في

الوقت الفعلي ويمكن إرساله لمركز التحقق في أي وقت مناسب، على سبيل المثال شهريًا. يتم تخزين المفاتيح الديناميكية219المرسلة إلى مركز التحقق114في قاعدة بيانات (على سبيل المثال، في خادم مركزي117) في مركز التحقق114أو يمكن الوصول إليها من خلاله. يتم على نحو مفضل تخزين المفتاح الديناميكي219لكل دفعة مع معلومات الدفعة المرسلة إلى مركز التحقق114في نفس الوقت.

على نحو مفضل، يتم حذف المفتاح الاستاتيكي النشط209عندما يكون مولد الرموز111في مركز إنتاج محدد103، 105، 107خارج الخدمة. يمنع ذلك المستخدم الخبيث من الدخول على المفتاح الاستاتيكي النشط209بدون تسجيل صحيح. قد يتم توفير وسيلة إضافية لتعطيل مولد الرموز111ومنع الاستخدام غير المصرح به لمولد الرموز111ومركز الإنتاج.

يوضح الشكل4الخطوات المنفذة بواسطة مركز التحقق114ومن قبل المستخدم601عندما يرغب المستخدم601في التصديق على عنصر مصنع فردي معلّم وفقًا للعملية في الشكل3. يقوم المستخدم601بقراءة الرمز221على العنصر ثم إرساله إلى مركز التحقق114. هذا مبين في الشكل1. قد يقوم المستخدم601بإرسال الرمز إلى مركز التحقق114بأي وسيلة مناسبة مثل وصلة إنترنت آمنة أو غير آمنة.

يستقبل مركز التحقق المعرف الآمن في الخطوة 321. يتم فك تشفير المعرف الآمن باستخدام المفتاح الشامل235 (أو المفتاح المطابق في زوج المفاتيح إذا تم استخدام مفاتيح لاتماثلية) في الخطوة 323لإظهار قيمة التشويش الفيزيائية227والمعرف الأول241. يتم إظهار معرف مولد الرموز أيضًا. باستخدام جدول البحث، يتم من ثم الحصول على مفتاح تعتيم مولد الرموز231من معرف مولد الرموز. ويتم من ثم فك شفرة المعرف الأول في الخطوة 325باستخدام مفتاح تعتيم مولد الرموز231لإظهار تشويش النظام225ومعرف المنتج الفريد221. بهذه المعلومات، مع المفتاح الاستاتيكيالنشط209والمفتاح الديناميكي219والمفتاح الفيزيائي الجديد، يمكن إعادة إنشاء كلاً من قيمة التشويش الفيزيائية وقيمة تشويش النظام للمصادقة على العنصر.

للقيام بإنشاء قيمة التشويش الفيزيائية، يجب الحصول على مفتاح فيزيائي جديد من قبل المستخدم601في الخطوة 327عن طريق تسجيل صورة للجزء من العنصر بنفس الطريقة وتحت نفس الظروف كما هى مستخدمة لتوليد المفتاح الفيزيائي الأصلي207. ثم، يتم تجزئة معرف المنتج الفريد والمفتاح الفيزيائي الجديد لتوليد قيمة تشويش فيزيائية جديدة في الخطوة 329. في الخطوة 331، تتم مقارنة قيمة التشويش الفيزيائية الجديد مع قيمة التشويش الفيزيائية المستخرجة الموضحة في الخطوة 323. إذا كانت قيمة التشويش الفيزيائية الجديدة مماثلة بشكل كافٍ لقيمة التشويش الفيزيائية المستخرجة، يتم استكمال جزء من عملية المصادقة. إذا لم تكن قيمة التشويش الفيزيائية الجديدة مماثلة بشكل كافٍ لقيمة التشويش الفيزيائية المستخرجة، يتم تحديد العنصر بأنه غير مصادق عليه في الخطوة 339.

قد يتطلب تماثل قيمة التشويش الفيزيائية الجديدة قيمة التشويش الفيزيائية المستخرجة للعنصر حتى يتم اعتباره مصادق عليه. ومع ذلك، من الممكن السماح ببعض الاختلافات بين قيمة التشويش الفيزيائية الجديدة وقيمة التشويش الفيزيائية المستخرجة عن طريق استخدام نتيجة الارتباط وطلب نتيجة ارتباط العتبة حتى يتم اعتبار العنصر مصادق عليه. تصف البراءة US2005/0257064طريقة إحصائية مناسبة لحساب درجة الارتباط أو التماثل بين توقيعين رقميين مشتقين من خواص فيزيائية مقاسة لوسط ليفى.

من الممكن لكلٍ من المستخدم601أو مركز التحقق114تنفيذ الخطوة 329و331. إذا تم تزويد المستخدم601بمعرف المنتج الفريد عن طريق مركز التحقق، يمكن للمستخدم النهائي المصادقة على العنصر علىأساس قيمة التشويش الفيزيائية. بالمثل، إذا تم إمداد المفتاح الفيزيائي الجديد إلى مركز التحقق114، فيمكن لمركز التحقق المصادقة على العنصر على أساس قيمة التشويش الفيزيائية.

لإعادة إنشاء قيمة تشويش النظام، يجب إعادة توليد المفتاح السري، في الخطوة 333، باستخدام معرف المنتج الفريد ومعرف مولد الرموز، ويصبح مركز التحقق114قادرًا على استعادة المفتاح الديناميكي219والمفتاح الاستاتيكي النشط209من سجلات محفوظة في مركز التحقق. ثم، تتم إعادة توليد المفتاح السري باستخدام معرف المنتج الفريد221،

والمفتاح الديناميكي219والمفتاح الاستاتيكي النشط209. في الخطوة 335، يتم إعادة إنشاء قيمة تشويش النظام الجديدة بواسطة تجزئة معرف المنتج الفريد والمفتاح السري. في الخطوة 337، تتم مقارنة قيمة تشويش النظام الجديدة بقيمة تشويش النظام المستخرجة في الخطوة 325. إذا تماثلت قيمة تشويش النظام الجديدة وقيمة تشويش النظام المستخرجة فيمكن تحديد أن العنصر مصادق عليه في الخطوة 339.

في أحد التجسيدات، مطلوب مقارنات كل من قيمة التشويش الفيزيائية وقيمة تشويش النظام لاعتبار العنصر مصادق عليه. مع ذلك، في الإمكان السماح بالمصادقة على أساس واحد فقط من تلك المراجعات حسب الرغبة.

من المفتاح الاستاتيكي النشط المشتق209، يمكن تحديد مركز الإنتاج103، 105، 107الذي تم فيه تصنيع العنصر، حيث أنه من المفضل تخزين المفاتيح الاستاتيكية النشطة في مركز التحقق مع تفاصيل مراكز الإنتاج المرتبطة بها. من المفتاح الديناميكى المشتق219، يمكن تحديد معلومات الدفعة للعنصر حيث أنه يتم على نحو مفضل تخزين المفاتيح الديناميكية في مركز التحقق مع معلومات الدفعة ذات الصلة. وبالتالي، يمكن أن يقوم مركز التحقق114باشتقاق، من الرمز221المرسل من المستخدم601، معلومات603مختلفة حول العنصر الفردي وكذلك مراجعة المصادقة للعنصر. ثم، يمكن إرسال جميع، أو أجزاء مختارة من، المعلومات603التي تتضمن إشارة عما إذا كان العنصر مصادق عليه إلى المستخدم601أو لا. هذا مبين في الشكل1. يتم على نحو مفضل إرسال المعلومات603إلى المستخدم601من خلال نفس الوسيلة مثلما تم إرسال الرمز الأصلي.

يوضح الشكل5عملية التعليم وفقًا للتجسيد الثاني للاختراع. في طريقة الشكل5، يتم إنتاج معرفين آمنين، أحدهما على أساس قيمة تشويش النظام225والآخر على أساس قيمة التشويش الفيزيائية227. يتم ضم قيمة تشويش النظام225مع معرف المنتج الفريد221في الخطوة 341. ثم يتم تشفير قيمة تشويش النظام وقيمة التشويش الفيزيائية مع مفتاح تعتيم مولد الرموز231 في الخطوة 343لإنتاج المعرف الأول241في التجسيد الأول للشكل3. ثم يتم ضم المعرف الأول241مع معرف مولد الرموز في الخطوة 345وتشفيره بالمفتاح الشامل235 في الخطوة 347 لإنتاج معرف آمن أول271. يتم ضم قيمة التشويش

الفيزيائية227مع معرف المنتج الفريد في الخطوة 221لإنتاج معرف ثانٍ 261. يتم تشفير المعرف الثاني بالمفتاح الشامل235في الخطوة 353لإنتاج معرف آمن ثانٍ. ثم يمكن تعليم العنصر في الخطوة 355بالمعرف الآمن الأول271والمعرف الآمن الثاني281، أو مع علامة أو علامات مشتقة من مجموعة المعرف الآمن الأول271والمعرف الآمن الثاني281.

يوضح الشكل6الخطوات المنفذة للمصادقة على العنصر المعلم باستخدام العملية الموضحة في الشكل5. في الخطوة 401تتم قراءة العلامة أو العلامات من قبل المستخدم ويقوم المستخدم باشتقاق المعرف الآمن الأول271والمعرف الآمن الثاني281. في الخطوة 403، يتم استخدام المفتاح الشامل235لاشتقاق قيمة التشويش الفيزيائية227، ونسخة أولى من معرف المنتج الفريد221، المعرف الأول241ومعرف مولد الرموز233. إذا كان لدى المستخدم المفتاح الشامل235، فيمكن أن يقوم المستخدم بالمصادقة على العنصر على أساس المعرف الآمن الثاني بدون اتصال، أي بدون الحاجة إلى الاتصال بمركز التحقق. يقوم المستخدم بتوليد مفتاح فيزيائي جديد في الخطوة 407ويتم تجزئة هذا مع معرف المنتج الفريد لتوليد قيمة تشويش فيزيائية جديدة في الخطوة 409. يمكن قيام المستخدم بمقارنة قيمة التشويش الفيزيائية الجديدة مع قيمة التشويش الفيزيائية المستخرجة في الخطوة 403، في الخطوة 411. كما هو موصوف بالإشارة إلى الشكل3، يمكن اعتبار العنصر مصادقًا عليه في الخطوة 419إذا كانت قيمة التشويش الفيزيائية الجديدة هي نفسها، أو مماثلة بما يكفي، لقيمة التشويش الفيزيائية المستخرجة.

في الخطوة 405، يتم استخدام معرف مولد الرموز بواسطة مركز التحقق لاستعادة مفتاح تعتيم مولد الرموز231، ويتم استخدام مفتاح تعتيم مولد الرموز لفك تشفير المعرف الأول241لإظهار تشويش النظام والنسخة الثانية من معرف المنتج الفريد. في الخطوة 408، يمكن اختياريًا مقارنة النسخة الثانية من معرف المنتج الفريد مع النسخة الثانية معرف المنتج الفريد كمراجعة. في الخطوة 423، يقوم مركز التحقق114باستعادة المفتاح الديناميكي219والمفتاح الاستاتيكي النشط209باستخدام معرف مولد الرموز ومعرف المنتج الفريد. في الخطوة 415، يتم توليد قيمة تشويش النظام الجديدة عن طريق إعادة توليد مفاتح سرى أولا من معرف المنتج الفريد، ومفتاح ديناميكي ومفتاح استاتيكي، ومن ثم عن طريق

تجزئة المفتاح السري مع معرف المنتج الفريد. في الخطوة 417، تتم مقارنة قيمة تشويش النظام الجديدة مع قيمة تشويش النظام المستخرجة في الخطوة 405. إذا كانتا متماثلتين، فيمكن إتمام المصادقة على العنصر في الخطوة 419. كما هو الحال مع التجسيد للشكل3، قد يكون مطلوبًا المصادقة على أساس كل من قيمة تشويش النظام وقيمة التشويش الفيزيائية لعنصر حتى يتم اعتباره مصادقًا عليه.

**طرق تطبيق الإختراع صناعياً:-**

بالرغم من أن الاختراع قد تم وصفه بالإشارة إلى صناعة السجائر، إلا أنه ينبغي أن يكون واضحًا أن الاختراع قابلاً للتطبيق على أي منتجات تتطلب مصادقة، مثل السلع الدوائية، والمشروبات الكحولية والسلع الكمالية.

## عناصر الحماية

1. طريقة تعليم العنصر المصنّع، تشمل:

إنشاء معرف منتج فريد للعنصر المصنع؛

إنشاء واحد أو أكثر من مفاتيح التشفير؛

توليد مفتاح سرى باستخدام معرف المنتج الفريد وواحد أو أكثر من مفاتيح التشفير؛

توليد مفتاح فيزيائي من خاصية فيزيائية مقاسة للعنصر المصنع؛

توليد معرف آمن مشتق من، أو يضم، المفتاح السري والمفتاح الفيزيائي؛ و

وضع علامة على العنصر المصنع، وتشتمل العلامة على المعرف الآمن أو معرف مشتق من المعرف الآمن.

2. طريقة، وفقًا لعنصر الحماية1، تشتمل أيضًا على توليد قيمة تشويش نظام باستخدام المفتاح السري ومعرف المنتج الفريد، حيث يتم اشتقاق المعرف الآمن من قيمة تشويش النظام أو يحتوي عليها.

3. طريقة، وفقًا لعنصر الحماية1أو2، تشتمل أيضًا على توليد قيمة تشويش فيزيائية باستخدام المفتاح الفيزيائي ومعرف المنتج الفريد، حيث يتم اشتقاق المعرف الآمن من قيمة تشويش النظام أو يحتوي عليها.

4. طريقة، وفقًا لأي عنصر حماية سابق، حيث يضم المعرف الآمن بها معرف المنتج الفريد.

5. طريقة، وفقًا لعنصر الحماية4عندما يعتمد على عنصري الحماية2و3، تشمل خطوة توليد المعرف الآمن بها توليد معرف أول بواسطة تشفير معرف المنتج الفريد مع قيمة

تشويش النظام وتوليد المعرف الآمن بواسطة تشفير المعرف الأول مع قيمة التشويش الفيزيائية.

6. طريقة، وفقًا لعنصر الحماية5، تشتمل أيضًا على المصادقة على العنصر المصنع في مركز تحقق، تشتمل خطوة المصادقة على:

تحديد العلامة على العنصر؛

فك تشفير العلامة لاشتقاق المعرف الأول وقيمة التشويش الفيزيائية؛

فك تشفير المعرف الأول لاشتقاق معرف المنتج الفريد وقيمة تشويش النظام؛

توليد مفتاح فيزيائي جديد من خاصية فيزيائية مقاسة للعنصر المصنع؛

توليد نسخة جديدة من قيمة التشويش الفيزيائية بإجراء دالة تجزئة على المفتاح الفيزيائي الجديد ومعرف المنتج الفريد المشتق؛

مقارنة النسخة الجديدة لقيمة التشويش الفيزيائية مع قيمة التشويش الفيزيائية المشتقة؛ و

توفير إشارة عما إذا كانت قيمة التشويش المشتقة مماثلة للنسخة الجديدة لقيمة التشويش الفيزيائية أو مرتبطة بها.

7. طريقة، وفقًا لعنصر الحماية6، تشتمل خطوة المصادقة أيضًا على:

توليد نسخة جديدة من المفتاح السري من معرف المنتج الفريد وواحد أو أكثر من مفاتيح التشفير؛

توليد نسخة جديدة من قيمة تشويش النظام بإجراء دالة تجزئة على النسخة الجديدة للمفتاح السري ومعرف المنتج الفريد؛

مقارنة النسخة الجديدة لقيمة تشويش النظام مع قيمة تشويش النظام المشتقة؛ و

توفير إشارة عما إذا كانت النسخة الجديدة لقيمة تشويش النظام وقيمة تشويش النظام المشتقة متماثلتان.

8. طريقة، وفقًا لعنصر الحماية4عندما يتعلق بعنصري الحماية2و3، تشتمل خطوة توليد المعرف الآمن فيها على توليد معرف آمن أول بتشفير معرف المنتج الفريد مع قيمة تشويش النظام؛

توليد معرف آمن ثانٍ بتشفير معرف المنتج الفريد مع معرف قيمة التشويش الفيزيائية؛ و

وضع علامة على العنصر المصنع، تشتمل العلامة على المعرفين الآمنين الأول والثاني أو معرف أو معرفات مشتقة من المعرفين الآمنين الأول والثاني.

9. طريقة وفقًا لعنصر الحماية8، تشتمل أيضًا على المصادقة على العنصر المصنع، في مركز تحقق، تشتمل خطوة المصادقة على:

تحديد العلامة على العنصر؛

فك ترميز العلامة لاشتقاق معرف المنتج الفريد، وتشويش النظام والتشويش الفيزيائي؛

توليد نسخة جديدة من المفتاح السري من معرف المنتج الفريد وواحد أو أكثر من مفاتيح التشفير؛

توليد نسخة جديدة من قيمة تشويش النظام بإجراء دالة تجزئة على النسخة الجديدة للمفتاح السري ومعرف المنتج الفريد؛

مقارنة النسخة الجديدة لقيمة تشويش النظام مع قيمة تشويش النظام المشتقة؛

توليد مفتاح فيزيائي جديد من خاصية فيزيائية مقاسة للعنصر المصنع؛

توليد نسخة جديدة من قيمة التشويش الفيزيائية بإجراء دالة تجزئة على المفتاح الفيزيائي الجديد ومعرف المنتج الفريد المشتق؛

مقارنة النسخة الجديدة لقيمة التشويش الفيزيائية مع قيمة التشويش الفيزيائية المشتقة؛ و

توفير إشارة عما إذا كانت النسخة الجديدة لقيمة تشويش النظام مماثلة لقيمة تشويش النظام المشتقة والنسخة الجديدة لقيمة التشويش الفيزيائية مماثلة لقيمة التشويش الفيزيائية المشتقة أو ذات علاقة بها.

10. طريقة، وفقًا لأي عنصر حماية سابق، حيث يشتمل واحد أو أكثر من مفاتيح التشفير على مفتاح استاتيكي ومفتاح ديناميكي، وحيث يتم إنشاء مفتاح ديناميكي جديد لكل دفعة من العناصر المصنعة.

11. طريقة، وفقًا لأي عنصر حماية سابق، حيث يتضمن معرف المنتج الفريد المعلومات التي تحدد دفعة العناصر التي ينتمي إليها العنصر.

12. جهاز تعليم العنصر المصنع، يشتمل على:

مولد مفاتيح مهيأ لتوليد مفاتيح تشفير؛

مولد رموز مهيأ لتوليد معرف منتج فريد لكل عنصر مصنع؛

مولد مفاتيح فيزيائي مهيأ لتوليد مفاتيح فيزيائية من خاصية فيزيائية مقاسة لكل عنصر مصنع؛

وسيلة معالجة مهيأة لـ :

توليد مفتاح سرى لكل عنصر مصنع باستخدام معرف المنتج الفريد وواحد أو أكثر من مفاتيح التشفير؛

توليد معرف آمن مشتق من أو يضم المفتاح السري والمفتاح الفيزيائي؛

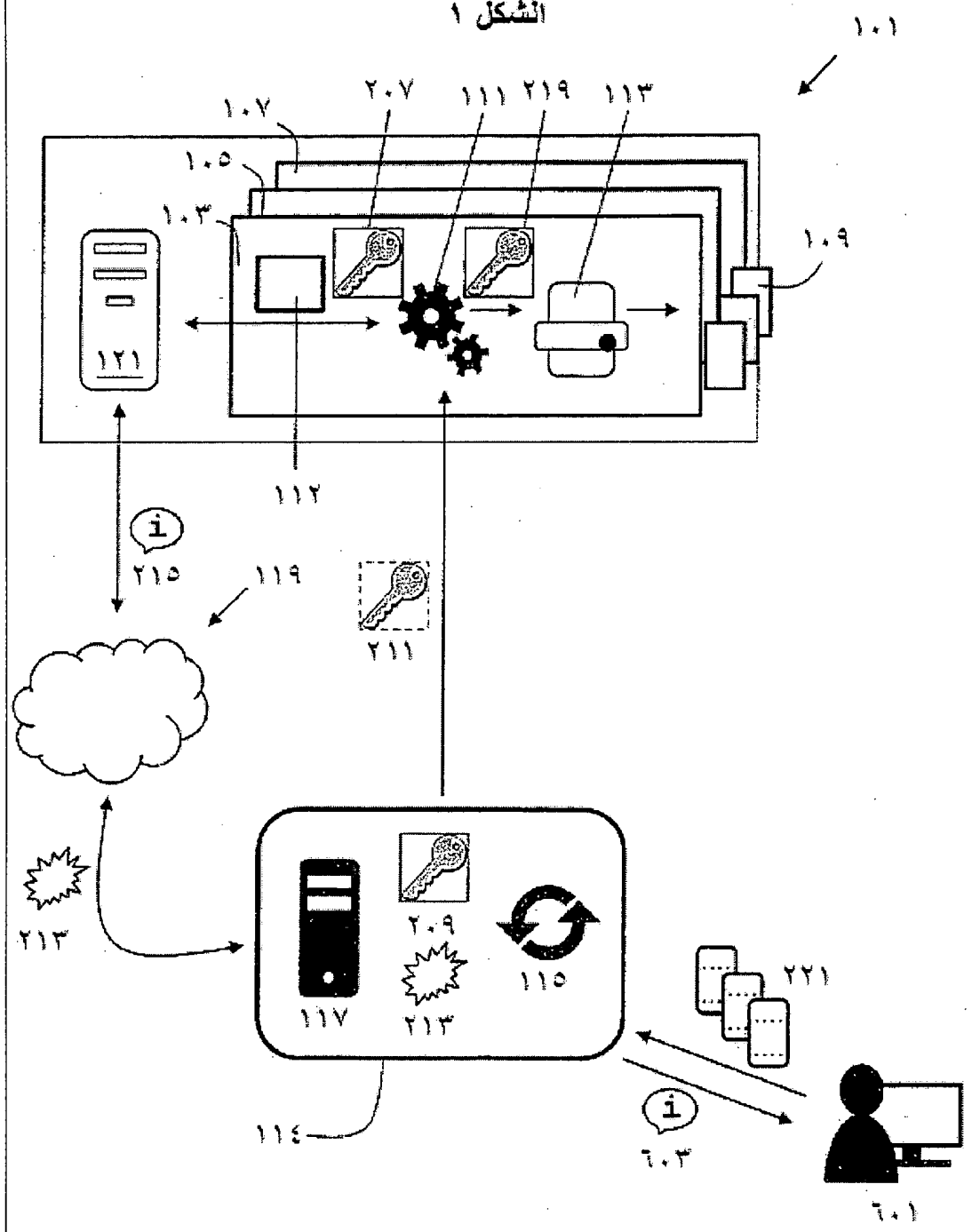
وجهاز تعليم لتعليم كل عنصر مصنع بالمعرف الآمن أو معرف مشتق من المعرف الآمن.

13. جهاز، وفقًا لعنصر الحماية12، تتم فيه تهيئة المعالج لتوليد قيمة تشويش نظام لكل عنصر مصنع بإجراء دالة تجزئة على المفتاح السري ومعرف منتج فريد، حيث يتم اشتقاق المعرف الآمن من قيمة تشويش النظام أو يحتوي عليها.

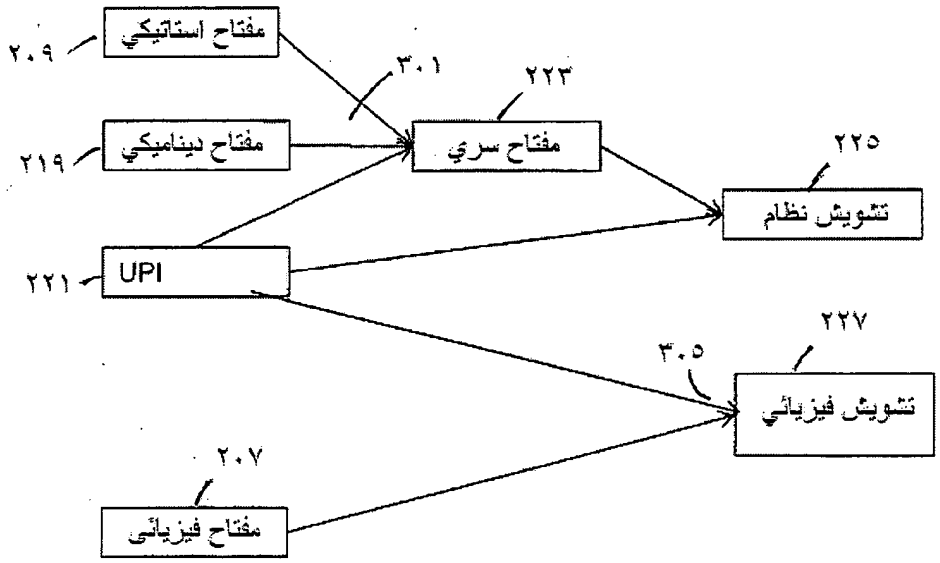
14. جهاز، وفقًا لعنصر الحماية12أو13، حيث تتم تهيئة المعالج لتوليد قيمة تشفير فيزيائية لكل عنصر مصنع بإجراء دالة تجزئة على المفتاح الفيزيائي ومعرف المنتج الفريد، حيث يتم اشتقاق المعرف الآمن من، أو يضم، قيمة التشويش الفيزيائية.

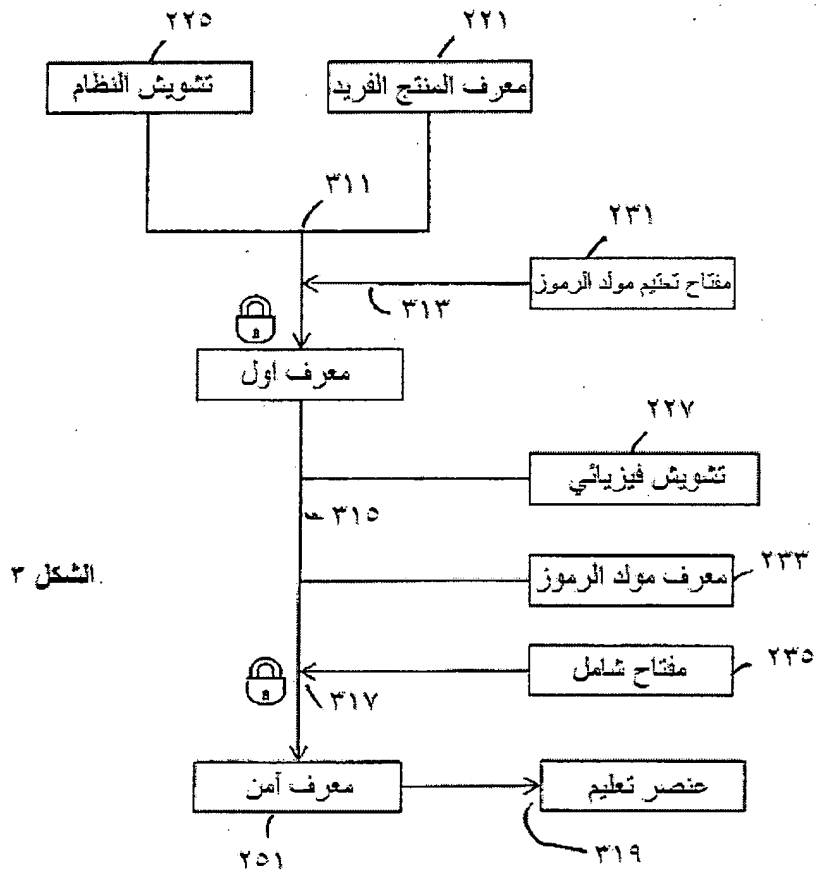
15. جهاز، وفقًا لأي من عناصر الحماية12إلى14، حيث يكون العنصر المصنع حاوية تحتوى على منتج تبغ.

الشكل ١

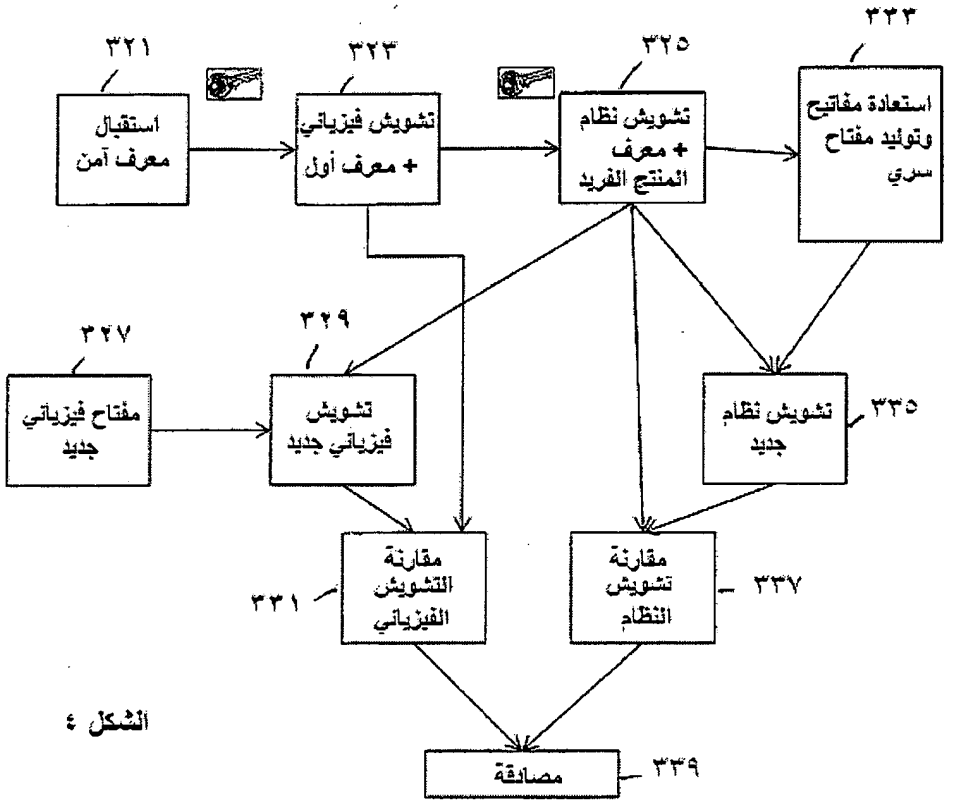

١٠١
١٠٧
٢٠٧
١١١
٢١٩
١١٣
١٠٥
١٠٣
١٠٩
١٢١
١١٢
i
٢١٥
١١٩
٢١١
٢١٣
٢٠٩
١١٥
٢٢١
١١٧
٢١٣
١١٤
i
٦٠٣
٦٠١

الشكل ٢

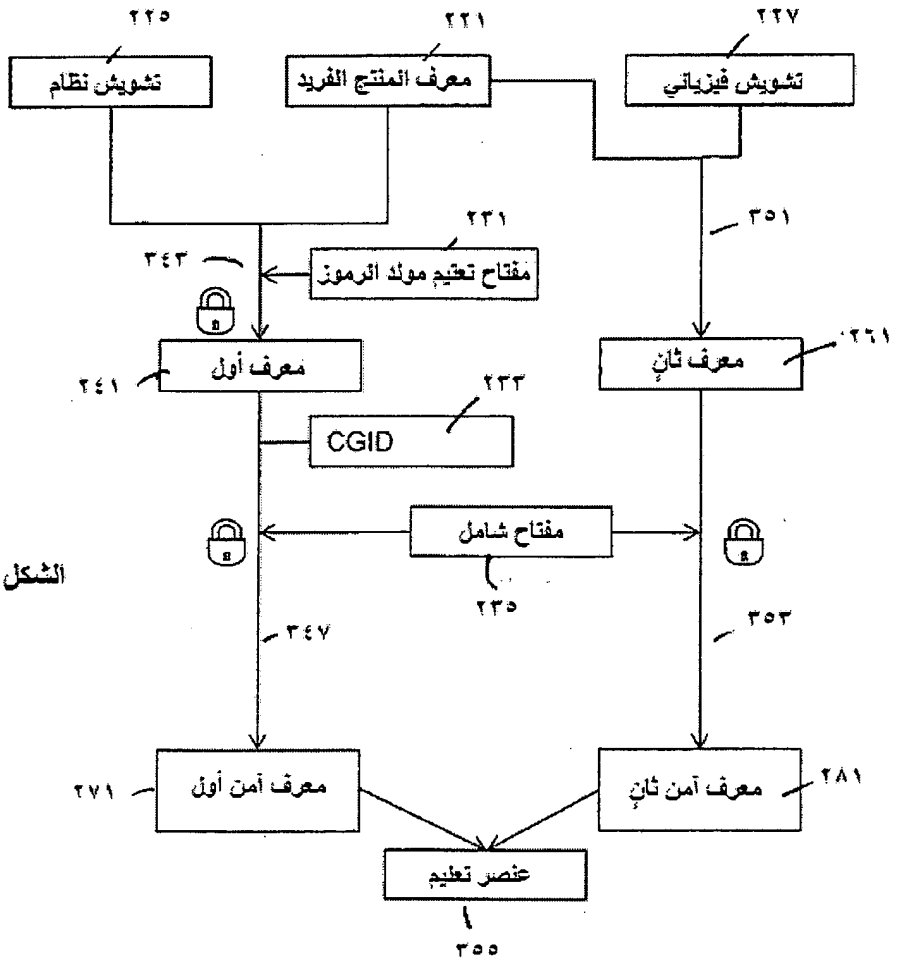

مفتاح استاتيكي
٢٠٩
٣٠١
٢٢٣
مفتاح ديناميكي
٢١٩
مفتاح سري
٢٢٥
تشويش نظام
UPI
٢٢١
٢٢٧
٣٠٥
تشويش فيزيائي
٢٠٧
مفتاح فيزيائي


٢٢٥
تشويش النظام
٢٢١
معرف المنتج الفريد
٣١١
٢٣١
مفتاح تعتيم موك الرموز
٣١٣
معرف اول
٢٢٧
تشويش فيزيائي
٣١٥
٢٣٣
معرف موك الرموز
٢٣٥
مفتاح شامل
٣١٧
معرف آمن
عنصر تعليم
٢٥١
٣١٩

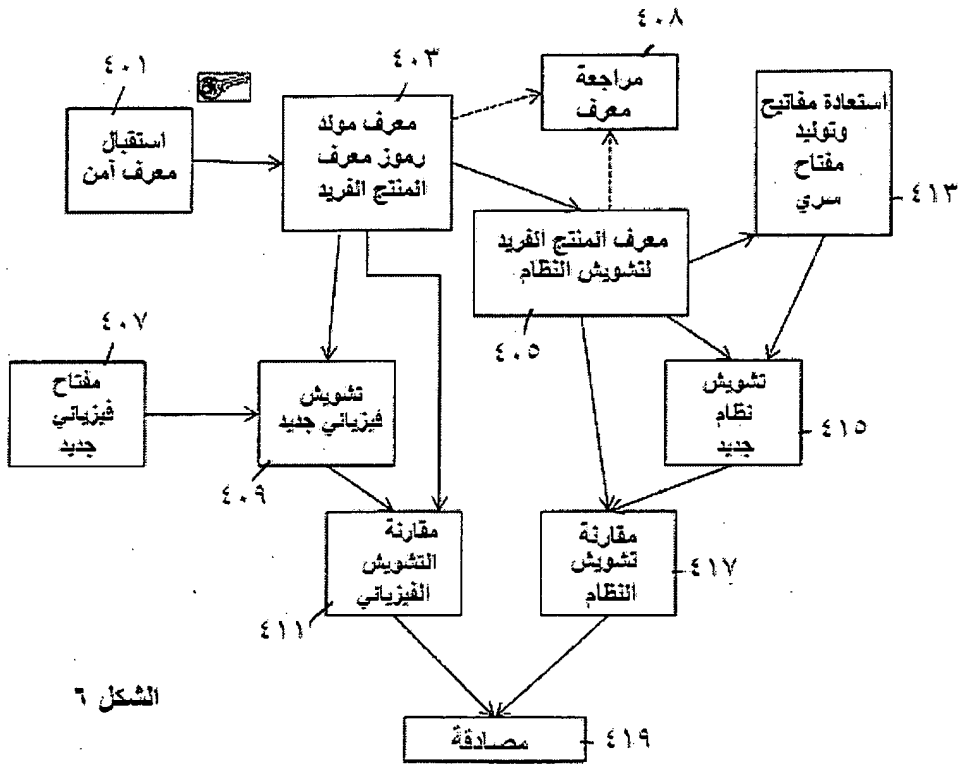
الشكل ٣


٣٢١
استقبال معرف آمن
٣٢٣
تشويش فيزيائي + معرف أول
٣٢٥
تشويش نظام + معرف المنتج الفريد
٣٣٣
استعادة مفاتيح وتوليد مفتاح سري
٣٢٧
مفتاح فيزيائي جديد
٣٢٩
تشويش فيزيائي جديد
٣٣٥
تشويش نظام جديد
٣٣١
مقارنة التشويش الفيزيائي
٣٣٧
مقارنة تشويش النظام
٣٣٩
مصادقة

الشكل ٤


٢٢٥
تشويش نظام
٢٢١
معرف المنتج الفريد
٢٢٧
تشويش فيزيائي
٣٥١
٢٣١
مفتاح تعتيم مولد الرموز
٣٤٣
معرف أول
٢٤١
معرف ثانٍ
٢٦١
٢٣٣
CGID
مفتاح شامل
٢٣٥
٣٤٧
٣٥٣
معرف آمن أول
٢٧١
معرف آمن ثانٍ
٢٨١
عنصر تعليم
٣٥٥

الشكل ٥


٤٠١
استقبال معرف آمن
٤٠٣
معرف مولد رموز معرف المنتج الفريد
٤٠٨
مراجعة معرف
استعادة مفاتيح وتوليد مفتاح سري
٤١٣
معرف المنتج الفريد لتشويش النظام
٤٠٥
٤٠٧
مفتاح فيزيائي جديد
تشويش فيزيائي جديد
٤٠٩
تشويش نظام جديد
٤١٥
مقارنة التشويش الفيزيائي
٤١١
مقارنة تشويش النظام
٤١٧
مصادقة
٤١٩

الشكل ٦

MA 38282B1

ROYAUME DU MAROC
*******
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
*******

OMPIC

المملكة المغربية
---
المكتب المغربي للملكية الصناعية و التجارية
---

# *RAPPORT DE RECHERCHE DEFINITIF AVEC OPINION SUR LA BREVETABILITE*

*Établi conformément à l'article 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13*

| **Renseignements relatifs à la demande** | |
|---|---|
| N° de la demande : 38282 | Date de dépôt : 16/12/2013 |
| Déposant : PHILIP MORRIS PRODUCTS S.A | Date d'entrée en phase nationale : 16/07/2015 |
| Intitulé de l'invention : PROCEDE ET APPAREIL PERMETTANT DE MARQUER DES ARTICLES MANUFACTURES AU MOYEN D'UNE CARACTERISTIQUE PHYSIQUE | |
| **Classement de l'objet de la demande :** CIB : G 09C 5/00, H 04L 9/00 | |

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales

- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité

Partie 2 : Opinion sur la brevetabilité

- ☐ Cadre 3 : Observations à propos de revendications modifiées qui s'étendent au-delà du contenu de la demande telle qu'initialement déposée
- ☒ Cadre 4 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 5 : Défaut d'unité d'invention

| | |
|---|---|
| **Examinateur:** I. Oubiyi | **Date d'établissement du rapport** : 29/12/2016 |
| **Téléphone:** (+212) 5 22 58 64 14 | |

**Partie 1 : Considérations générales**

***Cadre 1 : base du présent rapport***

Les pièces suivantes servent de base à l'établissement du présent rapport :

☒ Demande telle qu'initialement déposée

☐ Demande modifiée suite à la notification du rapport de recherche préliminaire :

☒ Observations à l'appui des revendications maintenues

☐ Observations des tiers suite à la publication de la demande

☐ Réponses du déposant aux observations des tiers

☐ Nouveaux documents constituant des antériorités :

- Suite à la recherche complémentaire *(Couvrant les documents de l'état de la technique qui n'étaient pas disponibles à la date de la recherche préliminaire)*

- Suite à la recherche additionnelle *(couvrant les éléments n'ayant pas fait l'objet de la recherche préliminaire)*

**Partie 2 : Opinion sur la brevetabilité**

***Cadre 4 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle***

| | | |
|---|---|---|
| Nouveauté (N) | Revendications 1-15<br>Revendications aucune | Oui<br>Non |
| Activité inventive (AI) | Revendications 1-15<br>Revendications aucune | Oui<br>Non |
| Possibilité d'application Industrielle (PAI) | Revendications 1-15<br>Revendications aucune | Oui<br>Non |

D1 : WO0143086

1. **Nouveauté (N) :**

Aucun des documents cités ci-dessus ne divulgue l'ensemble des caractéristiques techniques énoncées dans les revendications 1-15. Par conséquent, l'objet desdites revendications est nouveau au sens de l'art. 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2. **Activité inventive (AI) :**

Le document D1 (les références entre parenthèses s'appliquent à ce document) qui est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, divulgue un procédé de marquage d'un article manufacturé (page 4, lignes 1 à 3), comprenant:

- La création d'un identifiant unique de produit pour un article manufacturé (page 4, ligne 13, et page 7, ligne 25);
- La création d'une ou plusieurs clés de chiffrement (page 4, ligne 11);
- La génération d'une clé secrète au moyen de l'identifiant de produit unique et de la ou des clés de chiffrement (page 4, lignes 17 et 18, "code résultant");
- La génération d'une clé des données figurant dans l'image de l'article manufacturé (page 4, lignes 14 à 16, voir aussi les lignes 19 à 36 sur la même page);
- La génération d'un identifiant sécurisé dérivé de la clé secrète et de la clé liée au données figurant dans l'image ou l'incorporation de celle-ci (page 4, ligne 18) ;
- Le marquage de l'article par l'insertion de l'identifiant sécurisé sur l'article (marquage de l'article) (page 4, ligne 18).

Par conséquent, l'objet de la revendication 1 diffère de D1 en ce que l'identifiant sécurisé est dérivé à la fois de la clé secrète et la clé physique qui sont établies séparément. Aussi la clé physique est basée sur une propriété physique mesurée de l'article manufacturé.

L'effet technique apporté par cette différence réside dans le fait de fournir un processus d'authentification à deux niveaux, le premier sur la base des informations communiquées par le fabricant (clé secrète) et l'autre sur la base de l'objet manufacturé (clé physique).

Le problème que la présente invention se propose de résoudre peut donc être considéré comme fournir un procédé de marquage permettant la détection du clonage d'identifiants sur des articles authentiques, mais ne nécessite pas le stockage à grande échelle des codes d'authentification.

Par ailleurs, aucun enseignement n'a été trouvé dans l'état de la technique le plus proche, pris seul ou en combinaison avec l'art antérieur qui aurait incité la personne du métier à résoudre le problème posé. Par conséquent, la solution à ce problème proposée dans la revendication 1 implique une activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13 concernant l'activité inventive.

Le même raisonnement s'applique à l'objet de revendication indépendante 12 qui satisfait donc également, en tant que telle, aux exigences de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13 concernant l'activité inventive.

Les revendications dépendantes 2 à 11 et 13 à 15 dépendent d'une ou de plusieurs revendications indépendantes dont l'objet est considéré inventif, comme indiqué auparavant, et elles satisfont donc également, en tant que telles, aux exigences de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13 concernant l'activité inventive.

3. **Possibilité d'application industrielle (PAI) :**

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.