

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(43) Date de la publication internationale
04 janvier 2018 (04.01.2018)

WIPO | PCT

(10) Numéro de publication internationale
WO 2018/002491 A1

(51) Classification internationale des brevets :
G06F 21/64 (2013.01) G06F 21/34 (2013.01)

de la Suisse Normande, 61100 SAINT GEORGES DES
GROSEILLERS (FR).

(21) Numéro de la demande internationale :
PCT/FR2017/051682

(74) Mandataire : ORANGE IMT/OLPS/IPL/PATENTS ;
AMONOU Isabelle, ORANGE GARDENS -, 44 avenue de
la République - CS 50010, 92326 CHATILLON CEDEX
(FR).

(22) Date de dépôt international :
23 juin 2017 (23.06.2017)

(25) Langue de dépôt : français

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AO,
AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA,
CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,
HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR,
KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(26) Langue de publication : français

(30) Données relatives à la priorité :
1655945 27 juin 2016 (27.06.2016) FR

(71) Déposant : ORANGE [FR/FR] ; 78 rue Olivier de Serres,
75015 PARIS (FR).

(72) Inventeurs : REMERY, Patrick ; 43 rue de Cornouailles,
14000 CAEN (FR). TRAORE, Jacques ; 23 avenue

(54) Title: SECURING OF ELECTRONIC DOCUMENTS

(54) Titre : SÉCURISATION DE DOCUMENTS ÉLECTRONIQUES

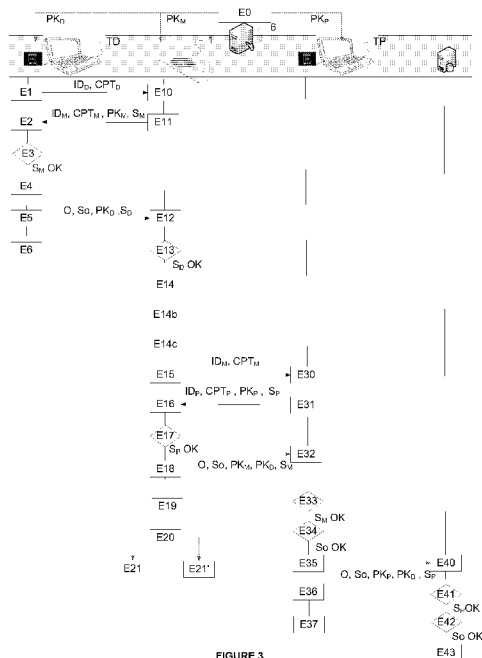


FIGURE 3

(57) Abstract: The invention applies to a portable object (1) for host-
ing an electronic document (O) in order to access a service. The elec-
tronic document is generated by a generating terminal (TD) and must be
processed by a processing terminal (TP). The portable object comprises
the following modules: - reception of an electronic document (O) and
of a signature (So); - obtaining (CLF) of the public key (PKD) of the
generating terminal (TD), and of a signature (SD) of said generating ter-
minal (TD); - obtaining (CLF) of the public key (PKP) of the processing
terminal (TP) and of a signature (SP) of said processing terminal (TP);
- authentication of the generating terminal; - authentication of the pro-
cessing terminal; - generation of a message - sending of said message
to the processing terminal - a module able to modify a datum relating
to said electronic document so as to prevent the document from being
sent again.

(57) Abrégé : L'invention s'applique à un objet portable (1) pour
l'hébergement d'un document électronique (O) pour accéder à un service.
Le document électronique est généré par un terminal de génération (TD)
et doit être traité par un terminal de traitement (TP). L'objet portable
comporte les modules suivants : - réception d'un document électronique
(O) et d'une signature (So); - obtention (CLF) de la clé publique (PKD)
du terminal de génération (TD), et d'une signature (SD) dudit terminal
de génération (TD); - obtention (CLF) de la clé publique (PKP) du ter-
minal de traitement (TP) et d'une signature (SP) dudit terminal de trai-
tement (TP); - authentification du terminal de génération; - authentifica-
tion du terminal de traitement; - génération d'un message - émission dudit
message vers le terminal de traitement - un module apte à modifier une
donnée relative audit document électronique afin de prévenir une autre
émission.



(84) États désignés (*sauf indication contraire, pour tout titre de protection régionale disponible*) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— avec rapport de recherche internationale (Art. 21(3))

Sécurisation de documents électroniques.

Domaine technique

L'invention se rapporte au domaine de la sécurisation de documents électroniques.

- 5 L'invention s'applique en particulier au domaine des prescriptions médicales électroniques dématérialisées, aussi appelées *e.prescriptions*.

L'invention s'applique à tout terminal portable équipé d'un microcontrôleur et d'une mémoire sécurisée. L'invention s'applique tout particulièrement à des terminaux portables équipés de ressources physiques et
10 logicielles incluant un module de communication en champ proche apte à communiquer avec des terminaux externes de lecture et à héberger des prescriptions médicales électroniques dématérialisées.

Etat de la technique

- Actuellement, une ordonnance médicale est un document géré sur un
15 support papier, incluant un certain nombre d'informations liées au patient ainsi qu'au traitement qui lui est proposé (prescriptions de médicaments et dispositifs médicaux, prescriptions d'actes de soins ou de rééducation, prescriptions de biologie, prescriptions de radiologie, etc.).

- Récemment, il a été proposé un certain nombre de solutions visant à
20 dématérialiser l'ordonnance médicale sous forme de document électronique, appelée dans la suite *e.prescription*.

- Dans ce contexte, des projets d'*e.prescriptions* centralisées sur une base de données sont en cours d'étude. Un tel système est décrit par exemple dans la note d'orientation établie par les Conseils Nationaux des Ordres des
25 Professions de santé, réunis en France au sein d'un Comité de Liaison Inter Ordres (CLIO Santé), disponible à l'adresse https://www.conseil-national.medecin.fr/sites/default/files/Prescription_electronique.pdf. Dans un tel système, l'*e.prescription* établie par le praticien est transmise et rangée dans une

base de données accessible de tout endroit du territoire acceptant les *e.prescriptions*. Depuis cette base, l'*e.prescription* est accessible aux professionnels de santé (pharmaciens, kinésithérapeutes, etc.) impliqués dans la démarche. Le professionnel de santé peut consulter la base de données à l'aide
5 de sa carte professionnelle de santé et de la carte de santé du patient.

Une telle gestion centralisée des *e.prescriptions* comporte cependant un certain nombre d'inconvénients, puisque la base de données pour gérer l'ensemble des *e.prescriptions* est complexe, volumineuse, nécessitant des investissements importants de la part des organismes de santé. De surcroît la
10 base de données centralisée peut-être inaccessible au moment où le patient se présente au professionnel de santé.

Plus récemment ont donc été proposés des systèmes décentralisés. Par exemple, le brevet US2003/0121972 propose un système de *e.prescriptions* dématérialisées sur un support électronique du patient. Dans ce système, le
15 praticien (l'hôpital) inscrit l'ordonnance dématérialisée dans le support électronique, de préférence une carte sécurisée. La carte électronique est lue ultérieurement par le professionnel de santé lorsque le patient souhaite voir délivrer son ordonnance. Un serveur centralisé reçoit les informations concernant l'*e.prescription* et sa délivrance par le pharmacien.

20 Cependant, ce système n'offre aucune protection contre la duplication éventuelle ou une attaque par « rejeu » de l'*e.prescription*. On rappelle qu'une attaque par rejeu (en anglais, « replay attack ») est une forme d'attaque sur un réseau de télécommunications, dans laquelle une transmission de données est frauduleusement répétée par une tierce partie interceptant les paquets de
25 données sur la ligne. Un tel système n'est donc pas fiable. Dans le contexte de l'ordonnance électronique elle peut notamment aboutir à une réplique de l'*e.prescription* (qui pourra être utilisée plusieurs fois). En effet, si une personne tierce a subtilisé soit le support électronique, soit l'application logicielle et l'ordonnance, il peut se présenter dans une ou plusieurs pharmacies pour
30 bénéficier de la *e.prescription*.

L'invention offre une solution ne présentant pas les inconvénients de l'état de la technique.

L'invention

L'invention sera mieux comprise à la lecture de la description qui suit,
5 donnée à titre d'exemple et faite en référence aux dessins annexés.

A cet effet, selon un aspect fonctionnel, l'invention a pour objet un procédé d'hébergement d'un document électronique sur un objet portable sécurisé pour accéder à un service, ledit document électronique ayant été généré par un terminal de génération et devant être traité par un terminal de traitement,
10 le procédé comportant les étapes suivantes dans l'objet :

- une étape de réception d'un document électronique et d'une signature dudit document électronique ;
- une étape d'obtention de la clé publique du terminal de génération complémentaire d'une clef privée du terminal de génération, et d'une
15 signature dudit terminal de génération ;
- une étape d'obtention de la clé publique du terminal de traitement complémentaire d'une clef privée du terminal de traitement et d'une signature dudit terminal de traitement ;
- une étape d'authentification du terminal de génération à l'aide de ladite
20 clef publique du terminal de génération ;
- une étape d'authentification du terminal de traitement à l'aide de ladite clef publique du terminal de traitement ;
- si les deux étapes d'authentification sont réussies :
 - une étape de génération d'un message comportant au moins :
25
 - le document électronique et sa signature ;
 - La clé publique du terminal de génération ;
 - La clé publique de l'objet complémentaire d'une clef privée de l'objet ;
 - une signature signée par la clé privée de l'objet ;
- une étape d'émission dudit message vers le terminal de traitement.
30

- ~ une étape de modification d'une donnée relative audit document électronique afin de prévenir une autre émission dudit document.

Par « document électronique », on entend tout document dématérialisé contenant des données électroniques d'un utilisateur, par exemple une
5 *e.prescription*.

Par « objet portable », on entend un objet qui peut être porté par un utilisateur, par exemple un bracelet, ou une carte électronique, ou un ordinateur portable, etc. Par objet portable « sécurisé » on entend un tel objet équipé d'un élément de sécurité apte à générer des signatures électroniques, par exemple
10 une carte à puce, ou une carte SIM, ou une zone mémoire dédiée d'un processeur de l'objet.

Par « donnée relative audit document électronique », on entend tout type de donnée dont une modification empêche l'objet portable, ultérieurement à sa modification, de transmettre une nouvelle fois le document.

15 Ainsi, l'invention offre l'avantage d'un procédé sécurisé de bout en bout pour la manipulation d'un document électronique sur un support électronique, par exemple une *e.prescription*. Un tel document est généré sur un terminal de génération, typiquement celui d'un praticien, puis transmis à l'objet par un protocole sécurisé basé sur une méthode cryptographique, puis transmis
20 ultérieurement de l'objet vers un terminal de traitement selon un autre protocole également sécurisé. L'échange est donc sécurisé de bout en bout. De surcroît, avantageusement, la modification d'une donnée liée au document après une première émission de celui-ci empêche sa réémission. Il reste ainsi possible de lire dans l'objet les informations transmises (à condition qu'elles n'aient pas été
25 effacées) mais pas de rejouer le protocole entre le patient (l'objet portable) et le praticien relativement au même document.

Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est en outre caractérisé en ce que l'étape de modification d'une donnée est une étape de modification d'une variable booléenne, dite
30 variable de réémission, dont l'état est représentatif de l'émission dudit document

Par variable booléenne, on entend une variable qui prend deux états distincts. Avantageusement selon ce mode de réalisation, la variable change d'état après la transmission du message. Une évaluation systématique de cette variable avant toute transmission permet de détecter un éventuel changement d'état et d'interdire la réémission du document. Cette interdiction est importante car elle évite que le document soit émis et utilisé plusieurs fois, ce qui pourrait être particulièrement gênant dans le cas d'un document sensible comme une *e.prescription*. De plus, ce changement d'état, s'il est correctement interprété, peut permettre au système de l'objet de libérer la mémoire relative au document et de faire ainsi de la place pour mémoriser d'autres documents.

Selon un deuxième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre alternativement avec le précédent, un procédé tel que décrit plus haut est en outre caractérisé en ce que l'étape de modification d'une donnée est une étape d'effacement du document électronique dans la mémoire de l'objet portable.

Ce mode de mise en œuvre de l'invention permet d'interdire simplement la réémission du document. Une fois le document effacé, tout calcul d'une nouvelle signature mènera à un résultat incorrect et empêchera automatiquement la réémission du document.

Selon encore un troisième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre alternativement ou cumulativement avec les précédents, un procédé tel que décrit plus haut est en outre caractérisé en ce que l'étape d'authentification du terminal de génération est suivie d'une étape de modification d'une variable booléenne, dite variable de réception, dont l'état est représentatif de la réception dudit document.

Un tel mode de mise en œuvre permet de savoir que le document (*e.prescription*) a effectivement été reçue sur l'objet portable et peut donc être traité. Ceci permet à l'utilisateur de vérifier que l'*e.prescription* est disponible et qu'il peut en bénéficier, c'est-à-dire la soumettre à un terminal de traitement

selon l'invention. Avantageusement selon ce mode, on peut de plus éviter de recevoir deux fois la même prescription.

Selon encore un quatrième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre alternativement ou cumulativement avec les précédents, un procédé tel que décrit plus haut est en outre caractérisé en ce qu'il comporte en outre une étape d'annulation du document .

Un tel mode de mise en œuvre permet à l'utilisateur d'annuler l'*e.prescription* s'il n'en a plus besoin, par exemple parce que le prescripteur souhaite modifier sa prescription. Avantageusement, on évite de surcharger la mémoire de l'objet portable, et d'émettre accidentellement une prescription inutile. L'objet portable peut ainsi détecter que l'*e.prescription* a été annulée, et peut avantageusement procéder à sa suppression ou à son écrasement, libérant ainsi de la mémoire sur l'objet portable ; il ne sera plus possible de calculer une signature valide sur le document, ni donc de l'émettre.

Selon encore un cinquième mode de mise en œuvre particulier de l'invention, qui pourra être mis en œuvre alternativement ou cumulativement avec les précédents, un procédé tel que décrit plus haut est en outre caractérisé en ce que l'objet comporte un compteur du nombre de présentations de documents électroniques, en ce que la signature signée par la clé privée de l'objet est fonction de ce compteur, et en ce qu'il comporte une étape de modification dudit compteur après chaque étape de signature

Avantageusement selon ce mode de réalisation, l'incrémentation du compteur permet de générer une signature différente. Le « rejeu » du document sera donc détectable et pourra être aisément évité.

Selon un aspect matériel, l'invention concerne également un objet portable pour l'hébergement d'un document électronique pour accéder à un service, ledit document électronique ayant été généré par un terminal de génération et devant être traité par un terminal de traitement, l'objet portable comportant :

- un module de réception d'un document électronique et d'une signature dudit document électronique ;
- un module d'obtention de la clé publique du terminal de génération complémentaire d'une clef privée du terminal de génération, et d'une signature dudit terminal de génération ;
- un module d'obtention de la clé publique du terminal de traitement complémentaire d'une clef privée (SK_p) du terminal de traitement et d'une signature dudit terminal de traitement ;
- un module d'authentification du terminal de génération à l'aide de ladite clef publique du terminal de génération ;
- un module d'authentification du terminal de traitement à l'aide de ladite clef publique du terminal de traitement ;
- un module de génération d'un message comportant au moins :
 - le document électronique et sa signature ;
 - La clé publique du terminal de génération ;
 - La clé publique de l'objet complémentaire d'une clef privée de l'objet ;
 - une signature signée par la clé privée de l'objet ;
- un module d'émission dudit message vers le terminal de traitement
- un module apte à modifier une donnée relative audit document électronique afin de prévenir une autre émission dudit document.

Selon un autre aspect matériel, l'invention concerne également un objet portable sécurisé tel que décrit ci-dessus, caractérisé en ce que le module d'obtention est un module de communication en champ proche.

Avantageusement selon ce mode de réalisation, la communication en champ proche permet de recevoir le document de manière très simple, en approchant l'objet portable d'un lecteur en champ proche, par exemple de type NFC, installé par exemple sur le terminal du praticien. La communication en champ proche, outre sa simplicité, permet d'assurer une sécurité intrinsèque à

l'échange puisque la portée d'un tel mode de communication est réduite à quelques centimètres.

Selon un autre aspect matériel, l'invention concerne également un objet portable sécurisé tel que décrit ci-dessus, caractérisé en ce que le module de transmission est un module de communication en champ proche

Selon un autre aspect matériel, l'invention concerne également un objet portable sécurisé tel que décrit ci-dessus, caractérisé en ce que le module d'authentification est une carte électronique d'abonné.

Selon un autre aspect logiciel, l'invention concerne également un procédé de traitement pour transmettre un document électronique d'un terminal de traitement vers un serveur de traitement, ledit document électronique provenant d'un terminal de génération et étant stocké sur un objet portable, le procédé de traitement comportant les étapes suivantes sur le terminal de traitement :

- 15 - une étape de réception d'un document électronique et d'une signature dudit document électronique ;
- une étape d'obtention de la clé publique complémentaire d'une clef privée de l'objet portable, et d'une signature dudit objet portable ;
- une étape d'obtention de la clé publique du terminal de génération ;
- 20 - une étape d'authentification de l'objet portable à l'aide de ladite clef publique de l'objet ;
- une étape d'authentification du terminal de génération à l'aide de ladite clef publique du terminal de génération;
- si les deux étapes d'authentification sont réussies :
 - 25 • une étape de génération d'un message comportant au moins :
 - le document électronique et sa signature ;
 - La clé publique du terminal de génération ;
 - La clé publique du terminal de traitement ;
 - une signature signée par la clé privée du terminal de
- 30 traitement ;

- une étape de transmission dudit message vers un serveur de traitement des documents électroniques.

Selon un autre aspect logiciel, l'invention concerne également un procédé de gestion d'un document électronique hébergé sur un objet portable
5 sécurisé pour accéder à un service, ledit document électronique ayant été généré par un terminal de génération et devant être traité par un terminal de traitement et stocké sur un serveur de gestion, le procédé comportant les étapes suivantes sur le serveur de gestion :

- réception d'un message en provenance du serveur de traitement, ledit
10 message comprenant :
 - le document électronique et sa signature ;
 - La clé publique du terminal de génération ;
 - La clé publique du terminal de traitement ;
 - une signature signée par la clé privée du terminal de
15 traitement ;
- authentification du terminal de traitement à l'aide de ladite clef publique du terminal de traitement ;
- authentification du terminal de génération à l'aide de ladite clef publique du terminal de génération ;
- 20 - si les deux étapes d'authentification sont réussies, une étape de stockage du message sur le serveur de gestion.

Selon un autre mode de réalisation, l'invention concerne également l'un quelconque des procédés décrits ci-dessus, caractérisé en ce que les données électroniques sont des données de prescription médicale dématérialisée.

25 Selon un autre mode de réalisation, l'invention concerne également l'un quelconque des procédés décrits ci-dessus où chacune des clés publiques est certifiée par une même entité de certification.

Selon un autre aspect matériel, l'invention concerne également un programme d'ordinateur apte à être mis en œuvre sur un objet portable tel que
30 défini ci-dessus, le programme comprenant des instructions de code qui, lorsque

le programme est exécuté par un processeur, réalise les étapes du procédé d'hébergement.

Ce programme d'ordinateur présente des caractéristiques et avantages analogues à ceux décrits précédemment en relation avec le procédé d'hébergement. Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

Selon encore un autre aspect matériel, l'invention a trait à un support d'enregistrement lisible par un processeur de données sur lequel est enregistré un programme comprenant des instructions de code de programme pour l'exécution des étapes du procédé défini ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur. D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet. Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

25

L'invention sera mieux comprise à la lecture de la description qui suit, donnée à titre d'exemple et faite en référence aux dessins annexés.

Les figures:

La figure 1 représente un système permettant de mettre en œuvre la gestion d'une *e.prescription* selon l'invention.

La figure 2 représente une architecture matérielle d'un dispositif de stockage d'une *e.prescription* selon un mode de réalisation de l'invention.

- 5 La figure 3 représente un organigramme illustrant les différentes étapes d'un procédé dans un système selon deux modes de réalisation de l'invention.

Description détaillée d'un exemple de réalisation illustrant l'invention

La figure 1 représente un système permettant de mettre en œuvre la gestion d'une *e.prescription* selon l'invention sur un objet portable (1).

- 10 L'architecture proposée ici fait intervenir quatre acteurs :

- le patient (ou Malade noté M) propriétaire de l'objet portable (1) destiné au stockage des *e.prescriptions* ; l'objet (1) est selon cet exemple un bracelet très simple et peu coûteux à porter au poignet, portant les services de l'utilisateur, incluant dans cet exemple le logiciel de gestion des *e.prescriptions* dématérialisées ainsi que les *e.prescriptions* elles-mêmes. L'objet portable (1) pourrait prendre une toute autre forme. Sa seule interface de communication obligatoire est une interface pour établir une communication locale, par exemple de type sans contact NFC (Near Field Communication), ou filaire série USB (Universal Serial Bus), pour pouvoir dialoguer avec les terminaux (TD, TP) du praticien et du professionnel de santé. Toute autre interface de communication permettant d'établir une communication point à point entre l'objet portable et le terminal pourrait être envisagée. Dans la suite, on considère qu'il s'agit d'une interface sans contact de type NFC. Dans ce contexte, le bracelet peut être utilisé comme une carte sans contact face à ces terminaux équipés de lecteurs NFC (2,4). Il comprend typiquement une antenne, un contrôleur NFC et un élément de sécurité (SE) de type carte à puce, par exemple une carte SIM, pour le stockage des *e.prescriptions* et des données secrètes de l'utilisateur. Il peut comporter un module de communication avec le réseau mobile ou un quelconque autre réseau de communication, par exemple Internet. Le chargement d'une

application pour la gestion des données et des données secrètes associées dans le bracelet se fait par exemple via ce mode de communication. L'objet peut aussi comporter, optionnellement, un afficheur et un clavier. Le patient peut alors lire les données de l'*e.prescription* sur l'afficheur du support électronique, ou à partir d'un lecteur NFC connecté à son terminal et possédant un afficheur. Il peut 5 entrer un code secret via le clavier. Un code secret ou toute autre empreinte biologique peut en effet être requis pour lire l'*e.prescription*.

- Le praticien qui délivre les *e.prescriptions* (ou Docteur, noté D dans la suite), dont le terminal (TD) est constitué ici d'un ordinateur (3) relié à un lecteur 10 sans contact (2) ; on rappelle qu'une ordonnance est un document électronique, ou *e.prescription*, incluant un certain nombre d'informations liées au patient ainsi qu'au traitement qui lui est proposé (prescriptions de médicaments et dispositifs médicaux, prescriptions d'actes de soins ou de rééducation, prescriptions de biologie, de radiologie, etc.) Le praticien peut, après avoir saisi l'*e.prescription*, 15 transmettre à l'aide du lecteur de proximité (2) connecté à son terminal de saisie les données au support électronique sécurisé (1) du patient selon un protocole sécurisé conforme aux normes d'échanges sécurisés garantissant l'intégralité et la confidentialité des données, comme il sera décrit plus en détails par la suite. Par lecteur de proximité, on entend un lecteur local, qui se trouve directement 20 relié au terminal de traitement du praticien ; un tel lecteur peut être notamment de type sans contact, ou avec contact via une liaison USB, etc.

- Le professionnel de santé (pharmacien, kinésithérapeute, etc.), noté P ; lorsqu'il souhaite le traitement de l'*e.prescription*, le patient présente son support électronique au professionnel de santé, celui-ci récupère les données de 25 l'*e.prescription* à partir d'un lecteur adapté, selon un protocole sécurisé conforme aux normes garantissant l'intégralité et la confidentialité. Selon cet exemple, le professionnel (P) est équipé d'un terminal (TP) constitué d'un ordinateur (5) relié à un lecteur sans contact (4).

- L'organisme de santé représenté par le serveur 7 ; le serveur 7 est par 30 exemple un serveur connecté à un réseau Internet (8). Le professionnel de santé

transmet l'*e.prescription* à l'organisme de santé par tout moyen, selon un protocole sécurisé.

De plus, le système selon ce mode de réalisation comporte une autorité de certification (6) mandatée par l'organisme de santé. Les quatre acteurs susceptibles d'émettre ou recevoir une *e.prescription* disposent d'un système à
5 clés publiques contenant une clé privée Si et une clé publique Pi. Chacune des clés publiques est certifiée par l'autorité de certification (6) et délivrée aux différents acteurs.

10 La figure 2 représente une architecture matérielle d'un dispositif de stockage d'*e.prescriptions* dématérialisées (1) selon un mode de réalisation de l'invention, par exemple un bracelet électronique à porter au poignet de l'utilisateur. Il comporte, selon cet exemple :

-une unité de traitement, ou « CPU » (pour « Central Processing Unit »),
15 destinée à charger des instructions en mémoire, à les exécuter, à effectuer des opérations ; un ensemble de mémoires M, dont une mémoire volatile, ou "RAM" (pour "Random Access Memory") utilisée pour exécuter des instructions de code, stocker des variables, etc. et une mémoire non volatile, de type « ROM » (de l'anglais « Read Only Memory »), ou « EEPROM » (pour « Electronically Erasable
20 Programmable Read Only Memory ») destinée à contenir des données persistantes, utilisées par exemple pour stocker l'application APM en charge notamment de la gestion de l'interface (dans la cas où un afficheur est utilisé) et de la lecture des données.

- un module de communication sans contact (CLF), apte à faire
25 communiquer l'objet avec un équipement proche, dans ce contexte les lecteurs 3 et 4 du praticien et du professionnel de santé, via une liaison sans contact de type NFC. Alternativement, cette liaison peut utiliser une autre technologie de communication de proximité avec ou sans fils (Bluetooth, Zigbee, DECT, USB, etc.)

30 - un module de communication MC apte à communiquer avec un élément de sécurité (SE), via une interface de communication (I1).

- un élément de sécurité (SE) ; dans cet exemple il s'agit d'une carte SIM (pour Subscriber Identification Module) mais on peut envisager sans perte de généralité une carte à mémoire hébergeant un élément sécurisé (SD card, Embedded Secure Controller, etc.) ou encore, avec cependant une sécurité moindre, une zone mémoire spécifique de l'objet comme il est envisageable dans le contexte de la norme HCE (pour Host Card Emulation). L'élément de sécurité SE a pour fonction de mettre en œuvre, dans le cadre de la présente invention, les mécanismes de sécurité (signature, chiffage) qui seront détaillés plus tard à l'appui de la figure 3 ; à cet effet, la carte SIM possède notamment la clé privée (SK_M) qui va lui permettre de chiffrer les données émises en association avec l'*e.prescription*, ainsi que, temporairement, les clés publiques (PK_p , PK_D) des autres entités. L'élément de sécurité SE comporte aussi un module d'émission-réception MC' apte à dialoguer avec le processeur principal (CPU) de l'objet (1) via l'interface de communication I1. Dans ce mode de réalisation de l'invention, l'élément de sécurité SE est une carte SIM et comporte classiquement des mémoires M' de type ROM contenant notamment le système d'exploitation de l'élément de sécurité et des programmes implémentant les mécanismes de sécurité, des mémoires de type EEPROM contenant les clés d'authentification, ainsi que des applications spécifiques aussi appelées *applets* s'exécutant dans une mémoire de type RAM. Sur la figure 2 est représentée l'applet (APS) de sécurité utilisée dans le cadre de la présente invention pour traiter les prescriptions électroniques suivant les protocoles de sécurité qui seront décrits par la suite.

La figure 3 représente un organigramme illustrant les différentes étapes d'un procédé de gestion de prescriptions dématérialisées selon deux modes de réalisation de l'invention.

Lors d'une étape E0 initiale, les clés de sécurité sont distribuées par le serveur (6) aux différents intervenants. Chaque couple de clés consiste en une clé privée SK_i et une clé publique PK_i .

De manière préférentielle, mais non obligatoire, un certificat est calculé pour chaque entité. Classiquement, le certificat sert à authentifier une clé publique en attestant son appartenance (par exemple le certificat C_D atteste que la clé publique PK_D appartient bien au praticien D). Ce certificat peut par exemple
5 être calculé selon la norme X509, une norme de cryptographie asymétrique pour les infrastructures à clés publiques (PKI) définie par l'Union internationale des télécommunications (UIT).

Ainsi, à la suite de cette étape :

- 10 • Le terminal du praticien (D) dispose d'une clé privée notée SK_D , d'une clé publique PK_D et du certificat de PK_D calculé par l'autorité de certification ;
- L'objet du patient (M) dispose d'une clé privée notée SK_M , d'une clé publique PK_M et du certificat de PK_M calculé par l'autorité de certification ;
- 15 • Le terminal du professionnel de santé (P) dispose d'une clé privée notée SK_P , d'une clé publique PK_P et du certificat de PK_P calculé par l'autorité de certification ;

Le serveur appartient à l'organisme d'assurance de santé et détient les clés de cet organisme et celles permettant de vérifier les signatures qu'il reçoit à
20 chaque transmission d'ordonnance (professionnels de santé).

Chaque entité dispose par ailleurs d'un identifiant (Id_i) et d'un compteur (CPT_i) qui lui sont propres, notées respectivement : ID_D , CPT_D pour le praticien ; ID_M , CPT_M pour le patient ; ID_P , CPT_P pour le professionnel de santé ; ID_S , CPT_S pour l'organisme d'assurance de santé. Ces compteurs ont pour but de rendre
25 impossible l'utilisation de signatures S déjà émises par l'un des intervenants (donc les rejeux).

On suppose par ailleurs que le bracelet a été correctement initialisé lors d'étapes préalables, notamment via :

- une étape d'installation de l'application (APM, APS). L'application peut être installée pendant l'étape de fabrication du bracelet puis personnalisée lors de sa commercialisation, à partir d'un dispositif en ligne de l'organisme de santé ; alternativement, l'application peut être téléchargée ou mise à jour après la vente du bracelet (par exemple sur le serveur de l'organisme de santé ou sur un autre serveur d'applications) et les données personnelles de l'utilisateur entrées par le dispositif en ligne de l'organisme de santé ;
- une étape de test d'éligibilité pour vérifier la compatibilité de la carte SIM avec l'application *e.prescription*.
- une étape de personnalisation des données de l'utilisateur dans la carte SIM.

On va maintenant décrire les étapes E1 à E43 relatives aux échanges d'une *e.prescription* depuis la prescription par le médecin jusqu'au stockage sur le serveur de l'assurance maladie. Ces étapes se regroupent en trois phases.

Au cours d'une première phase, le patient M se trouve chez le médecin/Praticien P. Il présente son bracelet au lecteur NFC associé au terminal du praticien P. Un certain nombre d'étapes s'ensuit dans le but d'assurer une communication sécurisée entre le bracelet et le terminal du praticien.

Lors d'une étape E1, les identifiants ID_D et CPT_D du praticien sont transmis au bracelet électronique qui les reçoit lors d'une étape E10 et répond lors d'une étape suivante E11 en transmettant ses propres identifiants ID_M et CPT_M ainsi que sa clé publique PK_M et un message signé en utilisant sa clé privée SK_M comportant les identifiants du patient et les identifiants préalablement reçus du praticien. Ce message est noté :

$$ID_M, CPT_M, PK_M, S_M = \{ID_M, CPT_M, ID_D, CPT_D\}SK_M$$

Puis lors d'une étape E3, le terminal du praticien teste la validité du message reçu, à l'aide de la clé publique PK_M qu'il vient de recevoir ; en particulier, il vérifie la validité de la signature S_M du message. Si le résultat de

vérification est correct, cela signifie que la signature a bien été émise par le patient (c'est-à-dire qu'il est correctement identifié). Dans le cas contraire, le procédé s'arrête. Il peut dans ce cas être demandé l'aide en ligne du service après-vente de l'application, ou il peut être décidé d'établir une prescription papier, etc. De manière préférentielle, non illustrée mais bien connue de l'homme du métier, le certificat C_M du patient est transmis dans le message et utilisé par le

5 récepteur (le praticien D) pour vérifier que la clé publique PK_M est bien celle du patient. Il en va de même pour les messages décrits par la suite, échangés entre le patient et le professionnel de santé.

10 Puis lors d'une étape E4, le praticien saisit son ordonnance O, et le terminal calcule une signature de l'ordonnance S_o , sous la forme :

$$S_o = \{O, PK_D\}SK_D$$

C'est à dire que l'ordonnance et la clé publique sont signées en utilisant la clé privée SK_D du terminal du praticien (TD) pour générer la signature S_o de

15 l'ordonnance, prouvant que l'ordonnance est authentique.

Puis, lors de l'étape E5, un message est transmis en champ proche depuis le lecteur du praticien jusqu'au bracelet. Ce message, comprenant l'*e.prescription*, sa signature, la clé publique du praticien et une signature S_D obtenue à l'aide de la clé privée SK_D du praticien, est noté :

20 $O, S_o, PK_D, S_D = \{ID_M, CPT_M, ID_D, CPT_D\}SK_D$

Le compteur de *e.prescriptions* CPT_D est incrémenté lors d'une étape E6 suivante. Ce compteur (irréversible) a pour but de rendre impossible l'utilisation de signatures S déjà émises (les rejeux). En effet, chaque signature calculée sur la base d'une valeur de compteur différente est unique. Il en va de même pour

25 les compteurs respectifs du professionnel de santé et du patient, qui sont incrémentés lors des étapes E14, E20 et E35. Selon une variante bien connue de l'homme du métier, ces compteurs peuvent être remplacés par des aléas.

Le bracelet reçoit le message lors d'une étape E12 et en teste la validité lors d'une étape E13, à l'aide de la clé publique PK_D qu'il vient de recevoir ;

l'élément de sécurité vérifie la validité de la signature S_D du message. Si le résultat de vérification est correct, cela signifie que la signature a bien été émise par le praticien, donc que le praticien est correctement identifié. Dans le cas contraire, le procédé s'arrête.

- 5 Le compteur du bracelet CPT_M est incrémenté lors d'une étape E14 suivante. L'incrémentation de ce compteur permet de se prémunir d'une duplication frauduleuse de l'*e.prescription*. On notera que cette étape E14 concerne le protocole Praticien-Patient. Ce même compteur sera incrémenté à l'étape E20 à la fin de l'échange entre le bracelet et le professionnel de santé,
- 10 mais selon une variante d'implémentation on pourrait utiliser deux compteurs distincts dans le bracelet : l'un pour sécuriser les protocoles Praticien-Patient et l'autre pour sécuriser les protocoles Patient-Professionnel de santé.

- Selon un premier mode de réalisation de l'invention, la carte SIM peut
- 15 utiliser une ou plusieurs variables représentatives de l'état du document pour éviter notamment sa réémission. Selon un exemple, on utilise un ou plusieurs drapeaux, en anglais flag(s), qui peuvent prendre des valeurs binaires (0 ou 1) correspondant à deux valeurs distinctes de la tension électrique de la mémoire EEPROM de l'élément de sécurité (le changement d'état entre deux valeurs étant
- 20 géré par le logiciel) associé à l'*e.prescription* : ce flag est par exemple initialisé à 1 et remis à 0 lorsqu'il est activé. Ces flags servent à indiquer les différents états de l'*e.prescription* (annulée, remise, non remise, etc.). Selon le contexte et le type de document, on pourrait envisager d'autres états.

- Selon ce mode de réalisation, afin de gérer plusieurs *e.prescriptions*
- 25 dans le bracelet, reçues d'un ou plusieurs praticiens, l'état de la prescription est géré dans l'application sécurisée (APS) qui s'exécute dans la carte SIM ; par exemple, un numéro d'ordre chronologique est choisi par l'application sécurisée pour la *e.prescription*, qui peut se trouver dans un des trois états suivants, par exemple gérés par trois flags f1 à f3 :

- « reçue non remise » ; le flag f1 est mis à jour au cours de l'étape E14b ; ce flag est appelé « variable de réception » ;

- « annulée » ; le flag f2 est mis à jour au cours de l'étape E14c si la demande d'annulation est effectuée ;

5 • « remise » ; le flag f3, appelé aussi « variable de réémission », est mis à jour au cours de l'étape E21. Lorsque la prescription est remise, il n'est plus possible de rejouer un échange de prescription avec un professionnel de santé, par contre il est possible de restituer les données dans l'état de la remise, dans la mesure où elles n'ont pas été effacées.

10 On notera que, pour que la prescription soit annulée par le patient dans la carte SIM, elle doit être annulée avant sa remise au professionnel de santé donc il ne doit pas être possible de restituer les données signées dans l'état annulé (dans ce cas les données n'ont pas été signées par l'élément de sécurité).

15 On notera également que, si pour une raison quelconque, les données de la remise sont perdues ou corrompues pendant le transfert (c'est un cas peu probable mais très gênant) il doit être possible de récupérer les données du transfert dans la carte SIM.

20 Ce mode de réalisation basé sur la gestion du document via les flags f1 à f3 apporte des améliorations dans la sécurité et la gestion d'un document électronique par rapport à l'état de l'art, qui n'empêche pas la réémission éventuelle ou le rejeu de l'*e.prescription* :

- il permet l'annulation par le patient d'une prescription ;

25 - il permet la gestion dans la carte SIM de plusieurs *e.prescriptions*, par exemple lorsque la mémoire EEPROM de la SIM allouée à l'application est pleine, les nouvelles *e.prescriptions* pourront prendre la place de celles qui ont été remises ou annulées, de préférence les plus anciennes.

Au cours d'une seconde phase, le patient M se trouve chez le professionnel de santé (le Pharmacien) P. Il présente son bracelet au lecteur NFC

associé au terminal de traitement du professionnel. Un certain nombre d'étapes s'ensuit dans le but d'assurer une communication sécurisée entre le bracelet et le terminal de traitement du professionnel de santé.

Lors d'une étape E15, les identifiants ID_M et CPT_M du patient sont
 5 transmis au professionnel qui les reçoit lors d'une étape E30 et répond lors d'une étape suivante E31 en transmettant ses propres identifiants ID_P et CPT_P ainsi que sa clé publique PK_P et un message signé en utilisant sa clé privée SK_P comportant les identifiants du professionnel et les identifiants préalablement reçus du patient. Ce message est noté :

$$10 \quad ID_P, CPT_P, PK_P, S_P = \{ID_P, CPT_P, ID_M, CPT_M\}SK_P$$

Le bracelet reçoit ce message lors d'une étape E16 puis en teste la validité lors d'une étape E17, à l'aide de la clé publique PK_P qu'il vient de recevoir ; il vérifie la validité de la signature S_P du message. Si le résultat de
 15 vérification est correct, cela signifie que la signature a bien été émise par le professionnel, et donc qu'il est correctement identifié.

Puis lors d'une étape E18, le bracelet calcule une signature $S_M = \{ID_M, CPT_M, ID_P, CPT_P, So\}SK_M$ à l'aide de sa clé SK_M .

Lors de l'étape E19, un message est transmis en champ proche depuis le bracelet jusqu'au professionnel. Ce message, comprenant l'*e.prescription*, sa
 20 signature, les clés publiques et un message signé en utilisant sa clé privée SK_M , est noté :

$$O, So, PK_M, PK_D, S_M = \{ID_M, CPT_M, ID_P, CPT_P, So\}SK_M$$

Le compteur de prescriptions CPT_M est incrémenté lors d'une étape E20 suivante. L'étape E20 a pour but la mise à jour du compteur CPT_M de l'objet
 25 portable, qui est utilisé pour générer la signature électronique S_M . On notera que la mise à jour de ce compteur n'empêche pas la réémission du message si l'algorithme est mis en œuvre une seconde fois pour la même *e.prescription*, mais que dans ce cas la signature S_M sera différente de celle obtenue lors de la

première mise en œuvre. De ce fait, ce mécanisme prévient le rejeu de l'*e.prescription*.

L'étape E21 a pour but la mise à jour du flag f3 (correspondant à l'état « e.prescription remise »), interdisant la réémission de l'*e.prescription* qui vient
5 d'être transférée, comme il a été expliqué précédemment.

On notera que ces variables peuvent aussi être remises à jour avant le transfert des données.

Dans le mode de réalisation décrit ci-dessus, les *e.prescriptions* restent en mémoire de l'objet portable. Cependant, si l'un des flags f2 ou f3 est activé
10 (c'est à dire à la valeur binaire 0), cela signifie que l'*e.prescription* peut être écrasée par l'arrivée d'une nouvelle *e.prescription*, ou effacée par le système d'exploitation (CPU) de l'objet.

Selon un autre mode de réalisation de l'invention, l'*e.prescription* est
15 effacée de la mémoire EEPROM de l'élément de sécurité lors de l'étape E21'. L'*e.prescription* étant effacée, il n'est plus possible de calculer une nouvelle signature à l'étape E18. Selon ce mode de réalisation, l'étape E21 de modification du flag de réémission (f3) n'est plus nécessaire car la réémission sera rendue impossible par cet effacement. La modification des flags f1 et f2 devient
20 également optionnelle car seules restent en mémoire de l'objet les *e.prescriptions* reçues et non émises. On notera que l'effacement peut être total ou partiel. il suffit par exemple de supprimer les premières données de l'*e.prescription* pour rendre impossible le calcul de la signature et de ce fait une nouvelle émission.

25 Le terminal de traitement du professionnel de santé reçoit les données lors d'une étape E32.

Puis lors d'une étape E33, ce terminal teste la validité du message reçu, à l'aide de la clé publique PK_M qu'il a reçue ; il vérifie la validité de la signature du

message. Si le résultat de vérification est correct, cela signifie que la signature a bien été émise par l'objet du patient.

- 5 Puis lors d'une étape E34, le terminal de traitement du professionnel de santé teste la validité de la signature So , à l'aide de la clé publique PK_D du praticien D , qu'il a reçue il vérifie la validité S_0 de la signature du message. Si le résultat de vérification est correct, cela signifie que l'e.prescription est authentique.

Le compteur du professionnel de santé CPT_p est incrémenté lors d'une étape E35 suivante.

- 10 L'e.prescription est traitée lors d'une étape E36 suivante (délivrance de médicament, acte de kiné, etc.)

Au cours d'une troisième phase, le professionnel de santé P , qui vient de traiter l'e.prescription, la transmet au serveur (7) de l'organisme de santé, via un moyen de communication quelconque, par exemple sur un réseau Internet.

- 15 Un certain nombre d'étapes s'ensuit dans le but d'assurer une communication sécurisée entre le terminal de traitement du professionnel de santé et le serveur de l'organisme de santé.

Le message est préparé lors d'une étape E36. Ce message est noté :

$$O, So, PK_p, PK_D, S_p = \{PK_p, PK_S, DD, So...\} SK_p$$

- 20 Lors de l'étape E37, le message est transmis à l'organisme de santé.

Il est traité par l'organisme de santé au cours des étapes E40 à E43 : les étapes E41 et E42 correspondent à la vérification du message reçu et de la signature So de l'e.prescription. Si le message est correctement déchiffré, cela signifie que les données envoyées par le professionnel de santé sont

- 25 authentiques et en particulier :

- que l'e.prescription est authentique ;
- qu'elle a été traitée par un professionnel de santé correctement authentifié ;

La base de données de l'organisme de santé peut être remise à jour lors d'une étape E43.

Il va de soi que le mode de réalisation qui a été décrit ci-dessus a été donné à titre purement indicatif et nullement limitatif, et que de nombreuses
5 modifications peuvent être facilement apportées par l'homme de l'art sans pour autant sortir du cadre de l'invention.

Notamment, elle peut être généralisée à tout échange de documents similaire à celui de la prescription médicale.

Par exemple, on peut envisager sans perte de généralités d'appliquer
10 l'invention à un système d'assurance automobile dans lequel l'utilisateur est un assuré, le praticien est un expert en assurance automobile fournissant un diagnostic des dégâts, le garage jouant le rôle du professionnel.

Ce système pourrait aussi s'appliquer à tout système d'assurance (habitation, ...) nécessitant l'intervention des trois acteurs précédemment cités :
15 l'utilisateur, l'expert et le professionnel.

Revendications

1. Procédé d'hébergement d'un document électronique (O) sur un objet portable sécurisé (1) pour accéder à un service, ledit document électronique ayant été généré par un terminal de génération (TD) et devant être traité par un terminal de traitement (TP), le procédé comportant les étapes suivantes dans l'objet :
 - une étape (E12) de réception d'un document électronique (O) et d'une signature (So) dudit document électronique (O) ;
 - une étape d'obtention (E12) de la clé publique (PK_D) du terminal de génération (TD) complémentaire d'une clef privée (SK_D) du terminal de génération (TD), et d'une signature (S_D) dudit terminal de génération (TD);
 - une étape d'obtention (E16) de la clé publique (PK_P) du terminal de traitement (TP) complémentaire d'une clef privée (SK_P) du terminal de traitement (TP) et d'une signature (S_P) dudit terminal de traitement (TP);
 - une étape (E13) d'authentification du terminal de génération à l'aide de ladite clef publique (PK_D) du terminal de génération ;
 - une étape (E17) d'authentification du terminal de traitement à l'aide de ladite clef publique (PK_P) du terminal de traitement ;
 - si les deux étapes d'authentification sont réussies :
 - une étape (E18) de génération d'un message comportant au moins :
 - le document électronique (O) et sa signature (So) ;
 - La clé publique (PK_D) du terminal de génération (TD) ;
 - La clé publique (PK_M) de l'objet complémentaire d'une clef privée (SK_M) de l'objet ;
 - une signature (S_M) signée par la clé privée (SK_M) de l'objet ;
 - une étape (E19) d'émission dudit message vers le terminal de traitement.
 - une étape (E21, E21') de modification d'une donnée relative audit document électronique afin de prévenir une autre émission dudit document.

2. Procédé d'hébergement d'un document électronique selon la revendication 1, caractérisé en ce que l'étape de modification d'une donnée (E21) est une étape de modification d'une variable booléenne, dite variable de réémission (f3), dont l'état est représentatif de l'émission dudit document.
- 5 3. Procédé d'hébergement d'un document électronique selon la revendication 1, caractérisé en ce que en ce que l'étape de modification d'une donnée (E21') est une étape d'effacement du document électronique dans la mémoire de l'objet portable.
- 10 4. Procédé d'hébergement d'un document électronique (O) selon la revendication 1, caractérisé en ce que l'étape (E13) d'authentification du terminal de génération est suivie d'une étape de modification (E14b) d'une variable booléenne, dite variable de réception (f1), dont l'état est représentatif de la réception dudit document.
- 15 5. Procédé d'hébergement d'un document électronique selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape d'annulation (E14c) du document.
- 20 6. Procédé d'hébergement d'un document électronique selon la revendication 1, caractérisé en ce que l'objet comporte en outre un compteur (CPT_M) du nombre de présentations de documents électroniques, en ce que la signature (S_M) signée par la clé privée (SK_M) de l'objet est fonction de ce compteur et en ce qu'il comporte une étape de modification dudit compteur après chaque étape de signature.
7. Procédé selon l'une des revendications précédentes, caractérisé en ce que le document électronique est une prescription médicale dématérialisée.
- 25 8. Procédé selon l'une des revendications précédentes, chacune des clés publiques (PK_D , PK_P , PK_M) étant certifiée par une même entité de certification (6).
9. Objet portable (1) pour l'hébergement d'un document électronique (O) pour accéder à un service, ledit document électronique ayant été généré par un

terminal de génération (TD) et devant être traité par un terminal de traitement (TP), l'objet portable comportant :

- un module (CLF) de réception d'un document électronique (O) et d'une signature (So) dudit document électronique (O) ;
- 5 - un module d'obtention (CLF) de la clé publique (PK_D) du terminal de génération (TD) complémentaire d'une clef privée (SK_D) du terminal de génération (TD), et d'une signature (S_D) dudit terminal de génération (TD);
- un module d'obtention (CLF) de la clé publique (PK_P) du terminal de traitement (TP) complémentaire d'une clef privée (SK_P) du terminal de traitement (TP) et d'une signature (S_P) dudit terminal de traitement (TP);
- 10 - un module (SE, APS) d'authentification du terminal de génération à l'aide de ladite clef publique (PK_D) du terminal de génération ;
- un module (SE, APS) d'authentification du terminal de traitement à l'aide de ladite clef publique (PK_P) du terminal de traitement ;
- 15 - un module (APS) de génération d'un message comportant au moins :
 - le document électronique (O) et sa signature (So) ;
 - La clé publique (PK_D) du terminal de génération (TD) ;
 - La clé publique (PK_M) de l'objet complémentaire d'une clef privée (SK_M) de l'objet ;
 - 20 - une signature (S_M) signée par la clé privée (SK_M) de l'objet ;
- un module (CLF) d'émission dudit message vers le terminal de traitement
- un module (SE, CPU) apte à modifier une donnée relative audit document électronique afin de prévenir une autre émission dudit document
- 25

10. Objet portable sécurisé (1) selon la revendication 9, caractérisé en ce que le module d'obtention est un module de communication en champ proche (CLF).

11. Objet portable sécurisé (1) selon la revendication 9, caractérisé en ce que le module de transmission est un module de communication en champ proche (CLF).

30

12. Objet portable sécurisé (1) selon la revendication 9, caractérisé en ce que le module d'authentification est une carte électronique d'abonné (SIM).

13. Procédé de traitement pour transmettre un document électronique (O) d'un terminal de traitement (TP) vers un serveur de traitement (7), ledit document électronique provenant d'un terminal de génération et étant stocké sur un objet portable, le procédé de traitement comportant les étapes suivantes sur le terminal de traitement :

- une étape (E32) de réception d'un document électronique (O) et d'une signature (So) dudit document électronique (O) ;
- 10 - une étape d'obtention (E32) de la clé publique (PK_M) complémentaire d'une clef privée (SK_M) de l'objet portable (1), et d'une signature (S_M) dudit objet portable (1) ;
- une étape d'obtention (E32) de la clé publique (PK_D) du terminal de génération ;
- 15 - une étape (E33) d'authentification de l'objet portable à l'aide de ladite clef publique (PK_M) de l'objet ;
- une étape (E34) d'authentification du terminal de génération à l'aide de ladite clef publique (PK_D) du terminal de génération ;
- si les deux étapes d'authentification sont réussies :
 - 20 • une étape (E36) de génération d'un message comportant au moins :
 - le document électronique (O) et sa signature (So) ;
 - La clé publique (PK_D) du terminal de génération (TD) ;
 - La clé publique (PK_p) du terminal de traitement (TD) ;
 - 25 - une signature (SP) signée par la clé privée (SK_p) du terminal de traitement.
 - une étape (E37) de transmission dudit message vers un serveur de traitement des documents électroniques.

30 14. Procédé de gestion d'un document électronique hébergé sur un objet portable sécurisé (1) pour accéder à un service, ledit document électronique ayant été généré par un terminal de génération (TD) et devant être traité par

un terminal de traitement (TP) et stocké sur un serveur de gestion (7), le procédé comportant les étapes suivantes sur le serveur de gestion (7) :

- réception (E40) d'un message en provenance du serveur de traitement, ledit message comprenant :
 - 5 - le document électronique (O) et sa signature (So) ;
 - La clé publique (PK_D) du terminal de génération (TD) ;
 - La clé publique (PK_p) du terminal de traitement (TP) ;
 - une signature (S_p) signée par la clé privée (SK_p) du terminal de traitement ;
 - 10 - authentification (E41) du terminal de traitement à l'aide de ladite clef publique (PK_p) du terminal de traitement (TP) ;
 - authentification (E42) du terminal de génération à l'aide de ladite clef publique (PK_D) du terminal de génération ;
 - si les deux étapes d'authentification sont réussies, une étape (E43) de
 - 15 stockage du message sur le serveur de gestion (7).
15. Programme d'ordinateur comportant des instructions de code pour la mise en œuvre du procédé d'hébergement conforme à la revendication 1, lorsque celle-ci est exécutée par un processeur.

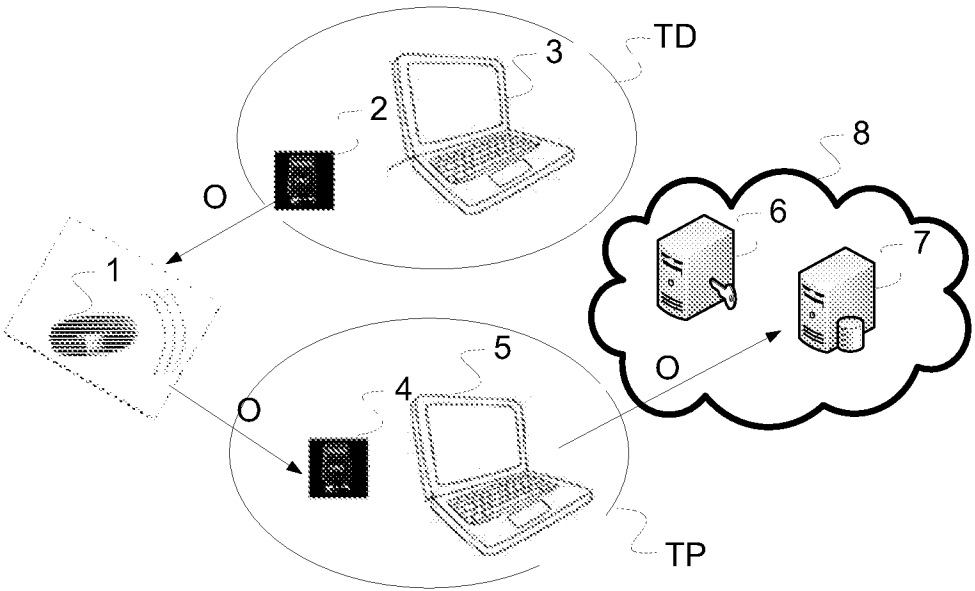


FIGURE 1

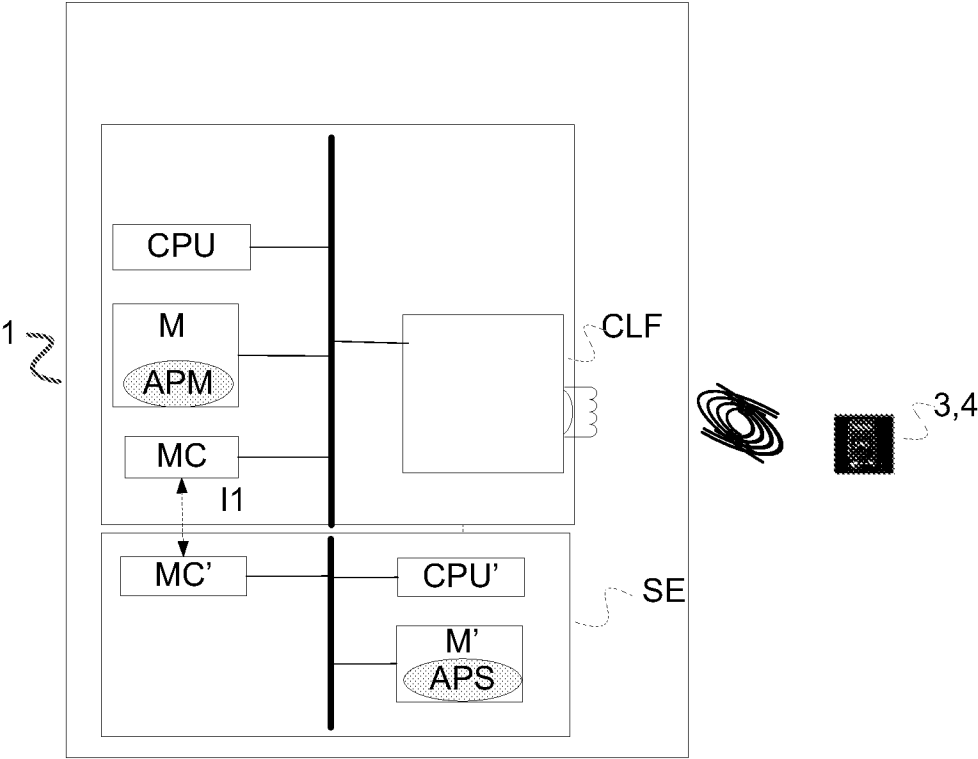


FIGURE 2

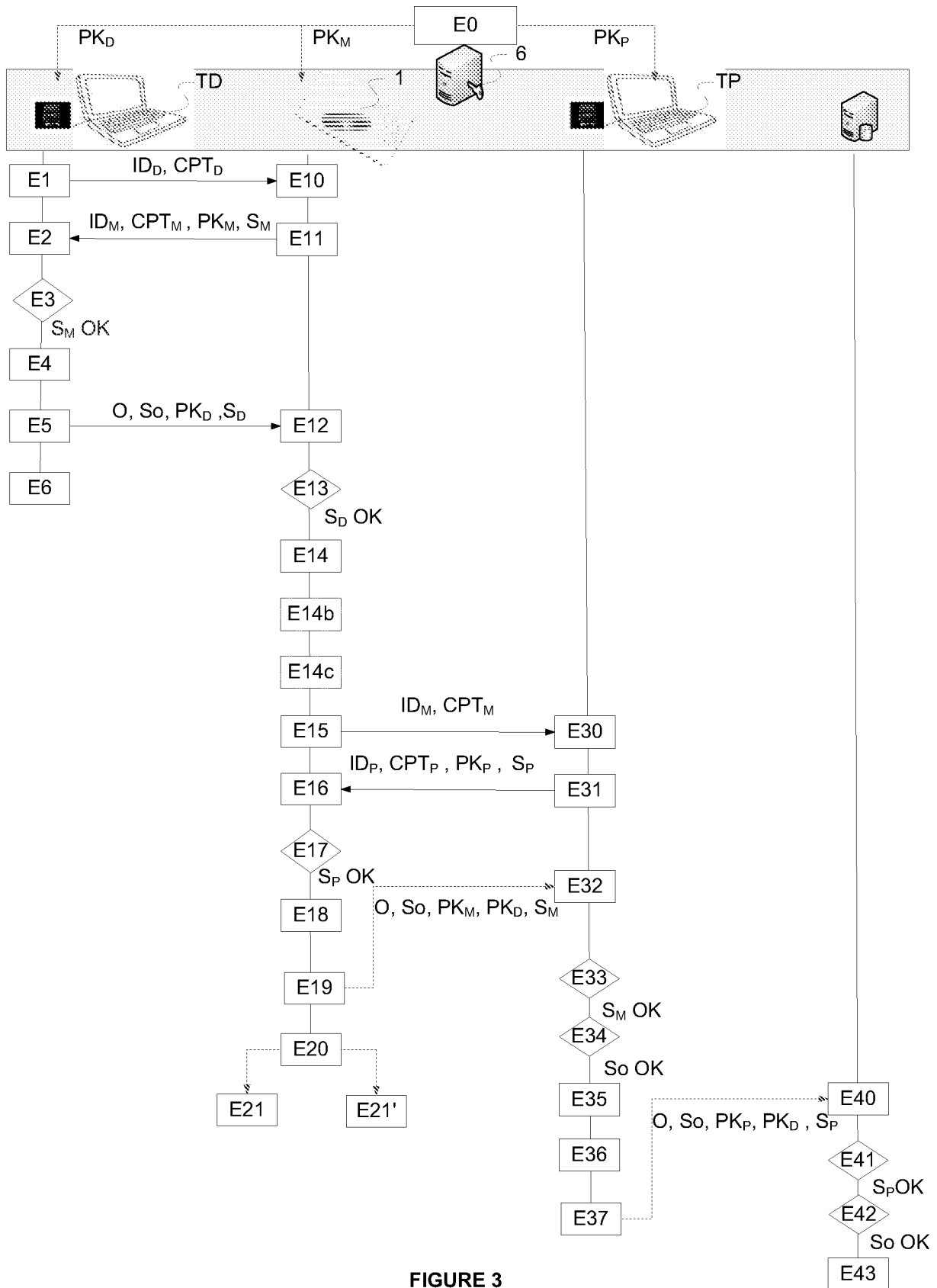


FIGURE 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/051682

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/64 G06F21/34
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Gematik: "Speicherstrukturen der eGK für Gesundheitsanwendungen", 18 March 2008 (2008-03-18), XP055383826, Retrieved from the Internet: URL:https://www.gematik.de/cms/media/dokumente/release_0_5_3/release_0_5_3_egk/gematik_eGK_Speicherstrukturen_V1_6_0.pdf [retrieved on 2017-06-21] page 17 - page 22 ----- -/--	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 August 2017

Date of mailing of the international search report

25/08/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Koblitz, Birger

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2017/051682

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"HBA Spezifikation Teil2_V2 1 0 Einführung der Gesundheitskarte Heilberufs-Ausweis und Security Module Card", 28 May 2006 (2006-05-28), pages 1-144, XP055152508, Retrieved from the Internet: URL:http://www.dkgev.de/pdf/1436.pdf [retrieved on 2014-11-12] page 26 - page 32 -----	1-15
X	Gematik: "Heilberufs-Ausweis und Security Module Card Einführung der Gesundheitskarte Heilberufs-Ausweis und Security Module Card", 28 May 2006 (2006-05-28), XP055384190, Retrieved from the Internet: URL:http://www.dkgev.de/pdf/1435.pdf [retrieved on 2017-06-22] page 70 - page 71 -----	1-15

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2017/051682

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G06F21/64 G06F21/34 ADD.		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) G06F		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	Gematik: "Speicherstrukturen der eGK für Gesundheitsanwendungen", 18 mars 2008 (2008-03-18), XP055383826, Extrait de l'Internet: URL: https://www.gematik.de/cms/media/dokumente/release_0_5_3/release_0_5_3_egk/gematik_eGK_Speicherstrukturen_V1_6_0.pdf [extrait le 2017-06-21] page 17 - page 22 ----- -/--	1-15
☒ Voir la suite du cadre C pour la fin de la liste des documents ☐ Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités:		
"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée	"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets	
Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale	
18 août 2017	25/08/2017	
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Koblitz, Birger

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	"HBA_Spezifikation_Teil2_V2_1_0 Einführung der Gesundheitskarte Heilberufs-Ausweis und Security Module Card", , 28 mai 2006 (2006-05-28), pages 1-144, XP055152508, Extrait de l'Internet: URL:http://www.dkgev.de/pdf/1436.pdf [extrait le 2014-11-12] page 26 - page 32 -----	1-15
X	Gematik: "Heilberufs-Ausweis und Security Module Card Einführung der Gesundheitskarte Heilberufs-Ausweis und Security Module Card", , 28 mai 2006 (2006-05-28), XP055384190, Extrait de l'Internet: URL:http://www.dkgev.de/pdf/1435.pdf [extrait le 2017-06-22] page 70 - page 71 -----	1-15