(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 743 893 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
18.06.2014 Bulletin 2014/25

(51) Int Cl.:
G07D 7/00 *(2006.01)*

(21) Numéro de dépôt: **12306575.7**

(22) Date de dépôt: **12.12.2012**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA ME

(71) Demandeur: **Gemalto SA**
92190 Meudon (FR)

(72) Inventeurs:
- **Akli, Olivier**
  13705 La Ciotat (FR)
- **Varuhaki, Yolanda**
  13705 La Ciotat (FR)

(54) **Procédé de sécurisation d'un document comprenant des informations imprimées et document correspondant**

(57) L'invention concerne notamment un procédé de sécurisation d'un document 10 comportant des informations imprimées, appelées informations de référence, ce procédé consistant à :
- signer la représentation numérique desdites informations de référence par une clé cryptographique pour obtenir des informations signées ;
- constituer un ensemble d'informations incluant les informations signées ;
- convertir l'ensemble d'informations en un premier code 12 lisible par une machine ;
- imprimer le premier code 12 sur le document 10.

FIG.1

EP 2 743 893 A1

Description

[0001] Le domaine de l'invention est celui de la sécurisation de documents comprenant des informations imprimées, cette sécurisation ayant pour objectif de lutter contre la falsification des informations imprimées.

[0002] De nombreux documents (administratifs ou officiels par exemple) comprennent des informations importantes qu'il est souhaitable de protéger contre leur falsification. A titre d'exemple, une carte d'identité, un passeport, un permis de conduire, une carte grise, un chèque, un bulletin de salaire, un relevé bancaire, un diplôme, un acte de naissance, un acte notarié ou un document médical (tel qu'une ordonnance médicale ou une attestation), une quittance d'électricité, comprennent des informations imprimées, appelées par la suite des « informations de référence », qui peuvent être plus ou moins facilement falsifiées par une personne mal intentionnée. Ces informations de référence sont par exemple un nom, un prénom, une date, un numéro, une adresse, une photographie ou le nom d'un médicament.

[0003] La falsification d'une ou de plusieurs de ces informations de référence peut notamment permettre une usurpation d'identité. Dans le cas d'une ordonnance médicale, la modification du nom d'un médicament ou de la quantité de médicaments prescrits peut également avoir des conséquences graves au niveau de la santé. La falsification des informations imprimées sur un diplôme peut également permettre d'accéder illégalement à un emploi.

[0004] Comme mentionné dans le brevet EP-727.316 B1, les moyens utilisés par les falsificateurs sont nombreux et incluent les agents chimiques du type solvant, les moyens de grattage et de gommage, qui visent à supprimer ou effacer certaines informations imprimées sur un document pour les remplacer par d'autres, telles que par exemple, pour un chèque, une somme et/ou le bénéficiaire.

[0005] Afin de déceler sur le document lui-même une tentative de falsification, on peut faire appel à des encres spéciales, telles que des encres magnétiques pour, par exemple, inscrire le code CMC7 (Caractères Magnétiques Codés à 7 bâtonnets) du numéro de chèque sur le chèque lui-même. Cependant, un falsificateur peut se procurer cette encre spéciale et, après avoir supprimé par grattage ou gommage l'ancienne information, peut imprimer un autre code sur le chèque.

[0006] Il est également connu de protéger un document à l'aide de guilloches ou de prévoir un motif de fond complexe et dense. Si ce moyen permet de dissuader en partie et/ou de rendre difficile et fastidieux tout effacement et recopiage du motif de fond, il n'est cependant pas totalement fiable, compte tenu de l'opiniâtreté et la patience de certains falsificateurs.

[0007] Il est connu également de la demande de brevet WO 95/02512 de revêtir la couche support de papier d'une couche de coloration contenant des microcapsules aptes à se briser sous l'effet de la pression lors de l'impression/écriture pour libérer une substance colorante apte à réagir avec un réactif incorporé également dans la couche de coloration. De tels papiers, appelés autocopiants, sont utilisés en liasse comprenant une première feuille de papier ordinaire à titre d'original et une ou plusieurs feuilles additionnelles associées servant de duplicata. Cependant, ce papier est d'une relativement grande fragilité, du fait de l'extrême sensibilité de la couche de coloration, ce qui oblige de prendre de grandes précautions lors des manipulations du papier pour éviter les frottements, créateurs d'inscriptions intempestives.

[0008] Il a également été proposé de signer électroniquement un document, tel qu'un document PDF. Cependant, cette solution ne s'applique qu'à des documents électroniques et pas à des documents imprimés.

[0009] Enfin, il a été proposé de protéger des documents, tels que des passeports, à l'aide d'une puce sécurisée comportant les mêmes informations que celles imprimées. Une comparaison des données lues dans la puce avec celles imprimées permet de détecter une modification des informations imprimées. Cette solution nécessite cependant une puce pour le stockage des informations à protéger (les informations de référence) ainsi qu'un lecteur spécifique.

[0010] La présente invention a notamment pour objectif de remédier à ces inconvénients.

[0011] Plus précisément, un des objectifs de l'invention est de fournir un procédé de sécurisation d'un document comportant des informations de référence, très peu coûteux et sûr, permettant à toute personne de vérifier l'authenticité de ce document.

[0012] Cet objectif, ainsi que d'autres qui apparaîtront par la suite, est atteint grâce à un procédé de sécurisation d'un document comportant des informations imprimées, appelées informations de référence, ce procédé consistant à :

- signer la représentation numérique des informations de référence par une clé cryptographique pour obtenir des informations signées ;
- constituer un ensemble d'informations incluant les informations signées ;
- convertir l'ensemble d'informations en un premier code lisible par une machine ;
- imprimer le premier code sur le document.

[0013] Les informations de référence sont préférentiellement des lettres, des chiffres, une photographie ou une signature manuscrite.

[0014] Dans un mode de mise en oeuvre, la clé cryptographique est une clé secrète.

[0015] Dans un second mode de mise en oeuvre, la clé cryptographique est une clé privée.

[0016] Le document est préférentiellement un passeport, une carte d'identité ou un document imprimé.

[0017] Dans un mode de mise en oeuvre avantageux, le procédé selon l'invention consiste également à imprimer sur le document un deuxième code lisible par une

machine correspondant aux informations de référence.

[0018] Dans un autre mode de mise en oeuvre, complémentaire des précédents, l'invention propose également d'imprimer sur le document un troisième code lisible par une machine comprenant au moins un identifiant de la clé cryptographique.

[0019] Avantageusement, le troisième code comprend la clé publique permettant de déchiffrer le premier code.

[0020] L'invention concerne également un document comportant des informations imprimées, appelées informations de référence, ce document comprenant un premier code lisible par une machine, le premier code comprenant les informations de référence signées par une clé cryptographique.

[0021] D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante d'un mode de mise en oeuvre de l'invention, donné à titre illustratif et non limitatif, et des figures annexées dans lesquelles :

- La figure 1 représente un modèle de permis de conduire comprenant des informations de référence imprimées ainsi qu'un code selon la présente invention ;
- La figure 2 montre schématiquement une mise en oeuvre du procédé selon l'invention.

[0022] La figure 1 représente un modèle d'un permis de conduire comprenant des informations de référence imprimées ainsi qu'un code selon la présente invention.

[0023] Un modèle de permis de conduire, se présentant par exemple sous la forme d'une carte en plastique 10, comprend classiquement la photo 11 de son titulaire, son nom (au point 1), son prénom (au point 2), sa date et lieu de naissance (au point 3), sa date d'obtention du permis (au point 4a), la date de validité du permis (au point 4b), le nom de la ville qui a délivré le permis (au point 4c), le numéro du permis (au point 5) et la signature de son titulaire (au point 6).

[0024] Les informations des points 1 à 5 sont des caractères imprimés, la signature étant une information imprimée. Au moins une partie de ces caractères ou informations imprimés, appelés génériquement informations de référence, sont des informations que l'invention propose de sécuriser contre leur modification, par exemple suite à un vol du permis de conduire.

[0025] A cet effet, en considérant par exemple que l'on veuille sécuriser le nom, le prénom et le numéro du permis (points 1, 2 et 5), l'invention propose de sécuriser ces informations de référence en les signant (en réalité en signant leur représentation numérique) par une clé cryptographique K (clé uniquement en possession de l'émetteur du permis de conduire 10) afin d'obtenir des informations signées IS.

[0026] On aura donc :

(SAMPLE SUSAN B072RRE2155, K) -> IS
avec IS = sig(K, SAMPLE SUSAN B072RRE2155)

[0027] Les informations signées IS sont, dans un premier mode de mise en oeuvre, converties en un premier code lisible par une machine. Ce code est ici un code QR référencé 12. Le code QR est simplement imprimé sur le permis 10 lors de sa fabrication.

[0028] La vérification de l'intégrité du permis 10 (vérification que celui-ci n'a pas été falsifié) peut par exemple s'opérer lors d'un contrôle routier par un agent de police : celui-ci scanne, à l'aide d'un terminal (par exemple à l'aide d'un téléphone mobile, un PDA ou un smartphone) le code QR 12. Une application dédiée installée dans son terminal comprend (ou télécharge, par exemple via Internet, dans un schéma de signature par clé partagée - PKI) la clé de déchiffrement appairée Kd avec la clé K ayant servi à signer les informations de référence. Après déchiffrement, l'agent de police peut visuellement comparer les informations de référence imprimées sur le permis 10 avec celles issues du déchiffrement. Ainsi, si une personne mal intentionnée venait à modifier le nom, le prénom ou le numéro du permis, il n'y aurait pas identité entre les informations de référence imprimées et celles issues du déchiffrement.

[0029] La personne malveillante ne peut pas modifier le code QR 12 puisqu'elle ne dispose pas de la clé de l'organisme ayant fabriqué le permis 10, cette clé étant confidentielle.

[0030] Les informations de référence peuvent être des lettres et/ou des chiffres et/ou encore une photographie.

[0031] En ce qui concerne les clés de signature K et de déchiffrement Kd, elles peuvent être identiques (dans un schéma à clé secrète) mais elles sont de préférence différentes (schéma à clés publiques). En effet, un schéma de signature à clé secrète n'est sûr que si la clé secrète n'est pas révélée. Ceci ne peut être garanti si la clé secrète est présente dans les terminaux des personnes autorisées à effectuer des contrôles d'authenticité de documents. En revanche, si la clé de signature est une clé privée, tout le monde peut déchiffrer le code QR 12 à l'aide de la clé publique associée. Des schémas de diversification de clés sont également possibles.

[0032] L'invention propose également, et ce à titre accessoire, d'imprimer sur le document 10 un deuxième code 13 lisible par une machine correspondant aux informations de référence. Il n'y a dans ce cas pas de signature des informations de référence qui sont simplement converties dans le code 13.

[0033] Enfin, l'invention propose d'imprimer sur le document 10 un troisième code 14 lisible par une machine comprenant au moins un identifiant de la clé cryptographique ayant servi à signer ces informations de référence. L'identifiant est par exemple la version de la clé, ou pourquoi pas, dans un schéma de PKI, la clé de déchiffrement Kd. La personne désirant vérifier que le document 10 n'a pas été falsifié peut alors simplement scanner le code 14 (pour reconstituer la clé publique) avant de scanner le code 12 pour vérifier l'authenticité des informations de référence. Le code 14 peut comprendre la clé de déchiffrement ou un lien vers cette clé de déchif-

frement.

[0034] Lorsqu'un schéma à clé secrète est utilisé, il est possible d'envoyer à l'émetteur du permis 10 les informations signées afin que celui-ci les déchiffre et les retransmette à la personne qui effectue le contrôle du document 10. Le code 14 comprend alors un simple lien (adresse Internet) vers un site de l'émetteur du document 10.

[0035] Dans un autre mode de mise en oeuvre de l'invention, le code imprimé est obtenu à partir d'informations incluant les informations signées. Cela signifie que les informations signées sont concaténées avec d'autres informations, par exemple avec les données permettant d'identifier la clé de signature utilisée ou un lien vers cette clé de signature (celle permettant d'obtenir le code 14 dans la figure 1) et/ou avec les informations imprimées (informations de référence ou toutes les informations imprimées).

[0036] Il est également possible de générer autant de codes qu'il y a d'informations de référence.

[0037] Il est également possible de protéger la photographie 11 du détenteur du document 10 par le mécanisme exposé ci-dessus, ainsi que la signature (point 6).

[0038] Une signature manuscrite et une photographie peuvent donc également constituer des informations de référence, l'essentiel étant qu'elles se présentent sous un format numérique (par exemple jpeg ou gif) lors de l'édition du document. Après impression de l'image (photographie et/ou signature), sa représentation numérique est signée (avec ou sans d'autres informations à protéger) et convertie en un code lisible par une machine, ce code étant ensuite imprimé sur le document. On garantit ainsi une impossibilité de falsification (non détectable) d'une photographie ou d'une signature.

[0039] Les codes présentés jusqu'ici sont des codes QR mais tout type de code peut être utilisé (Aztec, Maxicode, Datamatrix, Code One,...), de préférence à deux dimensions, l'important étant que les informations dont on souhaite protéger l'intégrité soient signées par une clé uniquement en possession de l'émetteur du document sur lequel sont imprimées ces informations.

[0040] Le document n'est pas nécessairement un permis de conduire et peut être un passeport, une carte d'identité ou tout document imprimé, par exemple un diplôme, une ordonnance médicale,...

[0041] L'invention permet également de vérifier l'intégrité d'un document transmis par e-mail ou par télécopie, tant que le ou les codes imprimés ne sont pas altérés.

[0042] L'invention concerne également un document comportant des informations de référence, ce document comprenant également un premier code lisible par une machine, le premier code comprenant les informations de référence signées par une clé cryptographique, ce premier code étant obtenu selon le procédé de l'invention.

[0043] La figure 2 montre schématiquement une mise en oeuvre du procédé selon l'invention.

[0044] Les informations de référence à protéger contre leur falsification, notées 20, sont converties par un algorithme 21 en un code 13 (appelé précédemment deuxième code) imprimé sur le document 10. Ici, on garantit également l'intégrité de la signature manuscrite 22 du détenteur du document 10 en signant cette signature manuscrite par la clé cryptographique (secrète ou préférentiellement privée) de l'autorité d'où émane le document 10. Le code résultant est référencé 23 et également imprimé sur le document 10.

[0045] La signature 24 de l'autorité est également utilisée pour signer les informations de référence et la signature manuscrite du détenteur du document 10. Cet ensemble signé est converti pour obtenir le premier code 12 qui est imprimé sur le document 10.

[0046] Enfin, l'identifiant 25 de la signature de l'autorité est converti par l'algorithme 21 pour obtenir le troisième code 14 qui est imprimé sur le document 10.

[0047] L'invention permet de garantir l'intégrité des informations imprimées sur un document, grâce au chiffrement de ces informations et leur codage sous la forme d'un code lisible par une machine. Le procédé est très simple à mettre en oeuvre et la vérification des informations imprimées (nom, date, photographie, signature,...) peut être réalisée à partir de n'importe quel terminal mobile comprenant une application dédiée à la reconnaissance de codes (QR par exemple) et au déchiffrement d'une clé de signature cryptographique.

Revendications

1. Procédé de sécurisation d'un document (10) comportant des informations imprimées, appelées informations de référence, **caractérisé en ce qu'il** consiste à :

   - signer la représentation numérique desdites informations de référence par une clé cryptographique pour obtenir des informations signées ;
   - constituer un ensemble d'informations incluant lesdites informations signées ;
   - convertir ledit ensemble d'informations en un premier code (12) lisible par une machine ;
   - imprimer ledit premier code (12) sur ledit document (10).

2. Procédé selon la revendication 1, **caractérisé en ce que** lesdites informations de référence sont des lettres.

3. Procédé selon la revendication 1, **caractérisé en ce que** lesdites informations de référence sont des chiffres.

4. Procédé selon la revendication 1, **caractérisé en ce que** lesdites informations de référence sont une photographie.

5. Procédé selon la revendication 1, **caractérisé en ce que** lesdites informations de référence sont une signature manuscrite.

6. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce que** ladite clé cryptographique est une clé secrète.

7. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce que** ladite clé cryptographique est une clé privée.

8. Procédé selon l'une des revendications 1 à 7, **caractérisé en ce que** ledit document (10) est un passeport, une carte d'identité ou un document imprimé.

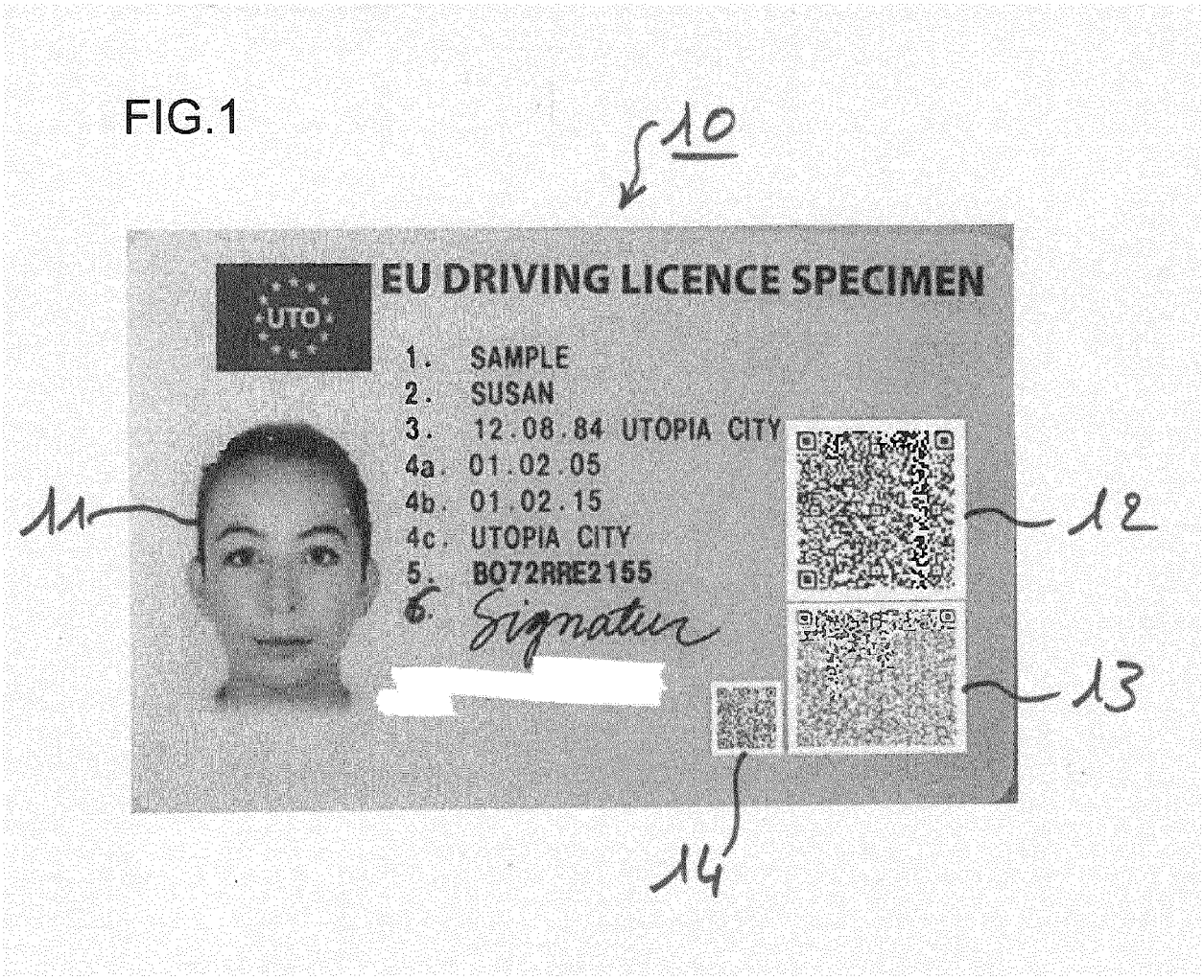
9. Procédé selon l'une des revendications 1 à 8, **caractérisé en ce qu'il** consiste également à imprimer sur ledit document (10) un deuxième code (13) lisible par une machine correspondant à la représentation numérique desdites informations de référence.

10. Procédé selon l'une des revendications 1 à 9, **caractérisé en ce qu'il** consiste également à imprimer sur ledit document un troisième code (14) lisible par une machine comprenant au moins un identifiant de ladite clé cryptographique.

11. Procédé selon la revendication 10, **caractérisé en ce que** ledit troisième code (14) comprend la clé publique permettant de déchiffrer ledit premier code (12).

12. Document (10) comportant des informations imprimées, appelées informations de référence, **caractérisé en ce qu'il** comprend un premier code (12) lisible par une machine, ledit premier code (12) comprenant la représentation numérique desdites informations de référence signées par une clé cryptographique.

FIG.1


10
EU DRIVING LICENCE SPECIMEN
UTO
1. SAMPLE
2. SUSAN
3. 12.08.84 UTOPIA CITY
4a. 01.02.05
4b. 01.02.15
4c. UTOPIA CITY
5. BO72RRE2155
6. Signature
11
12
13
14

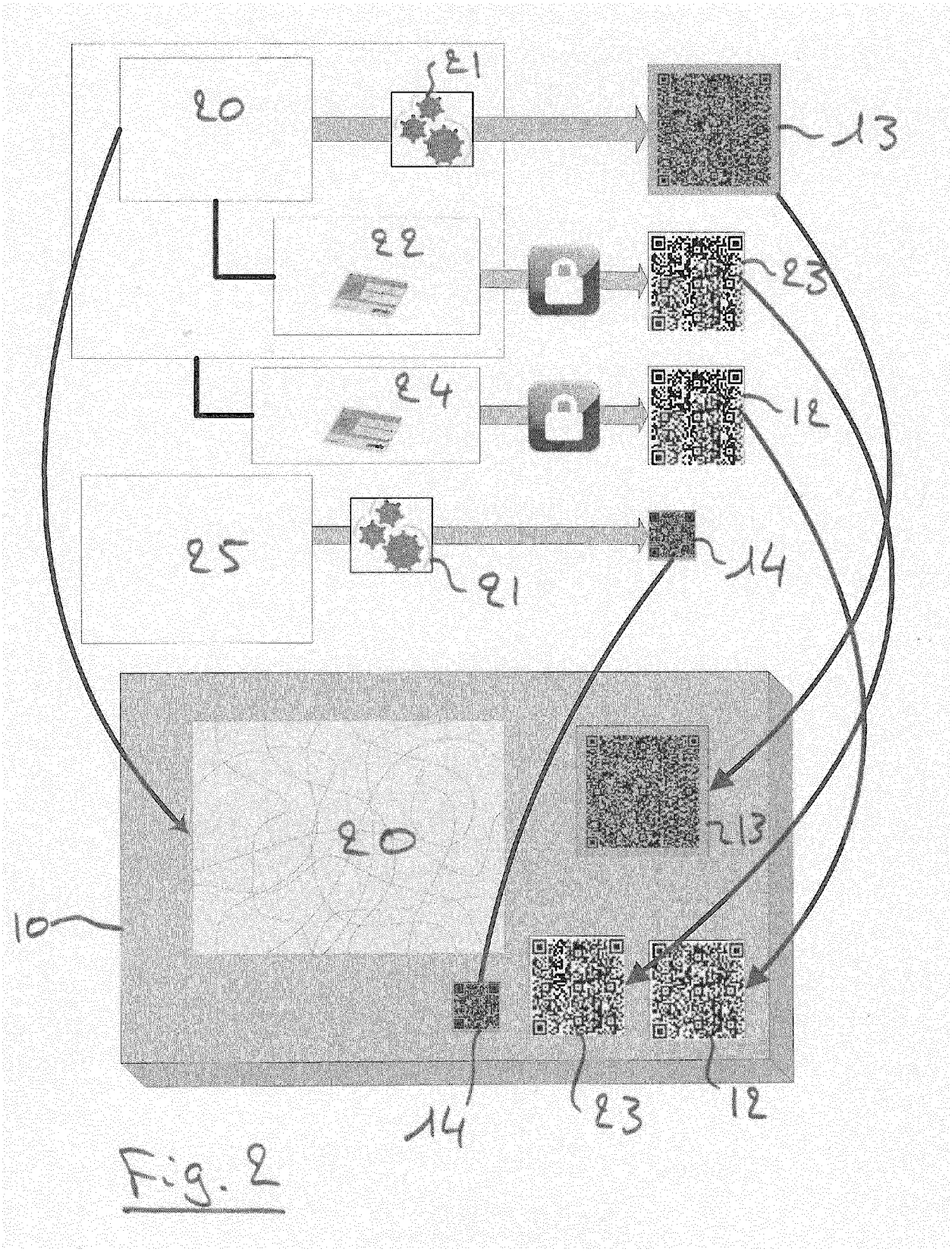


Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 12 30 6575

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X Y	US 3 990 558 A (EHRAT KURT) 9 novembre 1976 (1976-11-09) * colonne 1, ligne 31 - ligne 56 * * colonne 2, ligne 15 - ligne 36 * * colonne 2, ligne 52 - colonne 3, ligne 48 * * figure 1 * -----	1-9,12 10,11	INV. G07D7/00
X	EP 0 154 972 A2 (PITNEY BOWES INC [US]) 18 septembre 1985 (1985-09-18) * page 2, ligne 1 - ligne 17 * * page 2, ligne 26 - page 3, ligne 13 * * figure 1 * -----	1-3,8,12	
X	US 5 426 700 A (BERSON WILLIAM [US]) 20 juin 1995 (1995-06-20) * colonne 3, ligne 15 - colonne 4, ligne 4 * * colonne 5, ligne 10 - ligne 42 * -----	1-9,12	
X	EP 0 889 448 A2 (PITNEY BOWES INC [US]) 7 janvier 1999 (1999-01-07) * colonne 2, ligne 15 - ligne 55 * * colonne 3, ligne 9 - ligne 54 * * figure 1 * -----	1-3,6,7,12	DOMAINES TECHNIQUES RECHERCHES (IPC) G07D
Y	US 6 212 504 B1 (HAYOSH THOMAS DAVID [US]) 3 avril 2001 (2001-04-03) * colonne 11, ligne 10 - ligne 39 * * colonne 13, ligne 46 - ligne 67 * * figures 1-3,8 * -----	10,11	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	18 mars 2013	Paraf, Edouard

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1 EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 12 30 6575

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

18-03-2013

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 3990558 A	09-11-1976	CH 585439 A5	28-02-1977
		DE 2350418 A1	10-04-1975
		FR 2246913 A1	02-05-1975
		GB 1484042 A	24-08-1977
		JP S5067048 A	05-06-1975
		US 3990558 A	09-11-1976
EP 0154972 A2	18-09-1985	CA 1246226 A1	06-12-1988
		DE 3583249 D1	25-07-1991
		EP 0154972 A2	18-09-1985
		JP 2557041 B2	27-11-1996
		JP S60252994 A	13-12-1985
		US 4649266 A	10-03-1987
US 5426700 A	20-06-1995	CA 2130531 A1	24-02-1995
		DE 69416360 D1	18-03-1999
		DE 69416360 T2	24-06-1999
		EP 0640946 A1	01-03-1995
		US 5426700 A	20-06-1995
EP 0889448 A2	07-01-1999	CA 2242671 A1	01-01-1999
		DE 69819243 D1	04-12-2003
		DE 69819243 T2	29-07-2004
		EP 0889448 A2	07-01-1999
		US 6904525 B1	07-06-2005
US 6212504 B1	03-04-2001	US 6212504 B1	03-04-2001
		US 6611598 B1	26-08-2003

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- EP 727316 B1 **[0004]**
- WO 9502512 A **[0007]**