(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 922 702**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **07 58392**

(51) Int Cl[8] : ***H 04 L 9/28*** *(2006.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.10.07.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 24.04.09 Bulletin 09/17.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *AIRBUS FRANCE Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** CHOPART STEPHANE.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** SANTARELLI.

(54) SECURISATION DE FICHIERS INFORMATIQUES TELECHARGEABLES SUR UN AERONEF BASEE SUR L'IDENTITE D'ENTITES, PROCEDE D'AUTHENFICATION, SYSTEME ET AERONEF ASSOCIES.

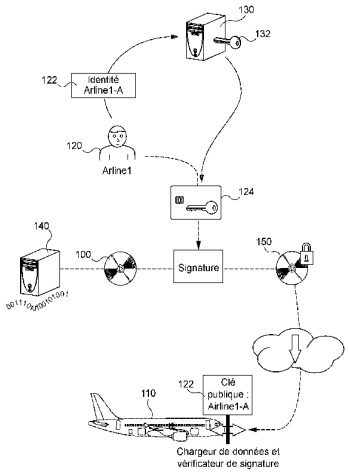
(57) La présente invention concerne de manière générale la sécurité de fichiers informatiques embarqués à bord d'un aéronef et en particulier les mécanismes qui permettent d'en garantir l'authenticité, c'est-à-dire l'origine et l'intégrité.

Selon une réalisation de l'invention, un procédé de traitement, en particulier de sécurisation, d'un fichier informatique (100) de fonctionnement d'un équipement embarqué sur un aéronef (110), le procédé comprenant la signature numérique dudit fichier informatique au moyen d'au moins une première clé privée (124, 124'), ladite première clé privée étant générée selon un schéma basé sur l'identité (122, 122') d'une première entité (120, 120').

Le procédé peut également comprendre la signature multiple des données et/ou la génération de clés privées composites à partir de plusieurs centres de génération de clés dédiés.

L'invention vise également un système et un procédé correspondant d'authentification ainsi qu'un aéronef muni d'un tel système.

L'invention s'applique à l'aviation civile, commerciale et privée.



FR 2 922 702 - A1

La présente invention concerne de manière générale la sécurité de fichiers informatiques embarqués à bord d'un aéronef et en particulier les mécanismes qui permettent d'en garantir l'authenticité, c'est-à-dire l'origine et l'intégrité.

Garantir l'origine d'un fichier s'entend comme garantir que le fichier émane bien du fournisseur du fichier, par exemple d'un constructeur aéronautique, d'une compagnie aérienne, d'un constructeur d'équipements.

Garantir l'intégrité d'un fichier s'entend comme garantir que le contenu de celui-ci n'a pas été altéré accidentellement ou intentionnellement.

Des opérations de configuration, de maintenance ou de mise à niveau d'un aéronef nécessitent couramment le chargement ou le téléchargement de fichiers de programmes ou de données à bord de calculateurs ou de systèmes avioniques embarqués.

De manière conventionnelle, le téléchargement de fichiers informatiques sur un aéronef est encadré par la norme industrielle ARINC 665. Cette norme définit, entre autres, le format de l'en-tête des fichiers téléchargeables sur l'aéronef, en-tête qui contient des informations de configuration, de compatibilité et d'intégrité.

L'intégrité des programmes ou données téléchargé(e)s, vis-à-vis par exemple d'erreurs de transmission ou d'enregistrement, est dans la pratique assurée par un code de détection d'erreur (CRC – "*Cyclic Redundancy Check*" selon la terminologie anglo-saxonne) présent dans l'en-tête de ces fichiers.

Cependant, ce code CRC n'a pas été conçu pour se prémunir d'actes de malveillance par lesquels un tiers modifie volontairement le code informatique des données ou programmes et recalcule le code CRC associé.

Afin de sécuriser ces fichiers contre ces actes de malveillance, il est connu de signer numériquement les fichiers à télécharger sur un aéronef et de contrôler cette signature numérique lors du téléchargement et de l'exécution.

Un mécanisme de signature numérique connu repose sur un algorithme de cryptographie asymétrique et une infrastructure à clés publiques tels que définis par la norme RFC 3647 – Internet X.509 Public Key Infrastructure (PKI).

Selon ce schéma, un fournisseur signe une empreinte numérique du fichier à l'aide de sa clé privée et joint au fichier signé la clé publique correspondante accompagnée d'un certificat électronique établi par une autorité de certification attestant que la clé publique appartient effectivement au fournisseur.

Le certificat électronique fournisseur est signé par la clé privée de l'autorité de certification. Cette clé privée est associée à un certificat dit "racine", auto-signé par l'autorité de certification. Le certificat "racine" est le cœur du mécanisme de certification et donc de toute la confiance apportée au système. Ce certificat est considéré comme authentique. La confiance que l'on accorde à ce certificat racine est proportionnelle à la confiance que l'on accorde à l'autorité de certification, au travers de son infrastructure de gestion de clés et de la politique de certification mise en place.

A bord de l'aéronef, l'utilisateur d'un fichier téléchargé ainsi signé peut vérifier à l'aide de la clé publique du fournisseur et de la signature numérique que le fichier en question est bien celui originellement signé par le fournisseur.

En pratique, l'utilisateur vérifie également, d'une part, que le certificat du fournisseur est authentique, et, d'autre part, que le certificat n'est pas révoqué ou expiré au moment de la signature.

Dans les systèmes actuels, la révocation/expiration ou non du certificat est vérifiée à l'aide de listes de révocation des certificats tenues à jour par l'autorité de certification. Une mise à jour régulière de ces listes de révocation nécessite qu'un chargement régulier de celles-ci à bord de l'aéronef soit mené. Ce processus nécessite donc un surcroît de travail et l'omission d'une mise à jour peut entraîner une impossibilité d'utiliser des fichiers valides téléchargés. Cette solution apparaît ainsi peu adaptée aux avions commerciaux.

L'authenticité du certificat du fournisseur est, quant à elle, vérifiée à l'aide de la clé publique de l'autorité de certification, le lien entre la clé publique et l'identité de l'autorité étant garantie par le certificat "racine".

Ainsi, la vérification de l'authenticité d'un fichier à bord d'un aéronef nécessite de disposer du certificat racine à bord de l'aéronef.

La sécurité du système de signature des fichiers téléchargeables à bord de l'aéronef est donc fortement liée à la façon dont le certificat racine est protégé à bord de l'aéronef.

Si le certificat racine est stocké dans un composant électronique "sûr" tel un composant matériel de type ROM ("*Read Only Memory*" selon la terminologie anglo-saxonne), la sécurité du système est forte mais l'accessibilité au certificat racine est complexe à mettre en œuvre à chaque modification demandée.

En revanche, si le certificat est rendu facilement accessible, alors la souplesse d'emploi est forte mais la sécurité du système est plus facilement compromise.

Il existe donc un besoin d'un mécanisme de sécurisation de fichiers informatiques adapté au téléchargement des fichiers à bord d'un aéronef, qui soit à la fois sûr et souple d'utilisation.

A cet effet, l'invention vise notamment un procédé de traitement, notamment de sécurisation, d'un fichier informatique de fonctionnement d'un équipement embarqué sur un aéronef, le procédé comprenant la signature numérique dudit fichier informatique au moyen d'au moins une première clé privée, ladite première clé privée étant générée selon un schéma basé sur l'identité (IBE acronyme de "*Identity Based Encryption*" selon la terminologie anglo-saxonne) d'une première entité.

L'entité peut être entendu comme une entité physique, par exemple un individu, un objet ou un groupe de sous-entités, ou une entité morale, par exemple une entreprise. L'entité peut être à titre d'exemple un éditeur d'un logiciel ou producteur de données, un fournisseur ou revendeur de ces fichiers de programmes ou de données, une compagnie aérienne, un constructeur aéronautique ou d'équipements aéronautiques embarqués.

On entend par "fichier de fonctionnement" tout fichier informatique de programme ou de données qui est utile pour ou lors du fonctionnement de l'équipement auquel il se rapporte. A titre d'exemple, on connaît les fichiers de commandes, les fichiers d'exécution, les fichiers de données, les fichiers de paramétrage.

Le principe du chiffrement basé sur l'identité repose sur l'unicité de l'identité de l'entité. L'invention permet de disposer d'une clé publique qui découle de l'identité de l'entité et qui diffère pour deux entités présentant une identité différente.

Du fait de l'unicité des clés publiques et de leur attachement à l'identité concernée, on s'affranchit de la nécessité d'un certificat. Les mécanismes de sécurisation des fichiers téléchargeables à bord d'un aéronef se trouvent alors simplifiés.

L'identité de l'entité est une information publique à disposition de tous pour identifier l'entité parmi toutes les entités existantes, notamment sous forme de chaîne de caractères intelligible. Il peut s'agir des informations d'identification couramment utilisées: nom d'un individu ou objet, numéro de sécurité sociale, numéro d'inscription au registre du commerce pour une société. L'identité peut également être vue comme un qualificatif d'un groupement de sous-entités (ou sous-groupe), par exemple les pilotes ou les agents de bord ("*steward*" selon la terminologie anglo-saxonne).

Au contraire des solutions connues, la sécurisation selon l'invention est plus adaptée à la durée de vie de l'avion. En effet, les certificats de l'infrastructure PKI exposée précédemment présentent un cycle de vie volontairement limitée pour des raisons de sécurité, en moyenne trois ans pour un certificat utilisateur et vingt ans pour un certificat racine. Ces durées de vie sont peu adaptées à la durée de vie d'un aéronef commercial (quarante ans). Un grand nombre de générations de nouveaux certificats est alors à prévoir tout au long de la vie de l'aéronef. En l'absence de certificats utilisateur, comme mis en œuvre par la présente invention, il n'y a plus lieu d'intervenir fréquemment sur les fichiers déjà signés.

L'invention présente également l'avantage d'éviter la mise en oeuvre d'une infrastructure de gestion des certificats et l'investissement lourd et coûteux associé.

La gestion de l'authentification selon l'invention est également améliorée en ce qu'il est possible d'éviter de mettre à jour une liste de révocation à bord de l'aéronef.

Selon un mode de réalisation, le procédé comprend la signature numérique du fichier informatique signé par au moins une deuxième clé privée générée selon un schéma basé sur l'identité d'une deuxième entité.

Selon l'invention, on signe ainsi une deuxième fois le fichier. Ce schéma accroît la sécurité en ce que la deuxième signature garantit une vérification et une validation préalables de la première signature, avant diffusion du fichier multi-signé à bord de l'aéronef. Des flux de travaux ("*workflow*" selon la terminologie anglo-saxonne) plus complexes tirant profit de la signature multiple peuvent également être prévus.

L'invention ne limite pas la multiplicité de signatures du fichier informatique.

En particulier, la signature est basée sur un schéma Gap Diffie-Hellman (GDH). Notamment, la signature met en oeuvre une application bilinéaire, par exemple définie à valeurs dans un groupe formé de points d'une courbe elliptique ou d'une courbe hyper-elliptique.

En particulier, on peut prévoir que ladite application bilinéaire réalise un pairage de Weil ou un pairage de Tate.

Sur la base des propriétés du schéma GDH, on prévoit que le procédé comprend en outre une étape d'authentification du fichier informatique au moins doublement signées par une clé publique liée à la combinaison des identités desdites au moins première et deuxième entités. La vérification de l'authenticité du fichier peut ainsi être effectuée à l'aide d'une unique clé publique composée à partir des identités des deux entités, par exemple par concaténation de ces identités.

En agrégeant les signatures, on obtient une protection accrue des fichiers téléchargeables, puisque même si l'une des deux clés privées est

compromise, l'autre co-signataire peut fournir (en fonction du degré de sécurité souhaité) la validation requise pour garantir l'authenticité du fichier téléchargé.

En outre, la garantie fournie par l'autre co-signataire évite de re-signer tous les fichiers déjà signés par la clé compromise et révoquée.

Dans un mode de réalisation, on prévoit une étape préalable de génération d'une clé privée (clé composite) composée d'au moins deux clés partielles générées chacune selon un schéma basé sur l'identité de l'entité correspondant à la clé privée et générées chacune par un serveur différent. En particulier, on opte pour deux demi-clés générées par deux serveurs.

Selon cette réalisation, on garantit que seul l'utilisateur signataire détient sa clé privée dans son intégralité. Chacun des deux ou plus serveurs ne connaît que la clé privée partielle qu'il a générée. Ce schéma satisfait au principe de non répudiation selon lequel le signataire du fichier ne peut nier avoir signé le fichier informatique puisqu'il est le seul à détenir la clé privée.

Afin de garantir un fonctionnement efficace de la solution selon l'invention, on prévoit que la génération d'une clé privée d'une entité comprend la mise en conformité de l'identité de l'entité avec une convention. La convention doit être entendu comme un formatage des informations d'identité, par exemple un format "nom_prénom". La convention est connue de tous et permet à tout un chacun de récupérer la clé publique sans intervention externe pour valider l'authentification d'un fichier signé.

En cas de compromission de la clé privée d'un individu, il convient de regénérer une nouvelle clé privée toujours sur la base de l'identité (inchangée) de l'individu. Dans ce dessein, on prévoit que ladite convention comprend l'ajout à ladite identité d'une information décorrélée de ladite identité. L'information est notamment variable, par exemple par incrément ou selon la date du jour ou l'heure.

Afin d'adapter l'invention au plus près de la durée de vie de l'aéronef (environ quarante ans), on prévoit que la génération de clés privées selon un schéma basé sur l'identité comprend l'utilisation de courbes elliptiques, notamment des courbes hyper-elliptiques. Les propriétés mathématiques des courbes elliptiques permettent effectivement de fournir des moyens

cryptographiques plus sûrs que ceux mis en oeuvre aujourd'hui par les infrastructures PKI de l'état de l'art.

L'invention a également trait à un système pour le traitement, en particulier la sécurisation, d'un fichier informatique de fonctionnement d'un équipement embarqué sur un aéronef, le système comprenant des moyens de signature numérique dudit fichier numérique au moyen d'au moins une première clé privée, ladite première clé privée étant générée selon un schéma basé sur l'identité d'une première entité.

Dans un mode de réalisation, on prévoit des moyens de génération d'une clé privée basée sur l'identité d'une entité et composée d'au moins deux clés partielles, lesdits moyens de génération comprenant au moins deux serveurs aptes à générer des clés partielles selon un schéma basé sur l'identité de l'entité correspondant à la clé privée.

De façon optionnelle, le système peut comprendre des moyens se rapportant aux caractéristiques de procédé de traitement présentées ci-dessus.

L'invention a également trait à un procédé d'authentification d'un fichier informatique de fonctionnement d'un équipement embarqué sur un aéronef, ledit fichier informatique étant signé (numériquement) par une première entité, le procédé comprenant une étape de vérification de la signature dudit fichier signé à partir d'une première clé publique déterminée selon un schéma basé sur l'identité de ladite première identité.

Dans un mode de réalisation, le procédé comprend une étape préalable de chargement dudit fichier informatique signé à bord dudit aéronef.

Dans un mode de réalisation, on prévoit également une étape préalable de détermination de la première clé publique, l'étape de détermination étant effectuée à bord dudit aéronef.

Dans un mode de réalisation, ledit fichier informatique est signé au moyen d'une pluralité de clés privées générées selon un schéma basé sur l'identité d'une pluralité d'entités, et ladite clé publique, dite clé publique globale, est formée à partir de clés publiques déterminées selon un schéma basé sur l'identité de la pluralité d'entités. Notamment, la clé publique globale est formée par la concaténation desdites clés publiques.

De façon optionnelle, le procédé peut comprendre des étapes et mettre en œuvre des moyens se rapportant aux caractéristiques de procédé et de système présentées ci-dessus.

L'invention vise également un système d'authentification d'un fichier informatique de fonctionnement d'un équipement embarqué sur un aéronef, ledit fichier informatique étant signé par une première entité, le système comprenant des moyens de vérification de la signature dudit fichier signé à partir d'une première clé publique déterminée selon un schéma basé sur l'identité de ladite première identité.

De façon optionnelle, le système peut comprendre des moyens se rapportant aux caractéristiques de procédé d'authentification présentées ci-dessus.

L'invention vise également un aéronef comprenant un tel système d'authentification.

Par l'utilisation de clés basées sur l'identité des entités, on évite également les difficultés liées à la gestion de certificats dans des solutions "ouvertes" reposant sur des accords de confiance entre autorités de certification de type certification croisée et/ou avec des autorités de certification déléguées.

Les caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture d'un mode préféré de réalisation illustré par les dessins joints, dans lesquels :

- la **figure 1** illustre les différentes étapes d'un processus de signature d'un fichier informatique mises en œuvre dans un exemple de l'invention ;
- la **figure 2** représente un exemple de génération de clé privée utilisateur alternatif à celui de la figure 1 ;
- la **figure 3** illustre les différentes étapes d'un processus de signatures multiples d'un fichier informatique mises en œuvre selon un exemple de l'invention ;
- la **figure 4** illustre un premier exemple de processus de renouvellement de clés privées utilisateur selon l'invention ;

- la **figure 5** illustre un deuxième exemple de renouvellement de clé privée en présence notamment de deux centres de génération de clés ; et
- la **figure 6** représente un en-tête de fichier téléchargeable pour la mise en œuvre de l'invention.

L'invention part du constat que les limites des infrastructures PKI connues pour leur intégration dans le monde aéronautique sont directement liées au besoin des certificats, et donc au besoin de garantir le lien entre une clé à utiliser et un individu.

Pour la suite, nous utiliserons des intervenants du monde aéronautique bien que l'invention s'applique à tout type d'entité signataire.

La **figure 1** illustre les différentes étapes mises en œuvre dans la chaîne de signature d'un fichier, ici des données utilisateur 100, à télécharger dans un avion 110.

L'utilisateur 120 possède une identité publique connus de tous, ici "Airline 1". Dans le schéma de cryptage basé sur l'identité, une convention de nommage des identités est connue afin de faciliter la gestion et la détermination des clés publiques d'utilisateurs. Dans ce schéma, la clé publique de l'utilisateur est notamment constituée de l'identité de l'individu selon la convention.

Par la suite, on appellera indifféremment "identité" et "clé publique" l'information d'identité de l'entité, ici l'utilisateur 120, qu'elle soit ou non formatée selon la convention prévue. Il est effectivement aisé de passer de l'identité "brute" à l'identité "formatée"/clé publique. En particulier, cette identité est sous forme d'une chaîne de caractères alphanumériques.

Dans l'exemple de la **figure 1**, la clé publique de cryptage 122 de l'utilisateur "Airline 1" est facilement déterminée comme étant "Airline1-A", ici la convention de nommage comprend une simple concaténation des données d'identité avec une lettre "A".

Comme on le verra par la suite, l'ajout d'une donnée complémentaire, décorrélée de l'utilisateur, ici "A", et qui de surcroît est variable permet de générer une "nouvelle" identité qui pourra être utilisée lorsqu'il y aura lieu de générer une nouvelle clé privée pour l'utilisateur.

A l'initialisation du système, l'utilisateur 120 émet une requête en génération d'une clé privée 124 à partir de son identité "Airline1-A" auprès d'un centre de génération de clés 130.

Le centre 130 héberge secrètement une clé "racine" 132 à partir de laquelle elle calcule les clés privées 124 des utilisateurs. Les clés privées 124 sont par exemple établies sur 2048 bits. Le centre 130 retourne alors la clé privée 124 de l'utilisateur.

Un exemple de génération de clé privée est décrit dans le document "*Identity-based encryption from the Weil pairing*" de Boneh *et al*. (SIAM J. of Computing, Vol. 32, N°3, pp. 586-615, 2003).

Lors de l'utilisation du système, des données 100 sont générées depuis une unité de génération 140, ici un serveur informatique, par exemple suite à des calculs d'amélioration ou paramétrage d'équipements aéronautiques.

Ces données sont signées par l'utilisateur 120 au moyen de sa clé privée 124 pour donner un fichier signé 150.

Les données signées 150 par l'utilisateur sont ensuite transmises sur un réseau de communication à l'avion 110.

Une unité de chargement des fichiers, également appelée *Data Loader* selon la terminologie anglo-saxonne, télécharge le fichier signé 150 à destination d'un ou de plusieurs équipements embarqués dans l'avion 110. Un exemple d'infrastructure de module de chargement et passerelle associée est fournie dans le document de brevet EP-1 349 078

Avant diffusion et/ou installation des données sur ces équipements, une vérification de la signature est effectuée.

La clé publique 122 de l'utilisateur 120 est connue au niveau de l'avion 110, ici parce que c'est l'utilisateur "Airline 1" qui est le générateur des données.

A partir de la clé publique 122, ici "Airline1-A", les données téléchargées peuvent être authentifiées et, en cas d'authentification positive, installées sur l'équipement concerné.

On utilise notamment un schéma de signature basé sur l'identité à partir de courbes elliptiques. Un tel schéma est, par exemple, exposé dans la publication "*ID-based signatures from pairings on elliptic curves*" de l'International Association for Cryptologic Research (Paterson, *http://eprint.iacr.org/2002/004.ps*) ou la publication "*Short signatures from the Weil Pairing*" (D. Boneh, H. Shacham et B. Lynn, *Advances in Cryptology – AISACRYPT 2001*, Springer-Verlag, 2001, pp. 514-532).

En pratique, le centre de génération de clés 130 rend public un certain nombre de paramètres relatifs au schéma de signature. A titre simplement d'exemple, ces paramètres peuvent être les suivants :

- un groupe G_1 additif d'ordre q formé de points sur une courbe elliptique,
- une application bi-linéaire **e** : G_1 x G_1 -> G_2, où G_2 est un groupe multiplicatif d'ordre q également. Cette application peut notamment être dérivée du pairage de Weil ou Tate,
- un générateur **P** du groupe G_1 choisi aléatoirement, et une valeur publique $\mathbf{P_{public}}$=s.P où s est la clé racine du centre 130,
- des fonctions de hachage $\mathbf{H_i}$, à sens unique.

La clé privée 124 de l'utilisateur est définie par $K_{privée}$=s.H_1("Airline1-A"), H_1 s'appliquant sur une écriture binaire de la chaîne de caractères et ayant valeur dans le groupe G_1 formé de points de l'ellipse. La publication Boneh-Shacham-Lynn ci-dessus fournit en son paragraphe 3.2 une illustration de fonction de hachage.

La signature M' des données M binaires 100 peut alors être calculée par l'utilisateur 120 selon par exemple: $M' = k^{-1}(H_2(M).P+H_3(R).K_{privée})$ où **R**=k.P et k est choisi aléatoirement par l'utilisateur, et k^{-1} est l'inverse de k pour la multiplication.

La signature transmise au *data loader* est alors composée de **R** et M'.

A réception d'un message $M_{reçu}$ et de la signature ($M'_{reçu}$, $R_{reçu}$) (données signées 150) à bord de l'aéronef, l'authentification des données 100 $M_{reçu}$ peut être réalisée par la vérification suivante :

$$\mathbf{e}(M'_{reçu}, R_{reçu}) = \mathbf{e}(\mathbf{P}, \mathbf{P})^{[\mathbf{H_2}(M_{reçu})]}.\mathbf{e}(P_{public}, \mathbf{H_1}(\text{"Airline1-A"}))^{\mathbf{H_3}(R_{reçu})}$$

Les paramètres publics du centre 130 sont générés une seule fois pendant une phase d'initialisation.

On remarque que la clé racine s n'est pas utilisée hors des phases d'initialisation. Il est donc possible de stocker cette clé racine dans un dispositif matériel sécurisé, ici une carte à puce, sans nuire à l'efficacité du système. Une alternative aux cartes à puce peut être apportée par l'utilisation de jetons ("*token*" selon la terminologie anglo-saxonne) qualifiées à haut niveau de sécurité selon la norme FIPS 140-1 (*Federal Information Processing Standard*) niveau 3 par exemple. L'invention présente ainsi un avantage par rapport aux solutions de l'art antérieur reposant sur les infrastructures PKI, puisque on s'affranchit du besoin permanent d'une infrastructure de gestion de la clé maître et des certificats associés.

En référence à la **figure 2**, on a représenté un schéma de génération de clé privée utilisateur 124 selon un autre mode de réalisation.

Le système de génération de clés privées utilisateur comprend plusieurs centre de génération de clés, ici deux serveurs 130, 130' sont utilisés.

Lors de la phase d'initialisation, l'utilisateur 120 "Airline 1" émet une requête de génération de clé privée à l'attention des deux serveurs. La requête comprend l'identité formatée 122 "Airline1-A".

Chaque centre 130, 130' génère une clé privée propre 124-a, 124-b sur la base de l'identité 122. Des mécanismes de génération similaires à ceux évoqués en lien avant la **figure 1** peuvent être employés.

L'utilisateur réceptionne chacune des clés privées générées par les centres, appelées ci-après clés partielles, ici des demi-clés.

L'utilisateur 120 forme ensuite sa clé privée 124 à partir des clés partielles reçues, ici par une simple concaténation des deux demi-clés 124-a et 124-b.

Dans la chaîne de signature de fichiers informatiques, l'utilisateur 120 signe les fichiers à l'aide de la clé privée 124, par exemple de manière similaire à celle évoquée en lien avec la **figure 1**, et non avec une seule des clés partielles.

Le système de signature de fichiers informatiques mettant en œuvre ce mécanisme de clés partielles garantit la non-répudiation de signature par l'utilisateur, puisque désormais seul lui possède la clé privée 124 dans son intégralité. En effet, les centres 130 et 130' ne connaissent chacun qu'une clé partielle.

En référence maintenant à la **figure 3**, on prévoit une signature multiple du message, ici notamment une double signature, d'une part par l'utilisateur 120 générateur des données 100 et d'autre part, par une autre entité, par exemple le constructeur de l'avion, identifié ici par "A400M-A" selon la convention de formatage applicable.

Cette signature multiple permet de mettre en œuvre différents niveaux successifs de validation des données avant chargement dans l'avion 110.

Plus en détail, les données 100 sont signés, par exemple sur l'exemple de la publication Lin *et al.* "*A Structured Multisignature Scheme from the Gap Diffie-Hellman Group*" de Chih-Yin Lin, Tzong-Chen Wu et Fangguo Zhan :

- un groupe GDH cyclique multiplicatif G_1 d'ordre premier q est formé de points sur une courbe elliptique,
- une application bi-linéaire **e** : G_1 x G_1 -> G_2 est établie, où G_2 est un groupe d'ordre q également. Cette application peut notamment être dérivée du pairage de Weil ou Tate. On peut également utiliser une application bi-linéaire modifiée ê, par exemple telle que définie dans la publication Boneh-Shacham-Lynn ci-dessus,
- un générateur **P** du groupe G_1 est choisi aléatoirement,
- deux fonctions de hachage à sens unique H_1 et H_2: {0,1}* -> G_1\{1} sont définies. H_1 est par exemple similaire à la fonction de hachage du même nom évoquée en lien avec la **figure 1**.

Les paramètres publics du système, à savoir **e**, **P**, q, G_i et H_i sont, par exemple, issus d'une librairie cryptographique implémentant le schéma GDH signature.

La clé privée 124 de l'utilisateur 120 est générée de façon similaire à la **figure 1** en utilisant la fonction de hachage H_1 et la clé racine s du centre 130: $K_{privée}=s.H_1("Airline1-A")$.

Les données 100 sont, dans un premier temps, signées par l'utilisateur 120, par exemple de façon simplifiée: $M' = [H_2(M)]^K_{privée}$.

A ce stade, l'authenticité des données signées 150 est vérifiée par le deuxième intervenant 120' "A400M-A" à l'aide de la clé publique 122 de l'utilisateur 120. On peut, par exemple, utiliser le même mécanisme de vérification que celui décrit en lien avec la **figure 1** pour une signature appropriée. En lien avec les propriétés du schéma GDH, on vérifie que le quadruplet (P, $H_1("Airline1-A")$, $H_2(M)$, M') est un uplet Diffie-Hellman valide. Cette vérification peut mettre en œuvre l'application bilinéaire e ou ê pour vérifier l'égalité : $e(P, M') = e(H_1("Airline1-A"), H_2(M))$.

En cas d'authentification/vérification positive, le deuxième intervenant 120' signe à nouveau les données 100 et 150 à l'aide de sa clé privée $K'_{privée}$ 124', et produit une nouvelle signature M".

Cette nouvelle signature peut être vue comme une garantie que les données signées par l'utilisateur 120 sont bel et bien authentiques, même si une compromission ultérieure des clés de l'utilisateur 120 intervient. En cas de perte d'une clé privée de l'un ou l'autre des co-signataires, ainsi l'on n'a pas nécessairement besoin de re-signer l'ensemble des fichiers déjà co-signés.

La clé privée 124' peut être générée de façon similaire à la clé privée 124 de l'utilisateur 120. Sur la **figure 2**, on a notamment représenté une génération de clé privée 124' par un unique centre 130'. Cette configuration peut être retenue lorsque aucun besoin de non répudiation n'est requis vis-à-vis du deuxième intervenant 120', par exemple lorsque la responsabilité de ce dernier est continuellement engagée.

On comprend également que plusieurs clés partielles peuvent être générées pour former la clé privée 124' et que notamment ce nombre de clés partielles peut être différent du nombre de clés partielles pour former la clé privée 124.

Le schéma de la deuxième signature M" peut être défini comme suit:

$$M'' = [H_2(M) \,.\, M'] \,\hat{}\, K'_{privée}.$$

Les données doublement signées 150' sont déposées sur un serveur de stockage 200 depuis lequel elles (150') peuvent être chargées sur l'avion 110. Une vérification d'authenticité des données 100 à l'aide des signatures fournies dans les données 150' et de la clé publique 1220 est alors effectuée avant transmission et installation sur les équipements concernés à bord de l'avion. Notamment, on vérifie que (P, H_1(clé publique 1220), H_2(M), M'') est un uplet Diffie-Hellman valide (ou encore que e(P, M'') = e(H_1(clé publique 1220), H_2(M))). La clé publique 1220 est issue par exemple de la concaténation des deux clés publiques 122 et 122'.

Le service rendu par le centre de génération de clés est seulement nécessaire pendant la phase de création de clés privées, aucune activité d'une tierce partie n'est nécessaire hors phase de création des clés, c'est-à-dire pendant la phase d'exploitation à proprement parler (signature et vérification de l'authenticité). Cette notion est illustrée par les cadenas des blocs 134 et 134'. Les clés racine 132 et 132' des centres de génération de clé 130 et 130' sont stockées dans un support matériel hautement sécurisé, ici une carte à puce, et ne sont pas accédées pendant le processus de signature et d'utilisation des fichiers signés. On dit que les clés sont "sanctuarisées".

Pour obtenir une double signature qui puisse être efficacement vérifiée par les identités connues des signataires, on utilise la bi-linéarité de l'application **e**. Une démonstration précise est fournie par le document "*Aggregate and verifiably encrypted signatures from bilinear maps*" (Boneh *et al.* §3.1).

En particulier, les deux signatures des données 100 par les deux clés privées 124 et 124' sont agrégées au moyen d'un schéma structuré de multisignatures. Au delà de la vérification de l'authenticité et de l'intégrité de la signature, l'ordre de création des différentes signatures est également vérifié.

Un exemple de schéma structuré de multisignatures est présenté au paragraphe 3 de la publication Lin *et al.* On note notamment que les multisignatures peuvent être réalisées en série, en parallèle ou de façon mixte.

Le schéma de signatures le mieux adapté pour la présente invention est la structure de type série.

A bord de l'avion, la vérification de la multisignatures peut être réalisée de façon similaire à la vérification de la **figure 1**, pour l'ensemble des deux signatures (ou plus en cas de multisignatures) lorsque les fonctions de signature utilisées correspondent.

Notamment, on prévoit que l'identité publique 1220 utilisée pour vérifier la multisignatures des données 100 est composée à partir des identités particulières de chacun des signataires.

Sur la **figure 3**, on prévoit notamment que la clé publique utilisée est formée de la concaténation du premier signataire "Airline1-A" et du deuxième signataire "A400M-A" selon un algorithme de vérification de multisignatures, par exemple celui du 3ème paragraphe de la publication Lin *et al*.

On peut notamment utiliser tout type de fonction (publique) pour générer la clé publique globale 1220 en fonction des identités publiques des diverses entités ayant signé le fichier. La fonction utilisée peut également tenir compte du schéma structuré de multisignatures utilisé. L'exemple du 3ème paragraphe de la publication Lin *et al*. tient, par exemple, compte du schéma de multisignatures. On note que contrairement à cet exemple, la présente invention s'appuie sur un couple clé publique/clé privée basé sur l'identité (IBE), c'est-à-dire sans certificat. Néanmoins, cette adaptation ne modifie en rien le principe de la signature tel qu'il est exposé dans cette publication.

D'une façon générale, il a été observé que la signature "*Gap Diffie-Hellman*" (publication Boneh-Shacham-Lynn) présente les propriétés mathématiques adaptées au schéma de multisignatures, parmi lesquelles on note :

1/ l'agrégat des signatures réalisées par les co-signataires est vérifiable par une fonction de type "multisignatures" ;

2/ la taille de la multisignatures est la même que celle d'une seule signature ;

3/ la taille de la multisignatures est indépendante du nombre de co-signataires ;

4/ toute partie de la multisignatures peut être publiquement verifiée ;

5/ l'algorithme de vérification de la multisignatures, d'une partie de la multisignatures ou d'une seule signature est le même.

La double signature permet notamment de conserver les fichiers déjà signés alors même qu'une des clés privées signataires a été depuis révoquée. Notamment, il suffit qu'une seule des clés privées signataires ne soient pas compromise pour garantir l'authenticité du fichier signé.

Néanmoins, selon la niveau de sécurité requis, il est possible de restreindre la validation de l'authenticité d'un fichier aux seuls fichiers dont aucune ou une quote-part prédéterminée des clés privées signataires a été compromise.

En référence à la **figure 4**, on décrit maintenant le processus de renouvellement des clés privées utilisateur lorsqu'un clé privée est compromise et donc révoquée par le système.

Dans cet exemple, la clé privée 124 "Airline1-A" a été compromise et un seul centre de génération de clés 130 est utilisé. L'utilisation Airline 1 est alors responsable d'avertir toutes les parties concernées de la révocation de sa clé privée "Airline1-A". En effet, le crypto-système de type IBE ne permet pas de s'affranchir des problèmes liés à la perte d'une clé privée et de la nécessité de révocation de cette clé. Ainsi, afin d'éviter qu'un tiers mal intentionné retrouve et utilise la clé perdue à des fins malveillantes, on prévoit d'avertir la communauté que la clé ne sera plus utilisée par son propriétaire légitime et que sa clé publique est par conséquent modifiée.

On étendra aisément cette réalisation à la présence de plusieurs centres de génération de clés ainsi qu'au cas de signatures multiples pour lequel la génération des clés privées est réalisée indépendamment d'une clé à une autre.

Pour l'opération de régénération de clé privée, la clé racine 132 est "désanctuarisée", c'est-à-dire remise en service, comme illustré par l'ouverture du cadenas du bloc 134. Le centre de génération de clés 130 a désormais un accès à la valeur **s** de la clé racine 132.

Une nouvelle identité 122 est tout d'abord générée pour l'utilisateur 120. Comme l'identité brute "Airline 1" ne peut être modifiée, on remplace la caractère additionnel "A" par un "B". Ainsi l'on obtient une nouvelle identité "Airline1-B". On incrémente ainsi successivement les identités au fur et à mesure de leur perte, ici de A à Z.

De façon générale, la convention de formatage ajoute, à l'identité brute, une donnée décorrélée de cette dernière que l'on modifie, par exemple par incrément lors de la génération d'une nouvelle clé privée. On envisage notamment l'utilisation d'un ou plusieurs caractères alphanumériques, l'utilisation d'une date, par exemple au format YYYYMMDD.

Une table publique tenant à jour la valeur courante de cette donnée supplémentaire peut être disponible sur le centre de gestion de clés 130. Cette table peut être signée par un ou plusieurs membres de la communauté pour en garantir l'authenticité. Une copie de tout ou partie de la table peut également être stockée à bord de l'avion 110.

A partir d'une requête de l'utilisateur 120 contenant la nouvelle identité "Airline1-B", le centre 130 génère, à l'aide de la clé racine 132 désanctuarisée, une nouvelle clé privée 124 pour l'utilisateur.

Après utilisation, la clé racine 132 est de nouveau sanctuarisée dans la carte à puce prévue à cet effet.

Comme l'ancienne clé publique compromise 124 "Airline1-A" ne doit plus être utilisée à bord de l'avion pour vérifier l'authenticité des fichiers, une requête 400 de mise à jour de la table des clés publiques est effectuée, notamment de la table à bord de l'avion 110.

Cette requête comprend l'effacement de l'ancienne clé avec la commande selon la terminologie anglo-saxonne "*Erase Public Key Airline1-A*" et son remplacement par la nouvelle clé privée avec la commande selon la terminologie anglo-saxonne "*Replace by Ailrine1-B*".

Les processus de signature de fichiers et de vérification de l'authenticité de ces fichiers signés, comme illustrés par les **figures 1 et 3**, peuvent continuer à s'appliquer désormais sur la base de l'identité "Airline1-B" et d'éventuellement "A400M-A".

Les fichiers en service déjà émis et signés par l'utilisation 120 Airline 1 et stockés dans le serveur de stockage 200 peuvent :

- soit être re-signés avec la nouvelle clé privée 124 associée à l'identité Airline1-B puis revalidés, dans le cas de la **figure 3** avec la clé privée associée à A400M-A ;

- soit être conservés en l'état puisque même en cas d'utilisation frauduleuse de la clé Airline1-A, aucun nouveau fichier signé avec cette clé ne sera validé par A400M-A. Seuls les fichiers signés lorsque la clé privée associée à Airline1-A n'était pas révoquée et validés par A400M-A seront désormais acceptés pour téléchargement sur l'avion 110.

La **figure 5** illustre ce renouvellement de clé privée 124 en présence de deux centres de génération de clés 130 et 130'.

La nouvelle identité "Airline1-B" 122 formée comme indiqué en référence à la **figure 4** est transmise en même temps sous forme de requête de nouvelle clé privée aux deux centres 130 et 130'.

Les clés racines 132 et 132' de ceux-ci ont été remises en service. Les deux centres génèrent alors chacun les deux demi-clés privées 124-a et 124-b.

Une nouvelle clé privée utilisateur 124 est alors formée au niveau de l'utilisateur 120 sur la base de ces deux demi-clés, ici par exemple par simple concaténation.

Une requête 400 de mise à jour des avions avec la nouvelle clé publique disponible 122 est effectuée sur les mêmes bases que la requête décrite en lien avec la **figure 4**.

En référence à la **figure 6**, on a représenté un en-tête 600 SHF ("*Secure Header File*" selon la terminologie anglo-saxonne) permettant le support de signatures pour des fichiers téléchargeables sur un avion.

Cet en-tête indique une liste de fichiers informatiques comprenant respectivement l'en-tête de chargement 610 selon la norme pré-citée ARINC 665, l'ensemble des fichiers de données et de support les composant 620 et le nom 622, la taille 624, le nombre 626 de blocs de données, la taille 628 respective de ces blocs et les éléments d'intégrité 630 de ces blocs.

De par la signature des données conformément à l'invention, il est inutile que l'en-tête SHF 600 comprenne un champ dédié à un certificat. De tels champs ont donc été supprimés par rapport aux en-têtes conventionnels.

Ainsi, aucun accès à une donnée sensible n'est plus nécessaire à bord de l'avion dans les processus principaux de signature de fichiers informatiques et de vérification de l'authenticité des fichiers. On protège alors plus efficacement les données sensibles, par exemple une clé racine de génération.

Notamment, si aucune clé privée n'est révoquée, aucun accès à la clé racine secrète 132 ne sera effectué durant toute la durée de vie de l'avion.

La présente invention peut être mise en œuvre sous forme de programme(s) informatique(s) exécuté(s) sur une ou plusieurs machines de calcul reprogrammables, par exemple un ordinateur personnel PC, un processeur de signal numérique DSP ("*Digital Signal Processor*" selon la terminologie anglo-saxonne) ou un microcontrôleur.

Les exemples qui précèdent ne sont que des modes de réalisation de l'invention qui ne s'y limite pas.

REVENDICATIONS

1. Procédé de traitement d'un fichier informatique (100) de fonctionnement d'un équipement embarqué sur un aéronef (110), le procédé comprenant la signature numérique dudit fichier informatique au moyen d'au moins une première clé privée (124, 124'), ladite première clé privée étant générée selon un schéma basé sur l'identité (122, 122') d'une première entité (120, 120').

2. Procédé de traitement selon la revendication 1, comprenant la signature numérique du fichier informatique signé (150, 150') par au moins une deuxième clé privée (124') générée selon un schéma basé sur l'identité (122') d'une deuxième entité (120').

3. Procédé de traitement selon l'une des revendications précédentes, comprenant une étape préalable de génération d'une clé privée (124) composée d'au moins deux clés partielles (124-a, 124-b) générées chacune selon un schéma basé sur l'identité (122) de l'entité (120) correspondant à la clé privée (124) et générées chacune par un serveur différent (130, 130').

4. Procédé de traitement selon l'une des revendications précédentes, dans lequel la génération d'une clé privée (124, 124') d'une entité (120) comprend la mise en conformité de l'identité de l'entité avec une convention.

5. Procédé de traitement selon la revendication précédente, dans lequel ladite convention comprend l'ajout à ladite identité d'une information décorrélée de ladite identité.

6. Procédé d'authentification d'un fichier informatique (100) de fonctionnement d'un équipement embarqué sur un aéronef (110), ledit fichier informatique (100) étant signé (150, 150') par une première entité (120, 120'), le procédé comprenant une étape de vérification de la signature dudit fichier signé (150, 150') à partir d'une première clé publique (122, 122', 1220) déterminée selon un schéma basé sur l'identité de ladite première entité (120, 120').

7. Procédé d'authentification selon la revendication précédente, comprenant une étape préalable de détermination de la première clé publique (122, 122', 1220) effectuée à bord dudit aéronef (110).

8. Procédé d'authentification selon la revendication 6 ou 7, dans lequel ledit fichier informatique (100) est signé au moyen d'une pluralité de clés privées (124, 124') générées selon un schéma basé sur l'identité d'une pluralité d'entités, et ladite clé publique (1220) est formée à partir de clés publiques (122, 122') déterminées selon un schéma basé sur l'identité de la pluralité d'entités (120, 120').

9. Système d'authentification d'un fichier informatique (100) de fonctionnement d'un équipement embarqué sur un aéronef (110), ledit fichier informatique (100) étant signé (150, 150') par une première entité (120, 120'), le système comprenant des moyens de vérification de la signature dudit fichier signé (150, 150') à partir d'une première clé publique (122, 122', 1220) déterminée selon un schéma basé sur l'identité de ladite première entité (120, 120').

10. Aéronef (110) comprenant un système d'authentification selon la revendication 9.

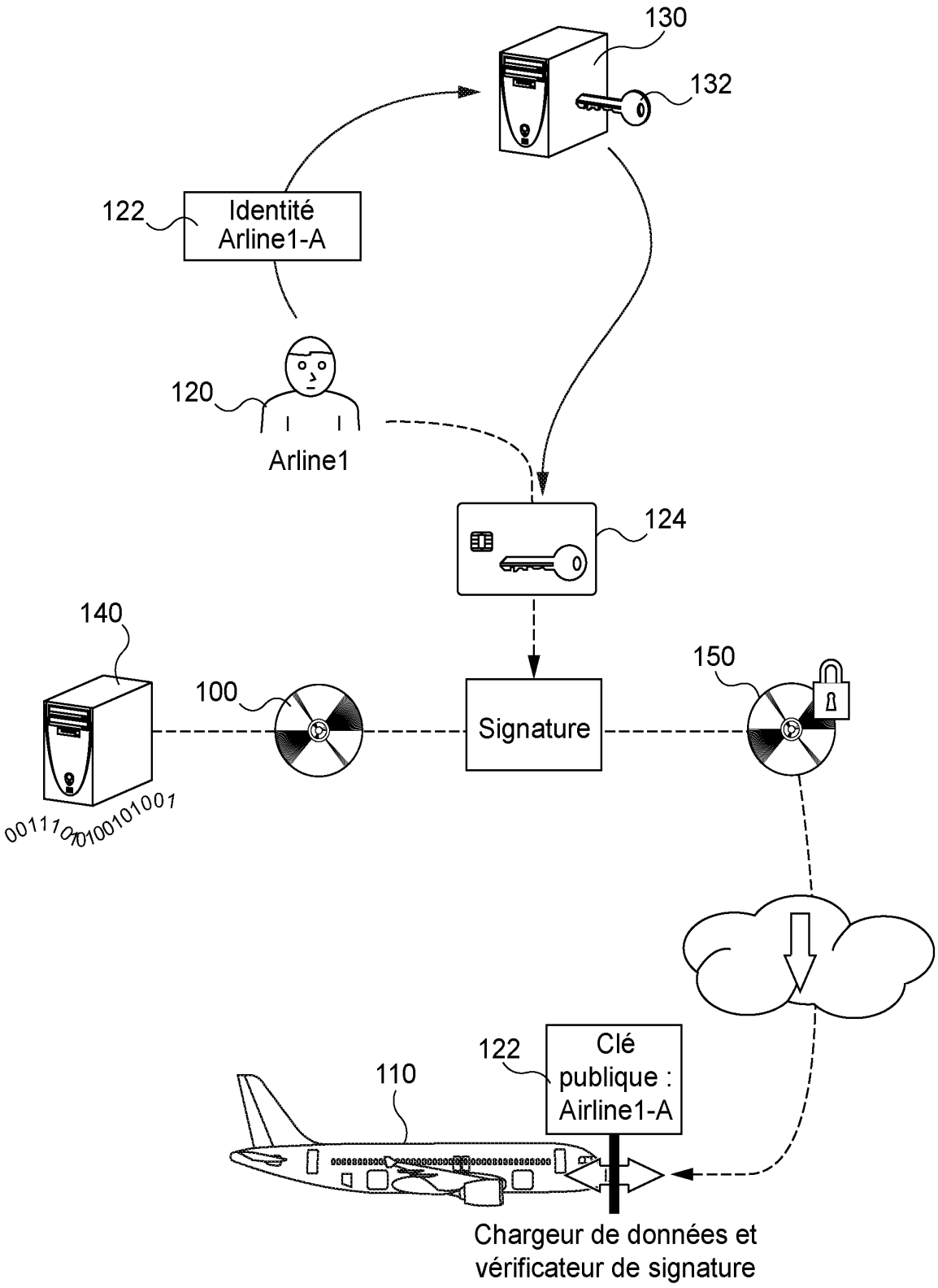

130
132
122
Identité
Arline1-A
120
Arline1
124
140
100
Signature
150
00111010100101001
122
Clé
publique :
Airline1-A
110
Chargeur de données et
vérificateur de signature

Fig. 1

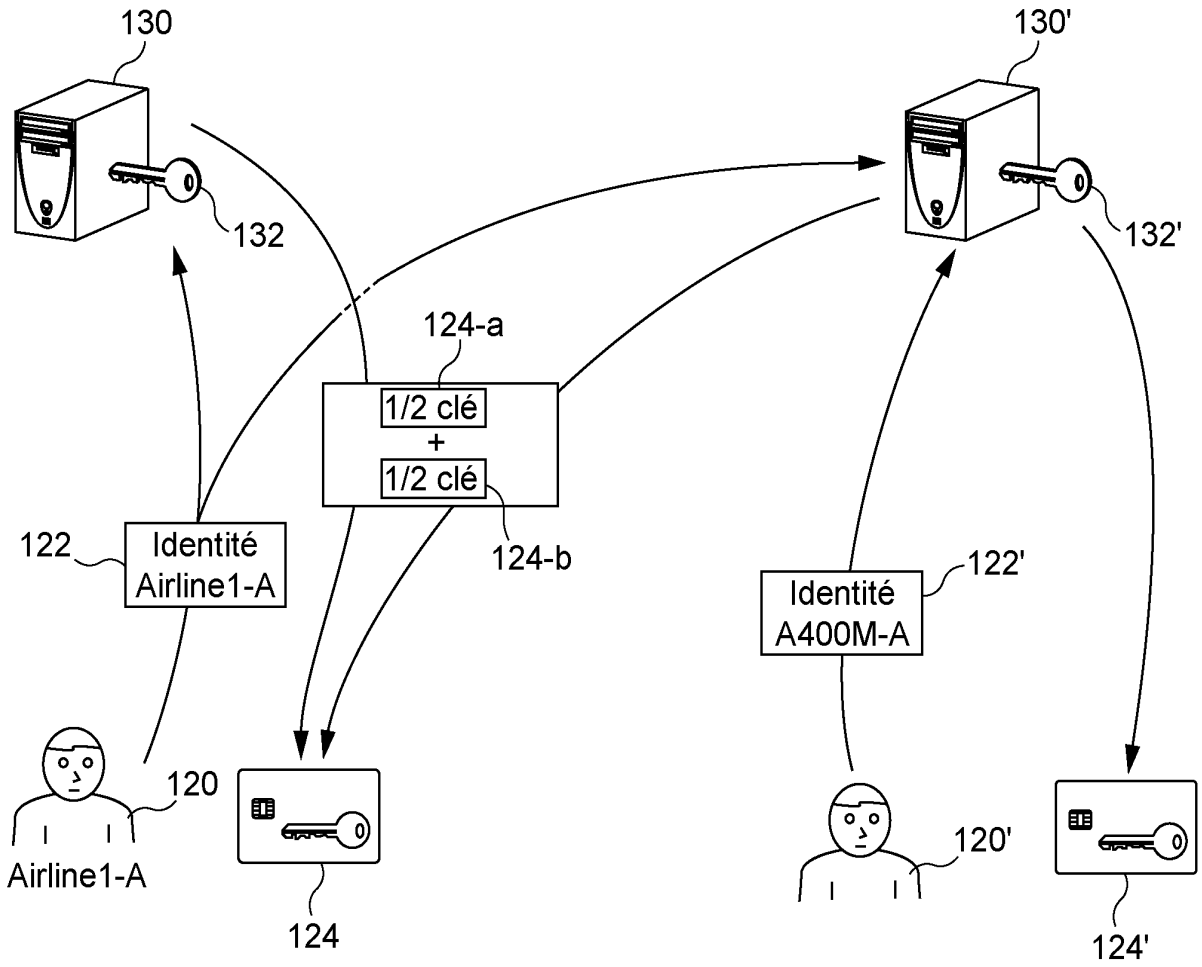

130
130'
132
132'
124-a
1/2 clé
+
1/2 clé
124-b
122
Identité
Airline1-A
Identité
A400M-A
122'
120
Airline1-A
120'
124
124'

Fig. 2

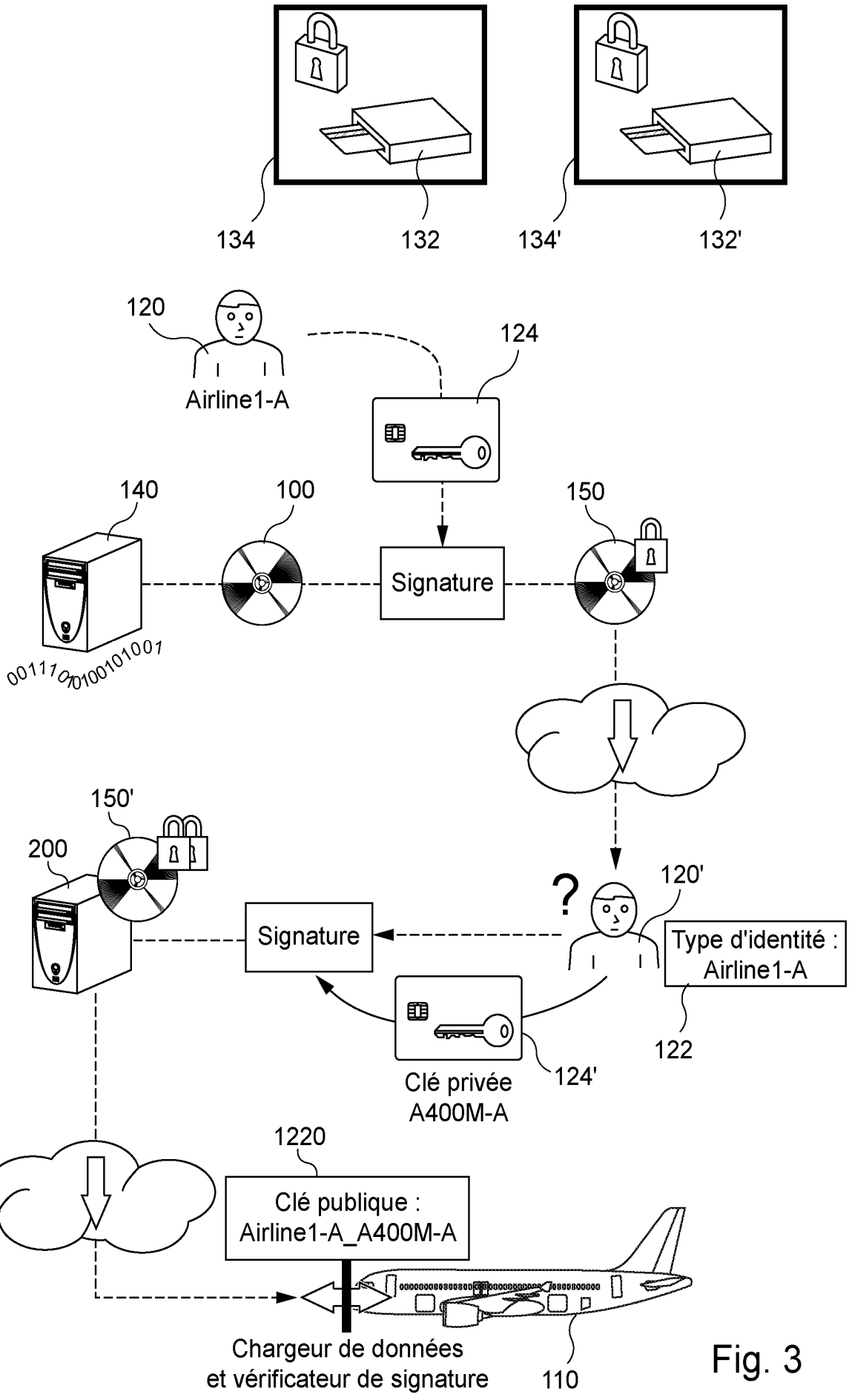

134
132
134'
132'
120
Airline1-A
124
140
100
150
Signature
00111010100101001
150'
200
120'
?
Signature
Type d'identité :
Airline1-A
122
Clé privée
A400M-A
124'
1220
Clé publique :
Airline1-A_A400M-A
Chargeur de données
et vérificateur de signature
110

Fig. 3

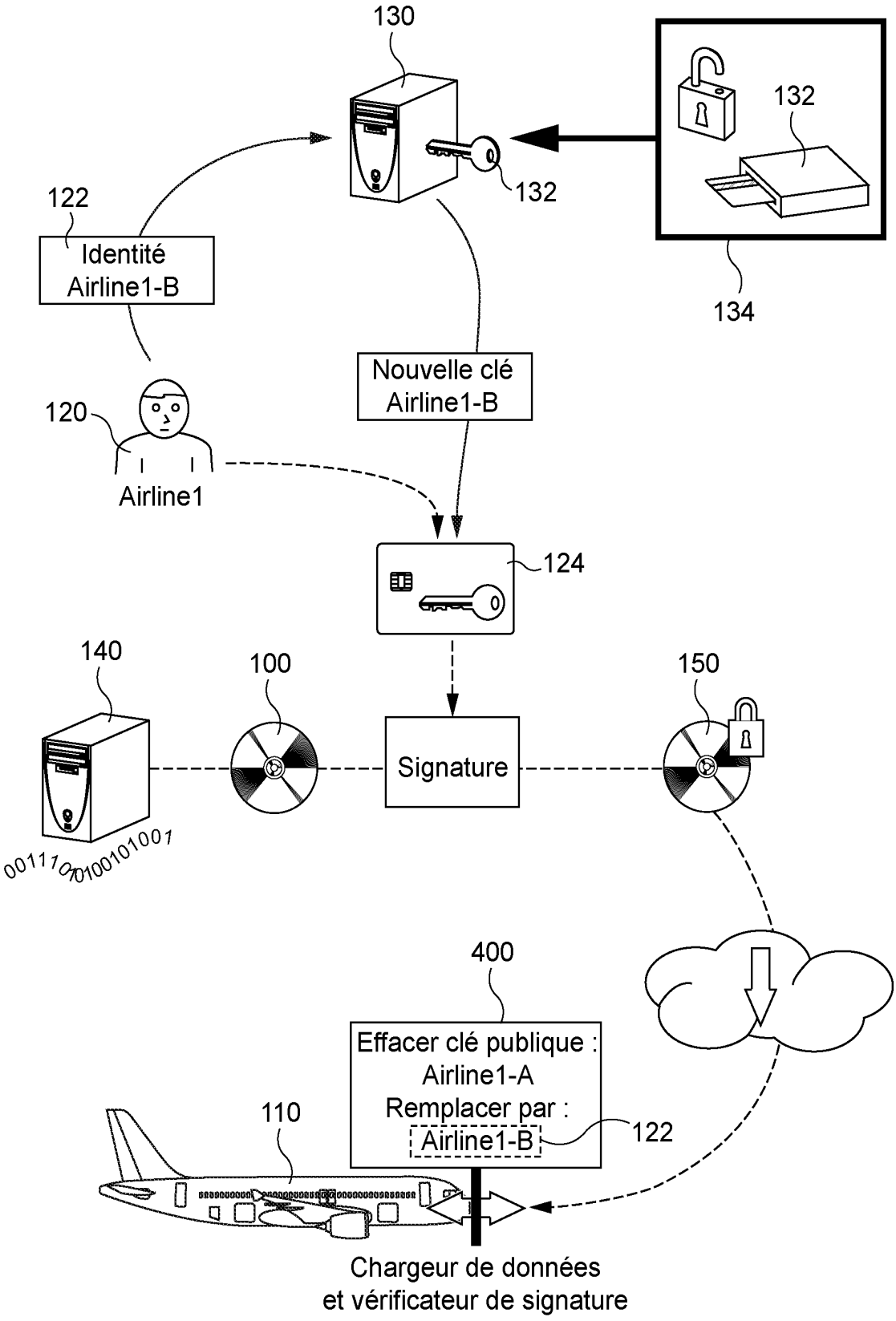

130
132
132
134
122
Identité
Airline1-B
Nouvelle clé
Airline1-B
120
Airline1
124
140
100
150
Signature
00111010100101001
400
Effacer clé publique :
Airline1-A
Remplacer par :
Airline1-B
122
110
Chargeur de données
et vérificateur de signature

Fig. 4

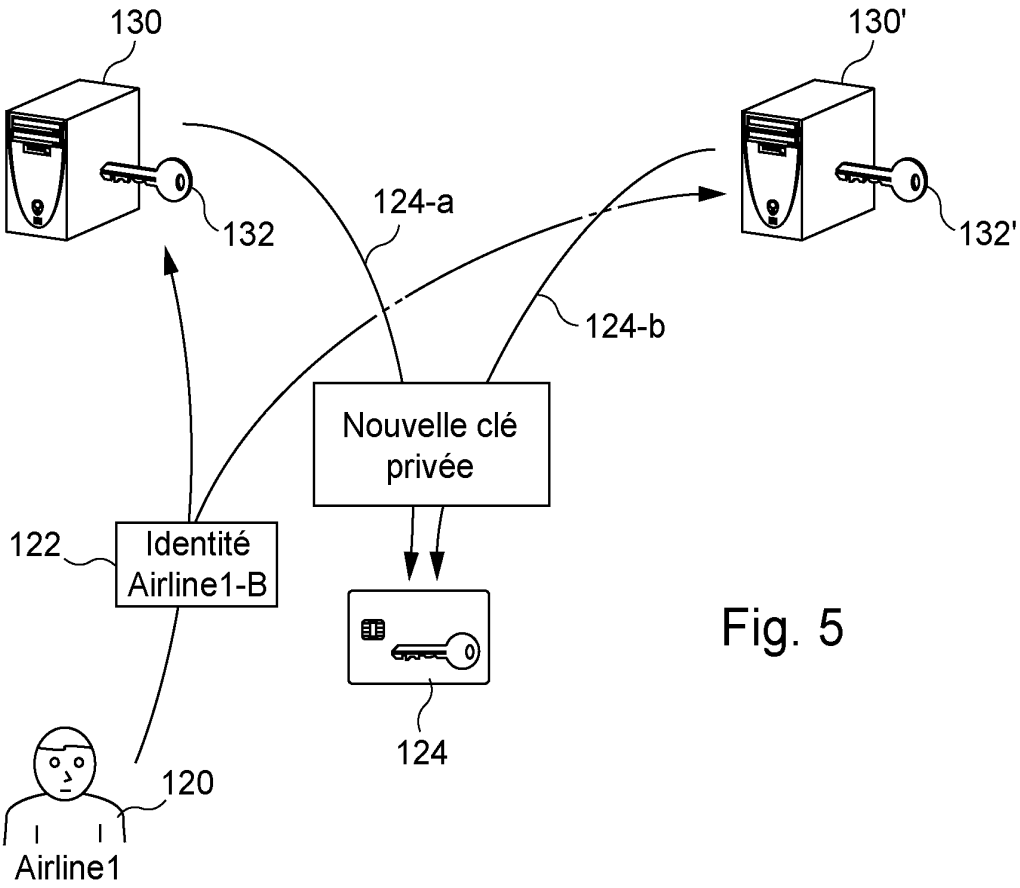

130
130'
132
132'
124-a
124-b
Nouvelle clé privée
122
Identité Airline1-B
124
120
Airline1

Fig. 5

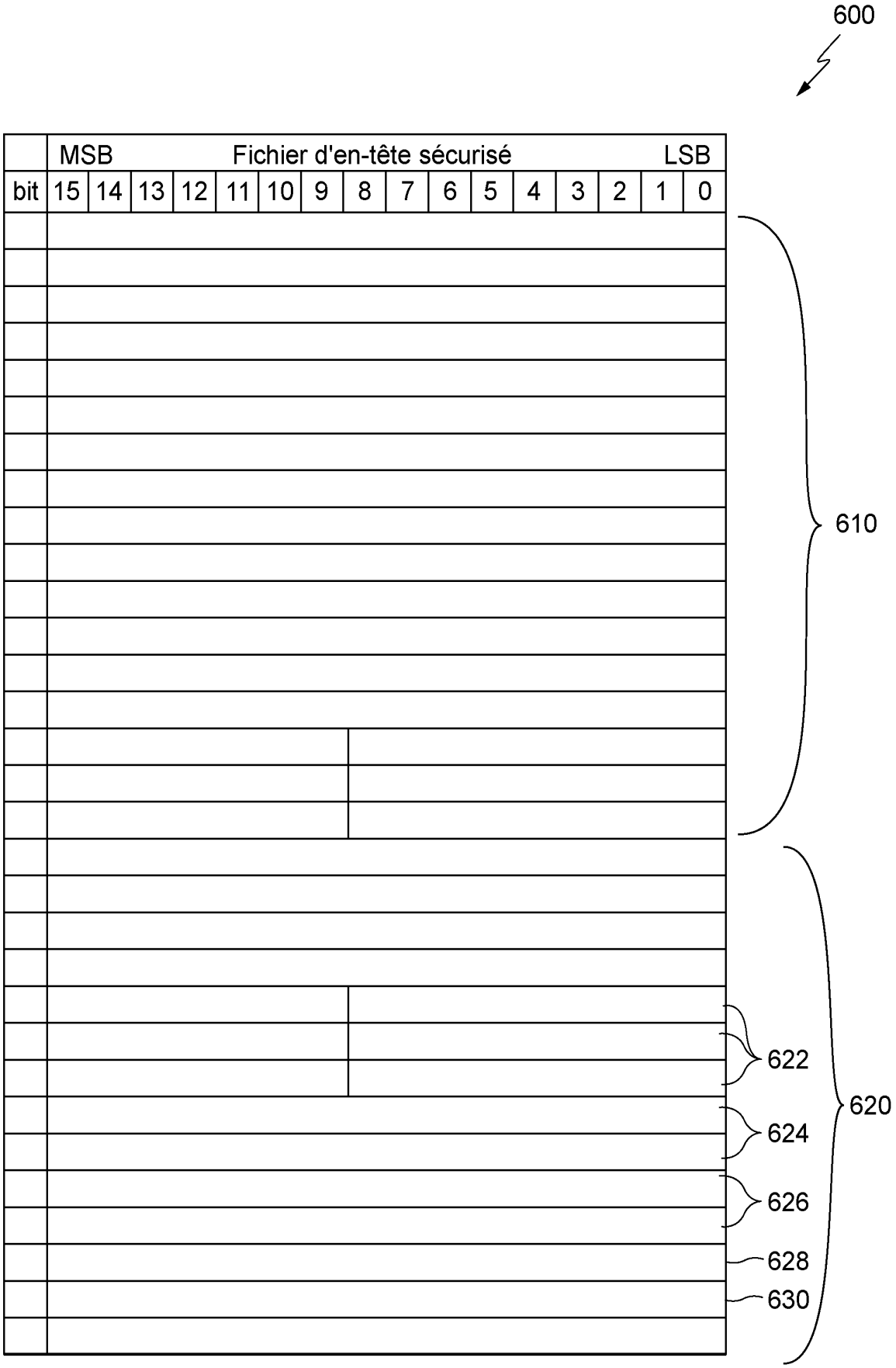

600
MSB
Fichier d'en-tête sécurisé
LSB
bit
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
610
620
622
624
626
628
630

Fig. 6

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 701655
FR 0758392

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	RICHARD ROBINSON ET AL: "Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety" COMPUTER SAFETY, RELIABILITY, AND SECURITY LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER BERLIN HEIDELBERG, BE, vol. 4680, 1 janvier 1900 (1900-01-01), pages 28-39, XP019071851 ISBN: 978-3-540-75100-7 * page 33, ligne 37 - page 35, ligne 33 * -----	1-10	H04L9/28
Y	LIHUA WANG ET AL: "ID-Based Series-Parallel Multisignature Schemes for Multi-Messages from Bilinear Maps" CODING AND CRYPTOGRAPHY LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER BERLIN HEIDELBERG, BE, vol. 3969, 1 janvier 2006 (2006-01-01), pages 291-303, XP019049466 ISBN: 978-3-540-35481-9 * page 294, ligne 33 - page 298, ligne 7 * -----	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC)
Y	OIKONOMIDIS N ET AL: "Identity based protocols for secure electronic content distribution and licensing" WEB DELIVERING OF MUSIC, 2004. WEDELMUSIC 2004. PROCEEDINGS OF THE FOU RTH INTERNATIONAL CONFERENCE ON BARCELONA, SPAIN 13-14 SEPT. 2004, PISCATAWAY, NJ, USA,IEEE, 13 septembre 2004 (2004-09-13), pages 92-100, XP010741623 ISBN: 978-0-7695-2157-2 * page 3, colonne de gauche, ligne 25 - page 5, colonne de droite, ligne 54 * ----- -/--	3	H04L G06F

Date d'achèvement de la recherche	Examinateur
25 juin 2008	Cretaine, Philippe

CATÉGORIE DES DOCUMENTS CITÉS

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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 701655
FR 0758392

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 2005/198517 A1 (IVANOV LAZAR I [US] ET AL IVANOV LAZAR IVANOV [US] ET AL) 8 septembre 2005 (2005-09-08) * alinéas [0045], [0066] *	1-10	
A	EP 0 686 906 A (SUN MICROSYSTEMS INC [US]) 13 décembre 1995 (1995-12-13) * abrégé *	1-10	
A	EP 1 380 917 A (HEWLETT PACKARD DEVELOPMENT CO [US]) 14 janvier 2004 (2004-01-14) * abrégé *	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
25 juin 2008	Cretaine, Philippe

CATÉGORIE DES DOCUMENTS CITÉS

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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0758392 FA 701655

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 25-06-2008
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2005198517 A1	08-09-2005	AUCUN	
EP 0686906 A	13-12-1995	DE 69534212 D1	23-06-2005
		DE 69534212 T2	12-01-2006
		JP 8166879 A	25-06-1996
		US 5724425 A	03-03-1998
EP 1380917 A	14-01-2004	GB 2390786 A	14-01-2004
		US 2004010700 A1	15-01-2004

EPO FORM P0465