(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 943 870**

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

(21) **N° d'enregistrement national :** **09 01441**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2006.01), H 04 L 29/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26.03.09.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.10.10 Bulletin 10/39.

(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) :** *TRUSTSEED Société à responsabilité limitée* — FR.

(72) **Inventeur(s) :** BLOT-LEFEVRE ERIC.

(73) **Titulaire(s) :** TRUSTSEED Société à responsabilité limitée.

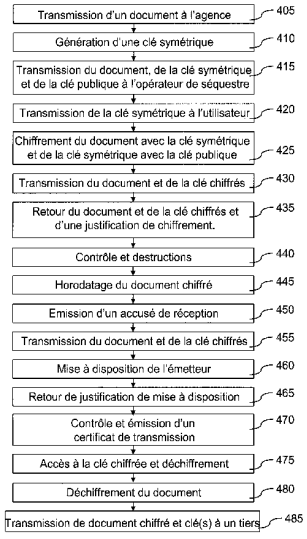
(74) **Mandataire(s) :** MARKS & CLERK FRANCE.

(54) PROCEDE ET DISPOSITIF DE CHIFFREMENT D'UN DOCUMENT.

(57) Le procédé de chiffrement d'un document comporte:
- une étape (405) de réception du document,
- une étape (425) de chiffrement du document avec une clé symétrique,
- une étape (425) de chiffrement de la clé symétrique avec une clé d'un biclés de clés asymétriques et
- une étape (430) de transmission du document chiffré et de la clé symétrique chiffrée.

Dans des modes de réalisation, le procédé comporte une étape de génération de ladite clé symétrique pour chaque document à chiffrer.

Selon qu'il est appliqué à l'archivage personnel ou à la transmission de document, au cours de l'étape de chiffrement avec la clé asymétrique, la clé asymétrique est celle de l'utilisateur ayant transmis ledit document ou celle du destinataire du document.



FR 2 943 870 - A1

PROCEDE ET DISPOSITIF DE CHIFFREMENT D'UN DOCUMENT

La présente invention concerne un procédé et un dispositif de chiffrement d'un document. Elle s'applique, en particulier, à l'archivage confidentiel ou secret de documents pour récupération ultérieure par leur propriétaire légitime et à la transmission confidentielle de documents à un destinataire.

On connaît de nombreuses méthodes de chiffrement, à clés symétriques ou à bi-clés asymétriques (par exemple conformes à l'infrastructure à clés publiques PKI, acronyme de « Public Key Infrastructure »). Cependant, ces méthodes de chiffrement ne sont pas adaptées à assurer, à la fois, un haut niveau de sécurité des documents et une possibilité de récupération des documents si les clés sont perdues (par exemple, en cas de décès de leur propriétaire ou de décision judiciaire visant à les récupérer).

La présente invention vise à remédier à ces inconvénients.

A cet effet, selon un premier aspect, la présente invention vise un procédé de chiffrement d'un document, caractérisé en ce qu'il comporte :

- une étape de réception du document,
- une étape de chiffrement du document avec une clé symétrique,
- une étape de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques et
- une étape de transmission du document chiffré et de la clé symétrique chiffrée.

Selon des caractéristiques particulières, le procédé de chiffrement objet de la présente invention comporte une étape de génération de ladite clé symétrique pour chaque document à chiffrer.

Selon des caractéristiques particulières, au cours de l'étape de chiffrement avec la clé asymétrique, ladite clé asymétrique est la clé publique de l'utilisateur ayant transmis ledit document.

Selon des caractéristiques particulières, au cours de l'étape de chiffrement avec la clé asymétrique, ladite clé asymétrique est la clé publique d'un utilisateur destinataire du document.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus, comporte une étape d'effacement du document chiffré et de conservation de la clé symétrique par le système informatique effectuant les étapes de chiffrement.

Selon un deuxième aspect, la présente invention vise un dispositif de chiffrement d'un document, caractérisé en ce qu'il comporte :

- un moyen de réception du document,
- un moyen de chiffrement du document avec une clé symétrique,
- un moyen de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques et
- un moyen de transmission du document chiffré et de la clé symétrique chiffrée.

Selon des caractéristiques particulières, le dispositif objet de la présente invention, tel que succinctement exposé ci-dessus, comporte un moyen de génération de ladite clé symétrique pour chaque document à chiffrer.

Selon des caractéristiques particulières, le moyen de chiffrement avec la clé asymétrique est adapté à ce que ladite clé asymétrique soit la clé publique de l'utilisateur ayant transmis ledit document.

Selon des caractéristiques particulières, le moyen de chiffrement avec la clé asymétrique est adapté à ce que ladite clé asymétrique soit la clé publique d'un utilisateur destinataire du document.

Selon des caractéristiques particulières, le dispositif objet de la présente invention, tel que succinctement exposé ci-dessus, comporte un moyen d'effacement du document chiffré et de conservation de la clé symétrique par le système informatique comportant les moyens de chiffrement.

Les avantages, buts et caractéristiques particulières de ce dispositif étant similaires à ceux du procédé objet de la présente invention, tel que succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre faite, dans un but explicatif et nullement limitatif, en regard des dessins annexés, dans lesquels :

- la figure 1 représente, schématiquement, un premier mode de réalisation particulier d'un dispositif objet de la présente invention adapté au cas dans lequel l'émetteur est aussi le destinataire du document traité,

- la figure 2 représente, sous forme d'un logigramme, un premier mode de réalisation particulier du procédé objet de la présente invention adapté à une transmission d'un document, adapté au cas dans lequel l'émetteur est aussi le destinataire du document traité et ne dispose pas d'un bi-clés personnel,
- la figure 3 représente, schématiquement, un deuxième mode de réalisation particulier d'un dispositif objet de la présente invention, adapté au cas dans lequel l'émetteur et le destinataire du document traité sont distincts,
- la figure 4 représente, sous forme d'un logigramme, un deuxième mode de réalisation particulier du procédé objet de la présente invention adapté à un archivage personnel d'un document, adapté au cas dans lequel ni l'émetteur, ni le destinataire ne disposent d'un bi-clés personnel,
- la figure 5 représente, sous forme d'un logigramme, un troisième mode de réalisation particulier du procédé objet de la présente invention adapté à une transmission d'un document, adapté au cas dans lequel l'émetteur est aussi le destinataire et dispose d'un bi-clés personnel et
- la figure 6 représente, sous forme d'un logigramme, un quatrième mode de réalisation particulier du procédé objet de la présente invention adapté à un archivage personnel d'un document adapté au cas dans lequel l'émetteur et le destinataires disposent d'un bi-clés personnel.

On observe, en figure 1, une agence/autorité d'ordonnancement et de certification 105, un opérateur de séquestre 110, un opérateur de transmission 120 et un opérateur d'archivage 145. Un premier utilisateur, aussi appelé par la suite utilisateur « émetteur », met en œuvre un terminal 125 pour interagir avec l'agence 105.

L'agence/autorité d'ordonnancement et de certification 105, l'opérateur de séquestre 110, l'opérateur de transmission 120 et l'opérateur d'archivage 145 mettent, généralement, en oeuvre des serveurs (non représentés) qui communiquent, entre eux, par l'intermédiaire de réseaux informatiques (non représentés), par exemple, le réseau Internet.

Pour chaque archivage ou transmission de document, il est, conformément à la présente invention, fait usage d'une clé symétrique. Cette clé symétrique est, préférentiellement, attribuée à l'utilisateur émetteur pour chaque document qu'il archive ou transmet.

Comme on l'observe en figure 2, pour effectuer un archivage chiffré d'un document lorsque l'émetteur ne dispose pas d'un bi-clés, le terminal 125 transmet ce document non chiffré, à l'agence d'ordonnancement et de certification 105, au cours d'une étape 205.

Au cours d'une étape 210, l'agence 105 génère une clé de chiffrement symétrique. En variante, c'est le terminal 125 de l'utilisateur émetteur qui fournit cette clé de chiffrement symétrique à l'agence 105.

Puis, au cours d'une étape 215, l'agence 105 transmet le document et la clé symétrique à l'opérateur de séquestre 110. Au cours d'une étape 220, l'agence 105 transmet cette clé symétrique au bureau privé de gestion « BPG » de l'utilisateur émetteur. Le bureau privé de gestion est un espace mis à disposition d'un utilisateur par un Fournisseur d'Application Communautaire, ici confondu avec l'agence 105, et protégé au moins par un nom d'utilisateur et un mot de passe connus de ce seul utilisateur.

Au cours d'une étape 225, l'opérateur de séquestre 110 effectue le chiffrement du document avec la clé symétrique reçue au cours de l'étape 215. Au cours d'une étape 230, l'opérateur de séquestre 110 conserve la clé symétrique et transmet le document, chiffré avec la clé symétrique, à l'opérateur d'archivage qui effectue un second chiffrement, avec sa propre clé privée, du document déjà chiffré avec la clé symétrique et conserve le document doublement chiffré.

Au cours d'une étape 235, l'opérateur de séquestre retourne à l'agence 105 le document chiffré avec la clé symétrique et une justification de liste récapitulative de chiffrement, qui justifie de la réalisation de toutes les étapes prévues pour réaliser les chiffrements.

Au cours d'une étape 240, l'agence 105 contrôle la justification de chiffrement, détruit le document non chiffré et la clé symétrique et fait détruire le document non chiffré conservé par le tiers de séquestre 110.

Au cours d'une étape 245, l'agence 105 effectue un horodatage du document chiffré et de la justification de chiffrement.

Au cours d'une étape 250, l'agence 105 émet une accusé de réception et de certification horodaté de chiffrement à l'opérateur de séquestre 110 et l'opérateur de séquestre 110 conserve cet accusé de réception et de certification ainsi que la clé symétrique de l'utilisateur émetteur mais détruit le document chiffré.

Au cours d'une étape 255, l'agence 105 transmet le document chiffré à l'opérateur de transmission 120. Au cours d'une étape 260, l'opérateur de transmission 120 met le document chiffré dans le compte courant de correspondance de l'émetteur. Au cours d'une étape 265, l'opérateur de transmission 120 retourne à l'agence 105, par l'intermédiaire du tiers de confiance 115, une justification de liste récapitulative du placement du document chiffré en compte courant de correspondance de l'émetteur. Cette justification représente la bonne réalisation de toutes les étapes liées au placement du document chiffré dans le compte courant de correspondance de l'utilisateur émetteur.

Au cours d'une étape 270, l'agence 105 transmet à l'opérateur de transmission 120 un certificat de transmission horodaté.

Pour relire le document, au cours d'une étape 275, l'émetteur accède à la clé symétrique et, au cours d'une étape 280, l'émetteur déchiffre le document chiffré. Les étapes 275 et 280 sont éventuellement réalisées par l'intermédiaire du tiers de séquestre avec horodatage et transmission à l'agence 105 d'une justification de liste récapitulative de déchiffrement.

En cas de besoin, par exemple pour des opérations d'instruction judiciaire et/ou sur commission rogatoire, au cours d'une étape 285, la clé symétrique conservée par l'opérateur de séquestre et le document chiffré conservé par l'opérateur d'archivage sont transmis à un tiers qui déchiffre le document chiffré avec cette clé symétrique.

Ainsi, dans le cas de l'archivage personnel (l'émetteur et le destinataire du document sont confondus) dans lequel l'émetteur ne dispose pas de bi-clés, le document est chiffré avec une clé symétrique exclusivement affectée à ce document. La clé symétrique ayant servi à chiffrer le document reste chez le tiers séquestre et est conservée par l'émetteur du document dans son bureau privé de gestion.

Le document chiffré par la clé symétrique chez le tiers séquestre est envoyé au tiers d'archivage (par exemple un Opérateur Tiers de Confiance) qui effectue un second chiffrement avec sa clé privée pour l'archivage légal.

Si l'émetteur veut déchiffrer et consulter en clair son document, il peut le faire de son bureau privé de gestion, qui est sécurisé. Soit il a conservé, dans ce bureau privé de gestion, la clé symétrique reçue au cours de l'étape 220 et le document chiffré disponible dans son compte courant de correspondance et le déchiffrement se fait simplement dans son bureau privé de gestion, sur la base de ces deux éléments.

Soit, le tiers d'archivage envoie le document déchiffré avec sa clé publique mais encore chiffré avec la clé symétrique, au Fournisseur d'Application Communautaire qui gère le bureau de gestion privé de l'émetteur. Ainsi, l'émetteur peut déchiffrer le document, en effectuant, un déchiffrement avec la clé symétrique associée à ce document, dans son bureau privé de gestion.

En variante, le tiers d'archivage envoie le document doublement chiffré au Fournisseur d'Application Communautaire. Ainsi, l'émetteur peut déchiffrer le document, en effectuant, d'abord un déchiffrement avec la clé publique de l'Opérateur Tiers de Confiance puis avec la clé symétrique détenue dans son bureau pour ce document déchiffrer le document.

En cas de commission rogatoire ou de procédure notariale (décès, tutelle, ...), il est toujours possible de demander au tiers séquestre de déchiffrer le document sans intervention de l'émetteur du document. En effet, comme on l'a vu, le tiers séquestre dispose d'une clé symétrique dédiée au document suffisante pour le déchiffrer.

On observe, en figure 3, une agence/autorité d'ordonnancement et de certification 105, un opérateur de séquestre 110, un opérateur de transmission 120, et un opérateur d'archivage 145. Un premier utilisateur, aussi appelé par la suite utilisateur « émetteur », met en œuvre un terminal 125 pour interagir avec l'agence 105. Un deuxième utilisateur, aussi appelé par la suite utilisateur « destinataire », met en œuvre un terminal 130 pour interagir avec l'opérateur de transmission 120.

On note que, en figures 4 et 6, il a été considéré que l'émetteur et le destinataire étaient liés au même opérateur de transmission et à la même agence. Au cas où ils seraient liés à des opérateurs et agences différents, les étapes concernant les documents chiffrés mentionnées dans ces figures, pour l'opérateur de transmission et pour l'agence, seraient effectuées, en parallèle et séparément, par les deux opérateurs et deux agences concernés.

Comme on l'observe en figure 4, pour effectuer une transmission chiffrée d'un document depuis un émetteur à un destinataire, le terminal 125 transmet ce document non chiffré, à l'agence d'ordonnancement et de certification 105, au cours d'une étape 305.

Au cours d'une étape 310, l'agence 105 génère deux clés de chiffrement symétriques différentes destinées, respectivement, à l'émetteur et au destinataire.

Puis, au cours d'une étape 315, l'agence 105 transmet le document et les clés symétriques à l'opérateur de séquestre 110. Au cours d'une étape 320, l'agence 105 transmet la clé symétrique de l'émetteur au bureau privé de gestion « BPG » de l'utilisateur émetteur et la clé symétrique de l'émetteur destinataire au bureau privé de gestion du destinataire.

Au cours d'une étape 325, l'opérateur de séquestre 110 effectue les chiffrements du document avec chacune des clés symétriques reçues au cours de l'étape 315. Au cours d'une étape 330, l'opérateur de séquestre 110 conserve les clés symétriques et transmet les documents, chiffrés avec les clés symétriques, à l'opérateur d'archivage qui effectue un second chiffrement, avec sa propre clé privée, des documents déjà chiffrés avec les clés symétriques et conserve les documents doublement chiffrés.

Au cours d'une étape 335, l'opérateur de séquestre retourne à l'agence 105 les documents chiffrés avec les clés symétriques et une justification de liste récapitulative de chiffrement, qui justifie de la réalisation de toutes les étapes prévues pour réaliser les chiffrements.

Au cours d'une étape 340, l'agence 105 contrôle la justification de chiffrement, détruit le document non chiffré et les clés symétriques et fait détruire le document non chiffré conservé par le tiers de séquestre 110.

Au cours d'une étape 345, l'agence 105 effectue un horodatage du document chiffré et de la justification de chiffrement.

Au cours d'une étape 350, l'agence 105 émet une accusé de réception et de certification horodaté de chiffrement à l'opérateur de séquestre 110 et l'opérateur de séquestre 110 conserve cet accusé de réception et de certification ainsi que les clés symétriques mais détruit les documents chiffrés.

Au cours d'une étape 355, l'agence 105 transmet les documents chiffrés à l'opérateur de transmission 120. Au cours d'une étape 360, l'opérateur de transmission 120 met le document chiffré avec la clé symétrique de l'émetteur dans le compte courant de correspondance de l'émetteur. Au cours de l'étape 360, l'opérateur de transmission 120 met aussi le document chiffré avec la clé symétrique du destinataire dans le compte courant de correspondance du destinataire. Au cours d'une étape 365, l'opérateur de transmission 120 retourne à l'agence 105, par l'intermédiaire du tiers de confiance 115, une justification de liste récapitulative du placement des documents chiffrés en comptes courants de correspondance. Cette

justification représente la bonne réalisation de toutes les étapes liées au placement des documents chiffrés dans les comptes courants de correspondance.

Au cours d'une étape 370, l'agence 105 transmet à l'opérateur de transmission 120 un certificat de transmission horodaté.

Pour relire le document, au cours d'une étape 375, l'émetteur accède à sa clé symétrique et déchiffre le document chiffré. L'étape 375 est éventuellement réalisée par l'intermédiaire du tiers de séquestre avec horodatage et transmission à l'agence 105 d'une justification de liste récapitulative de déchiffrement.

Pour lire le document, au cours d'une étape 380, le destinataire accède à sa clé symétrique, par l'intermédiaire du tiers de séquestre, et au document chiffré, et déchiffre le document chiffré. A la fin de cette opération, sont effectués un horodatage et une transmission à l'agence 105 d'une justification de liste récapitulative de déchiffrement.

En cas de besoin, par exemple pour des opérations d'instruction judiciaire et/ou sur commission rogatoire, au cours d'une étape 385, l'une des clés symétriques conservées par l'opérateur de séquestre et le document chiffré correspondant conservé par l'opérateur d'archivage sont transmis à un tiers qui déchiffre le document chiffré avec la clé symétrique.

En variante du mode de réalisation illustré en figure 4, les deux clés symétriques sont identiques.

Comme on l'observe en figure 5, pour effectuer un archivage chiffré d'un document lorsque l'émetteur dispose d'un bi-clés, le terminal 125 transmet ce document non chiffré, à l'agence d'ordonnancement et de certification 105, au cours d'une étape 405.

Au cours d'une étape 410, l'agence 105 génère une clé de chiffrement symétrique. En variante, c'est le terminal 125 de l'utilisateur émetteur qui fournit cette clé de chiffrement symétrique à l'agence 105.

Puis, au cours d'une étape 415, l'agence 105 transmet le document, la clé symétrique et la clé publique de l'émetteur à l'opérateur de séquestre 110. Au cours d'une étape 420, l'agence 105 transmet cette clé symétrique au bureau privé de gestion « BPG » de l'utilisateur émetteur.

Au cours d'une étape 425, l'opérateur de séquestre 110 effectue le chiffrement du document avec la clé symétrique reçue au cours de l'étape 415 et le chiffrement de la clé symétrique avec la clé publique de l'émetteur. Au cours d'une étape 430,

l'opérateur de séquestre 110 conserve la clé symétrique et transmet le document, chiffré avec la clé symétrique et la clé symétrique chiffrée avec la clé publique de l'émetteur, à l'opérateur d'archivage qui effectue un troisième chiffrement, avec sa propre clé privée, du document déjà chiffré avec la clé symétrique et de la clé symétrique chiffrée avec la clé publique de l'émetteur et conserve le document doublement chiffré et la clé doublement chiffrée.

Au cours d'une étape 435, l'opérateur de séquestre retourne à l'agence 105 le document chiffré avec la clé symétrique, la clé symétrique chiffrée avec la clé publique de l'émetteur et une justification de liste récapitulative de chiffrement, qui justifie de la réalisation de toutes les étapes prévues pour réaliser les chiffrements.

Au cours d'une étape 440, l'agence 105 contrôle la justification de chiffrement, détruit le document non chiffré et la clé symétrique et fait détruire le document non chiffré conservé par le tiers de séquestre 110.

Au cours d'une étape 445, l'agence 105 effectue un horodatage du document chiffré et de la justification de chiffrement.

Au cours d'une étape 450, l'agence 105 émet une accusé de réception et de certification horodaté de chiffrement à l'opérateur de séquestre 110 et l'opérateur de séquestre 110 conserve cet accusé de réception et de certification ainsi que la clé symétrique de l'utilisateur émetteur chiffrée mais détruit le document chiffré et la clé symétrique non chiffrée.

Au cours d'une étape 455, l'agence 105 transmet le document chiffré et la clé symétrique chiffrée à l'opérateur de transmission 120. Au cours d'une étape 460, l'opérateur de transmission 120 met le document chiffré et la clé symétrique chiffrée dans le compte courant de correspondance de l'émetteur. Au cours d'une étape 465, l'opérateur de transmission 120 retourne à l'agence 105, par l'intermédiaire du tiers de confiance 115, une justification de liste récapitulative du placement du document chiffré et de la clé symétrique chiffrée en compte courant de correspondance de l'émetteur. Cette justification représente la bonne réalisation de toutes les étapes liées au placement du document chiffré et de la clé symétrique chiffrée dans le compte courant de correspondance de l'utilisateur émetteur.

Au cours d'une étape 470, l'agence 105 transmet à l'opérateur de transmission 120 un certificat de transmission horodaté.

Pour relire le document, au cours d'une étape 475, l'émetteur accède à la clé symétrique chiffrée, la déchiffre avec sa clé privée et, au cours d'une étape 480,

l'émetteur déchiffre le document chiffré. Les étapes 475 et 480 sont éventuellement réalisées par l'intermédiaire du tiers de séquestre avec horodatage et transmission à l'agence 105 d'une justification de liste récapitulative de déchiffrement.

En cas de besoin, par exemple pour des opérations d'instruction judiciaire et/ou sur commission rogatoire, au cours d'une étape 485, la clé symétrique chiffrée conservée par l'opérateur de séquestre, le document chiffré conservé par l'opérateur d'archivage et la clé privée conservée par un tiers de confiance (non représenté) sont transmis à un tiers qui déchiffre le document chiffré avec cette clé symétrique après avoir déchiffré la clé symétrique avec la clé privée de l'émetteur.

En variante, au cours de l'étape 450, la clé symétrique non chiffrée est conservée par l'opérateur de séquestre et, au cours de l'étape 485, l'opérateur de séquestre transmet cette clé symétrique non chiffrée au tiers chargé du déchiffrement.

On note que l'émetteur peut consulter le document de deux manières.

Soit il demande au tiers d'archivage de rapatrier dans son bureau privé de gestion uniquement le document chiffré avec la clé symétrique dont il détient le double dans ce même bureau. Avec la deuxième clé symétrique, il peut lire le document chiffré dans son bureau privé de gestion.

L'émetteur peut aussi demander au tiers d'archivage de transférer sur son poste de travail l'ensemble du document chiffré par la clé symétrique, et la clé symétrique chiffrée par sa clé publique. A réception du lot de ces deux éléments chiffrés, il commence par déchiffrer la clé symétrique avec sa clé privée personnelle. Ensuite, il utilise la clé symétrique déchiffrée pour déchiffrer le document chiffré.

Il existe aussi, pour le Coffre Fort Citoyen, une autre possibilité qui est de faire conserver, par l'opérateur de séquestre et non par le bureau privé de gestion de l'émetteur, la clé symétrique. Cependant, dans ce cas, l'émetteur ne peut utiliser son bureau privé de gestion pour déchiffrer le document puisqu'il ne dispose pas de la clé symétrique nécessaire. Par contre, il peut demander le transfert du document chiffré et de la clé symétrique chiffrée sur son poste de travail pour déchiffrer le tout en utilisant d'abord sa clé privée pour déchiffrer la clé symétrique servant à déchiffrer le document.

Cette option est préférentiellement retenue dans l'hypothèse où l'adhérent a une carte nationale d'identité numérique fonctionnant avec un coffre fort électronique citoyen.

Comme on l'observe en figure 6, pour effectuer une transmission chiffrée d'un document à un destinataire, lorsque l'émetteur et le destinataires disposent de bi-clés, le terminal 125 transmet le document non chiffré, à l'agence d'ordonnancement et de certification 105, au cours d'une étape 505.

Au cours d'une étape 510, l'agence 105 génère deux clés de chiffrement symétriques destinées, respectivement, à l'émetteur et au destinataire. En variante, c'est le terminal 125 de l'utilisateur émetteur qui fournit ces clés de chiffrement symétriques à l'agence 105.

Puis, au cours d'une étape 515, l'agence 105 transmet le document, les clés symétriques et les clés publiques de l'émetteur et du destinataire à l'opérateur de séquestre 110. Au cours d'une étape 520, l'agence 105 transmet ces clés symétriques aux bureaux privés de gestion « BPG », respectivement de l'émetteur et du destinataire.

Au cours d'une étape 525, l'opérateur de séquestre 110 effectue le chiffrement du document avec chaque clé symétrique reçue au cours de l'étape 515 et le chiffrement des clés symétriques avec les clés publiques respectivement de l'émetteur et du destinataire. Au cours d'une étape 530, l'opérateur de séquestre 110 conserve les clés symétriques et transmet les documents chiffrés avec les clés symétriques et les clés symétriques chiffrées avec les clés publiques de l'émetteur et du destinataire, à l'opérateur d'archivage qui effectue un troisième chiffrement, avec sa propre clé privée, des documents déjà chiffrés avec les clés symétriques et des clés symétriques chiffrées avec les clés publiques et conserve les documents doublement chiffrés et les clés doublement chiffrées.

Au cours d'une étape 535, l'opérateur de séquestre retourne à l'agence 105 les documents chiffrés avec les clés symétriques, les clés symétriques chiffrées avec les clés publiques des utilisateurs et une justification de liste récapitulative de chiffrement, qui justifie de la réalisation de toutes les étapes prévues pour réaliser les chiffrements.

Au cours d'une étape 540, l'agence 105 contrôle la justification de chiffrement, détruit le document non chiffré et les clés symétriques.

Au cours d'une étape 545, l'agence 105 effectue un horodatage des documents chiffrés et de la justification de chiffrement.

Au cours d'une étape 550, l'agence 105 émet une accusé de réception et de certification horodaté de chiffrement à l'opérateur de séquestre 110 et l'opérateur de

séquestre 110 conserve cet accusé de réception et de certification mais détruit les documents chiffrés et les clés symétriques non chiffrées.

Au cours d'une étape 555, l'agence 105 transmet les documents chiffrés et les clés symétriques chiffrées à l'opérateur de transmission 120. Au cours d'une étape 560, l'opérateur de transmission 120 met les documents chiffrés et les clés symétriques chiffrées dans les comptes courants de correspondance respectivement de l'émetteur et du destinataire. Au cours d'une étape 565, l'opérateur de transmission 120 retourne à l'agence 105, par l'intermédiaire du tiers de confiance 115, une justification de liste récapitulative du placement des documents chiffrés et des clés symétriques chiffrées en comptes courants de correspondance.

Au cours d'une étape 570, l'agence 105 transmet à l'opérateur de transmission 120 un certificat de transmission horodaté.

Pour relire le document, au cours d'une étape 575, l'émetteur accède à sa clé symétrique chiffrée, la déchiffre avec sa clé privée et déchiffre le document chiffré disponible dans son compte de correspondance. L'étape 575 est éventuellement réalisée par l'intermédiaire du tiers de séquestre avec horodatage et transmission à l'agence 105 d'une justification de liste récapitulative de déchiffrement.

Pour lire le document, au cours d'une étape 580, l'émetteur accède à sa clé symétrique chiffrée, la déchiffre avec sa clé privée et déchiffre le document chiffré disponible dans son compte de correspondance. L'étape 580 est éventuellement réalisée par l'intermédiaire du tiers de séquestre avec horodatage et transmission à l'agence 105 d'une justification de liste récapitulative de déchiffrement.

En cas de besoin, par exemple pour des opérations d'instruction judiciaire et/ou sur commission rogatoire, au cours d'une étape 585, une clé symétrique chiffrée conservée par l'opérateur de séquestre, le document chiffré correspondant, conservé par l'opérateur d'archivage et la clé privée correspondante, conservée par un tiers de confiance (non représenté) sont transmis à un tiers qui déchiffre le document chiffré avec cette clé symétrique après avoir déchiffré la clé symétrique avec la clé privée de l'un des utilisateurs.

En variante, au cours de l'étape 550, les clés symétriques non chiffrées sont conservées par l'opérateur de séquestre et, au cours de l'étape 485, l'opérateur de séquestre transmet une de ces clés symétriques non chiffrées au tiers chargé du déchiffrement.

On observe que la présente invention permet de créer un coffre-fort de documents personnels dont la clé privée peut être conservée dans une carte d'identité électronique. L'utilisateur peut ainsi sauvegarder des copies de ses papiers d'identité, de ses diplômes, de ses assurances, de ses feuilles de paye, de ses déclarations fiscales et sociales, par exemple.

REVENDICATIONS

1 - Procédé de chiffrement d'un document, caractérisé en ce qu'il comporte :

- une étape (405, 505) de réception du document,
- une étape (425, 525) de chiffrement du document avec une clé symétrique,
- une étape (425, 525) de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques et
- une étape (430 à 460, 530 à 560) de transmission du document chiffré et de la clé symétrique chiffrée.

2 – Procédé selon la revendication 1, caractérisé en ce qu'il comporte une étape (410, 510) de génération de ladite clé symétrique pour chaque document à chiffrer.

3 – Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que, au cours de l'étape (425, 525) de chiffrement avec la clé asymétrique, ladite clé asymétrique est la clé publique de l'utilisateur ayant transmis ledit document.

4 – Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que, au cours de l'étape (425, 525) de chiffrement avec la clé asymétrique, ladite clé asymétrique est la clé publique d'un utilisateur destinataire du document.

5 – Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comporte une étape (415, 440, 515, 540) d'effacement du document chiffré et de conservation de la clé symétrique par le système informatique effectuant les étapes de chiffrement.

6 - Dispositif de chiffrement d'un document, caractérisé en ce qu'il comporte :

- un moyen de réception du document,
- un moyen de chiffrement du document avec une clé symétrique,
- un moyen de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques et
- un moyen de transmission du document chiffré et de la clé symétrique chiffrée.

7 – Dispositif selon la revendication 6, caractérisé en ce qu'il comporte un moyen de génération de ladite clé symétrique pour chaque document à chiffrer.

8 – Dispositif selon l'une quelconque des revendications 6 ou 7, caractérisé en ce que le moyen de chiffrement avec la clé asymétrique est adapté à ce que ladite clé asymétrique soit la clé publique de l'utilisateur ayant transmis ledit document.

9 – Dispositif selon l'une quelconque des revendications 6 ou 7, caractérisé en ce que le moyen de chiffrement avec la clé asymétrique, est adapté à ce que ladite clé asymétrique soit la clé publique d'un utilisateur destinataire du document.

10 – Dispositif selon l'une quelconque des revendications 6 à 9, caractérisé en ce qu'il comporte un moyen d'effacement du document chiffré et de conservation de la clé symétrique par le système informatique comportant les moyens de chiffrement.

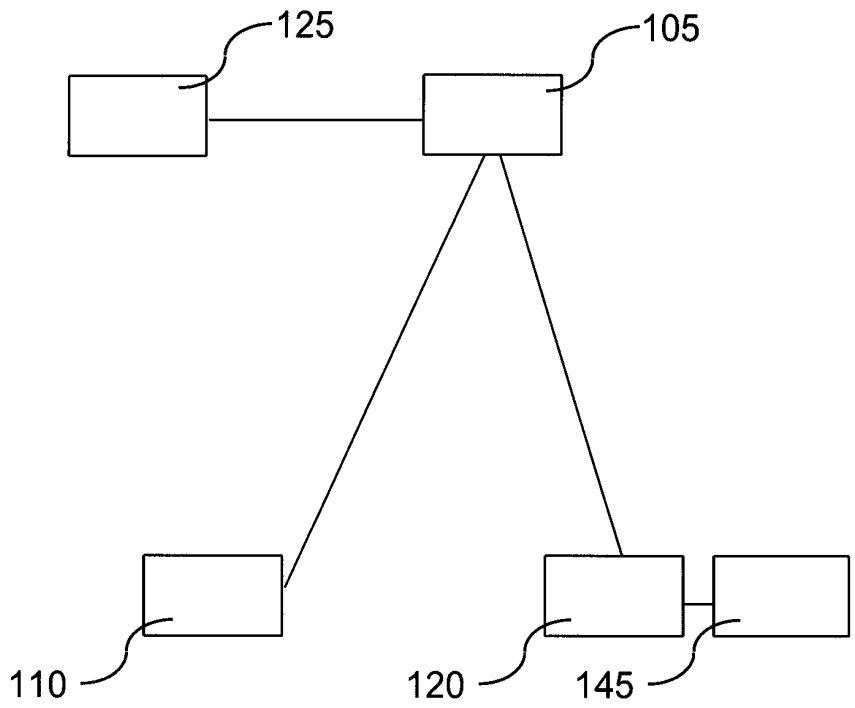


Figure 1

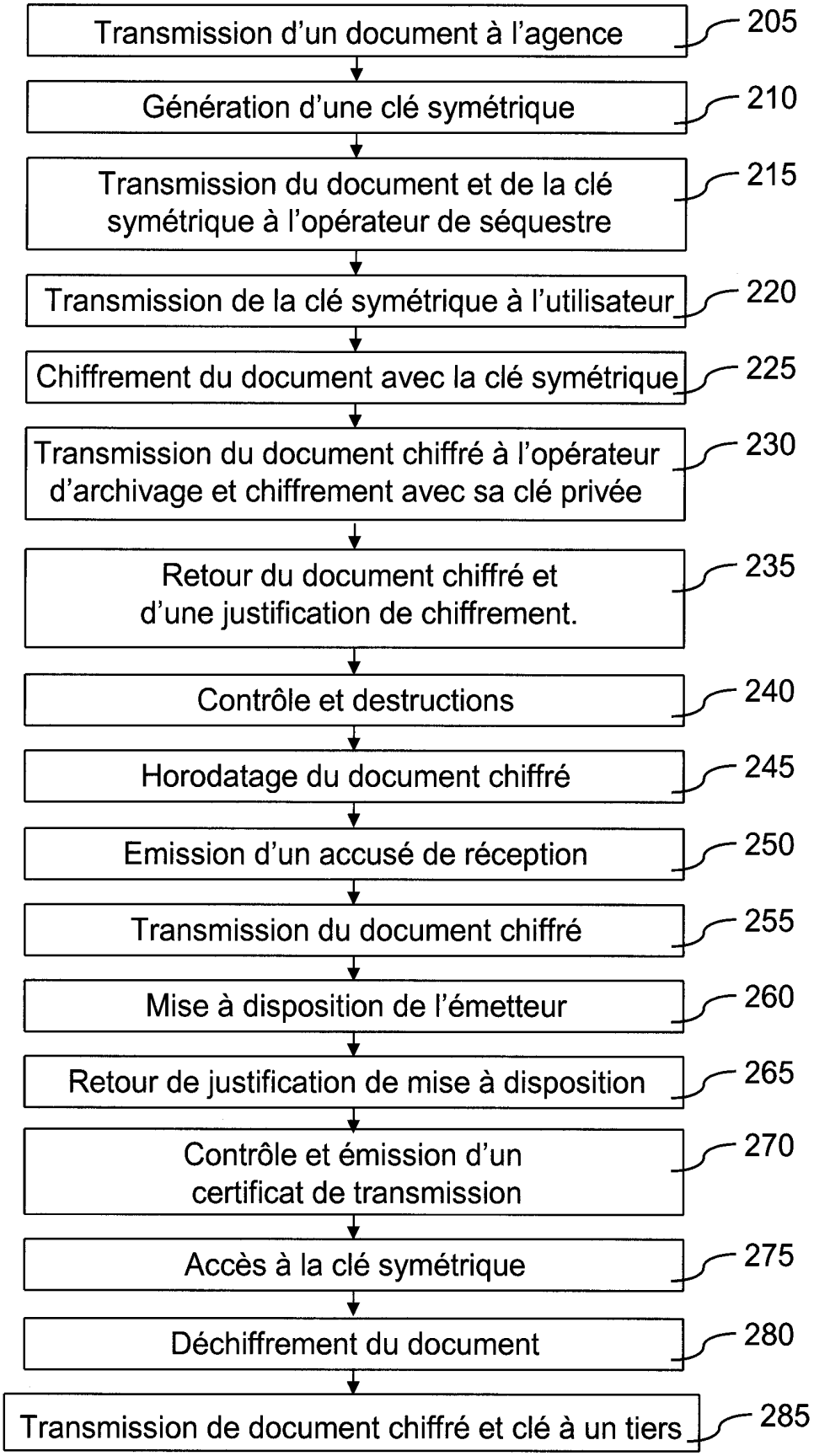

Transmission d'un document à l'agence
205
Génération d'une clé symétrique
210
Transmission du document et de la clé symétrique à l'opérateur de séquestre
215
Transmission de la clé symétrique à l'utilisateur
220
Chiffrement du document avec la clé symétrique
225
Transmission du document chiffré à l'opérateur d'archivage et chiffrement avec sa clé privée
230
Retour du document chiffré et d'une justification de chiffrement.
235
Contrôle et destructions
240
Horodatage du document chiffré
245
Emission d'un accusé de réception
250
Transmission du document chiffré
255
Mise à disposition de l'émetteur
260
Retour de justification de mise à disposition
265
Contrôle et émission d'un certificat de transmission
270
Accès à la clé symétrique
275
Déchiffrement du document
280
Transmission de document chiffré et clé à un tiers
285

Figure 2

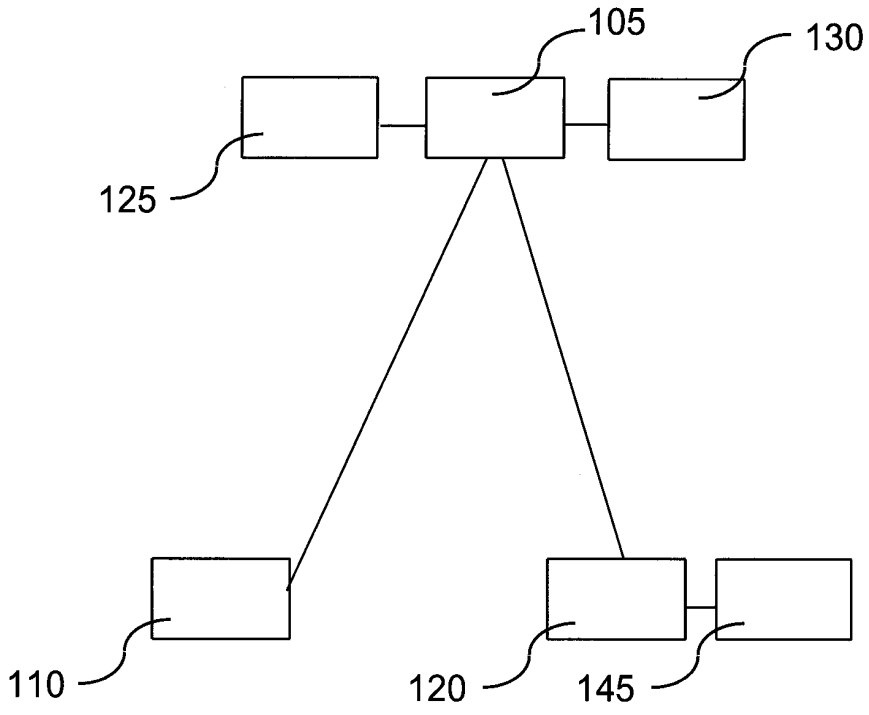


Figure 3

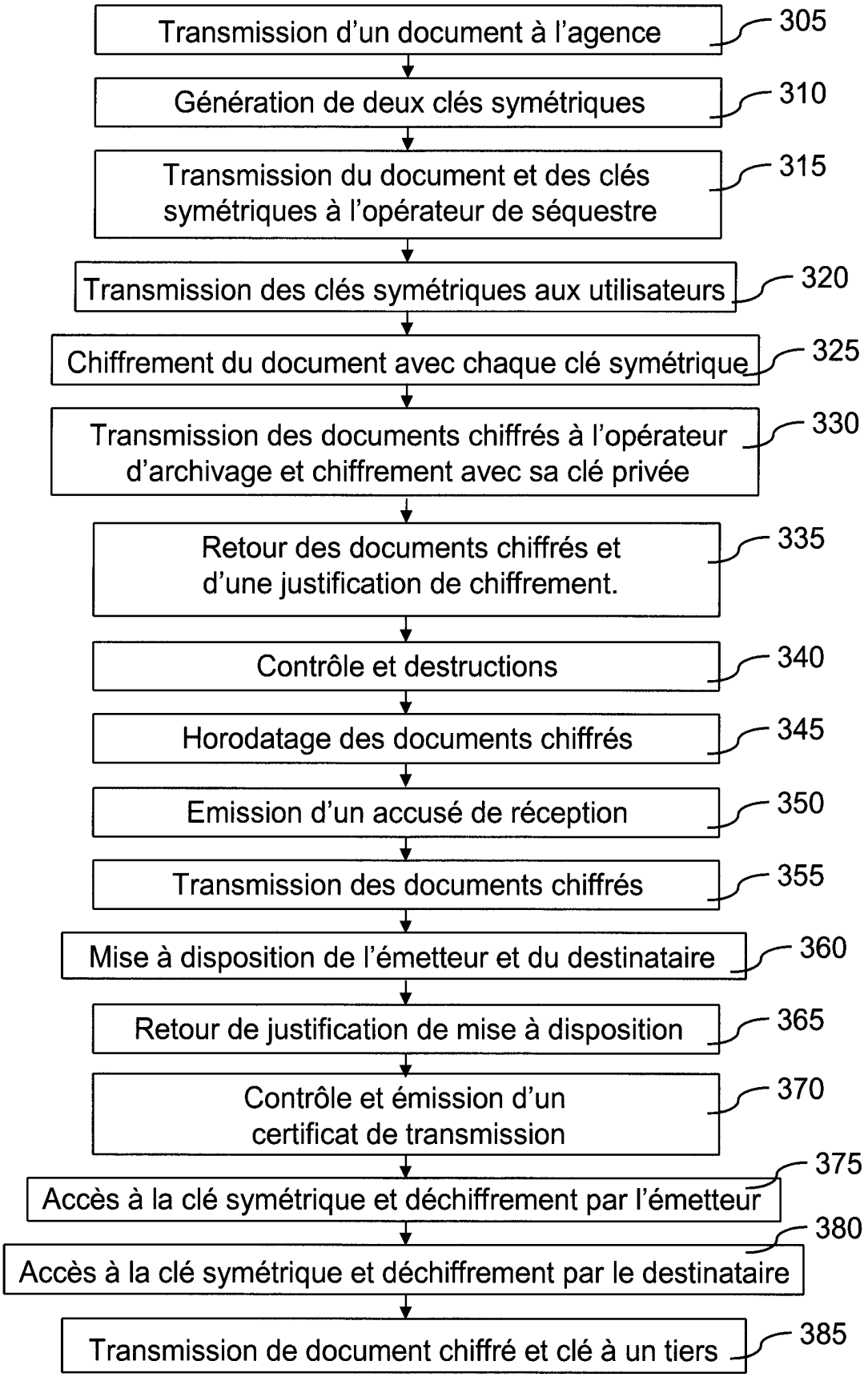

Transmission d'un document à l'agence
305
Génération de deux clés symétriques
310
Transmission du document et des clés symétriques à l'opérateur de séquestre
315
Transmission des clés symétriques aux utilisateurs
320
Chiffrement du document avec chaque clé symétrique
325
Transmission des documents chiffrés à l'opérateur d'archivage et chiffrement avec sa clé privée
330
Retour des documents chiffrés et d'une justification de chiffrement.
335
Contrôle et destructions
340
Horodatage des documents chiffrés
345
Emission d'un accusé de réception
350
Transmission des documents chiffrés
355
Mise à disposition de l'émetteur et du destinataire
360
Retour de justification de mise à disposition
365
Contrôle et émission d'un certificat de transmission
370
Accès à la clé symétrique et déchiffrement par l'émetteur
375
Accès à la clé symétrique et déchiffrement par le destinataire
380
Transmission de document chiffré et clé à un tiers
385

Figure 4

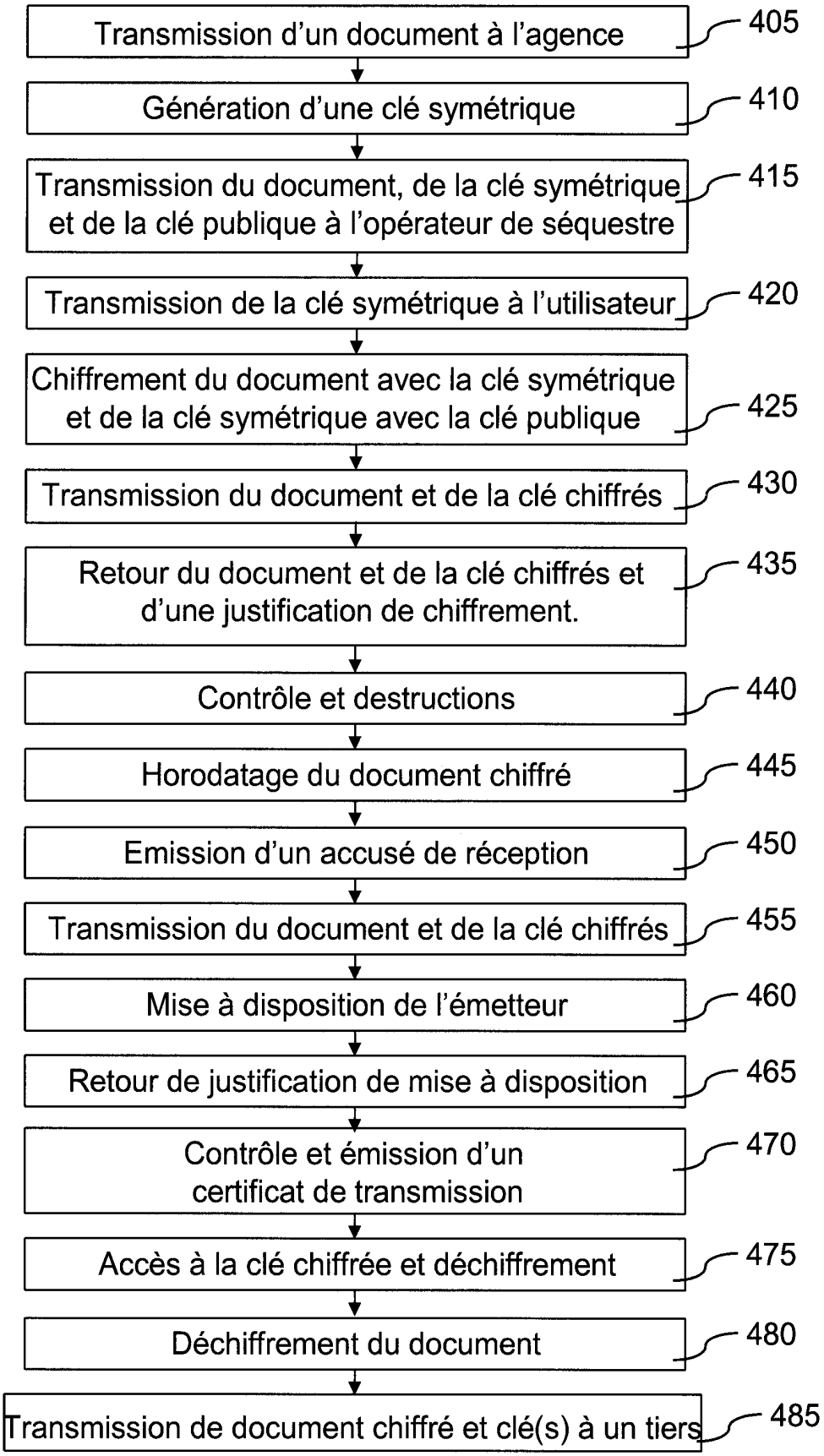

Transmission d'un document à l'agence
405
Génération d'une clé symétrique
410
Transmission du document, de la clé symétrique et de la clé publique à l'opérateur de séquestre
415
Transmission de la clé symétrique à l'utilisateur
420
Chiffrement du document avec la clé symétrique et de la clé symétrique avec la clé publique
425
Transmission du document et de la clé chiffrés
430
Retour du document et de la clé chiffrés et d'une justification de chiffrement.
435
Contrôle et destructions
440
Horodatage du document chiffré
445
Emission d'un accusé de réception
450
Transmission du document et de la clé chiffrés
455
Mise à disposition de l'émetteur
460
Retour de justification de mise à disposition
465
Contrôle et émission d'un certificat de transmission
470
Accès à la clé chiffrée et déchiffrement
475
Déchiffrement du document
480
Transmission de document chiffré et clé(s) à un tiers
485

Figure 5

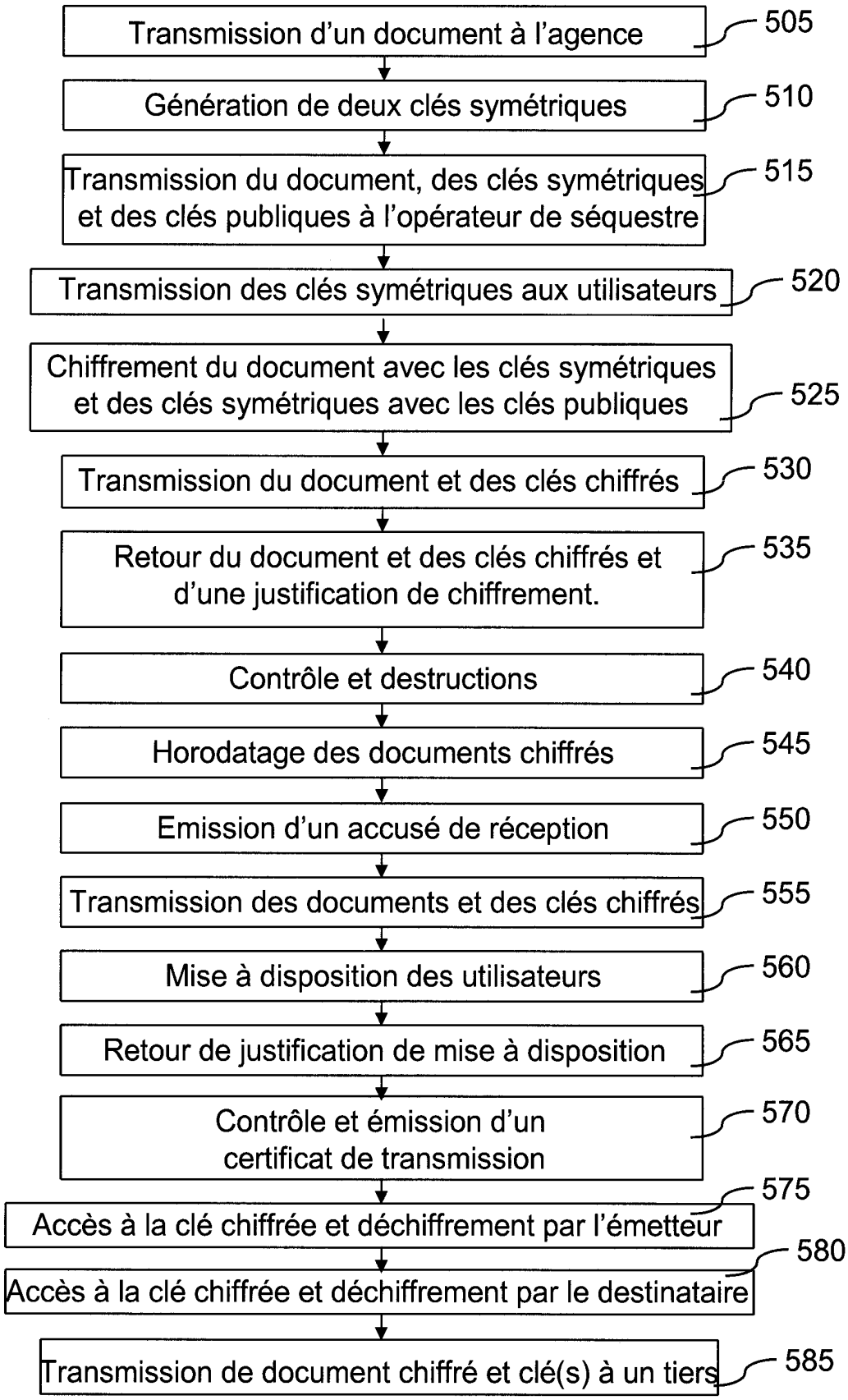

Transmission d'un document à l'agence
505
Génération de deux clés symétriques
510
Transmission du document, des clés symétriques et des clés publiques à l'opérateur de séquestre
515
Transmission des clés symétriques aux utilisateurs
520
Chiffrement du document avec les clés symétriques et des clés symétriques avec les clés publiques
525
Transmission du document et des clés chiffrés
530
Retour du document et des clés chiffrés et d'une justification de chiffrement.
535
Contrôle et destructions
540
Horodatage des documents chiffrés
545
Emission d'un accusé de réception
550
Transmission des documents et des clés chiffrés
555
Mise à disposition des utilisateurs
560
Retour de justification de mise à disposition
565
Contrôle et émission d'un certificat de transmission
570
Accès à la clé chiffrée et déchiffrement par l'émetteur
575
Accès à la clé chiffrée et déchiffrement par le destinataire
580
Transmission de document chiffré et clé(s) à un tiers
585

Figure 6

RÉPUBLIQUE FRANÇAISE

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 723141
FR 0901441

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		
X	FR 2 804 561 A (FRANCE TELECOM [FR]) 3 août 2001 (2001-08-03) * abrégé * * page 5, ligne 21 - page 8, ligne 14 * * page 11, ligne 16 - page 15, ligne 19 *	1-10	H04L9/32 H04L29/06
X	VICTOR SHOUP: "A Proposal for an ISO Standard for Public Key Encryption (version 2.1)" INTERNET CITATION, [Online] 20 décembre 2001 (2001-12-20), page Complete, XP007910787 Extrait de l'Internet: URL:http://eprint.iacr.org/2001/112.pdf> [extrait le 2009-12-04]	1,2,6,7	
A	* alinéa [0003] - alinéa [0005] *	3-5,8-10	
X	WO 02/093849 A (KASTEN CHASE APPLIED RES LTD [CA]; MULDER DAVID G [CA]; MISKIMMIN ROBE) 21 novembre 2002 (2002-11-21)	1,2,6,7	
A	* abrégé * * page 5, ligne 1 - page 8, ligne 2 * * revendication 1 *	3-5,8-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L
A	FR 2 786 049 A (LEFEVRE JEAN PIERRE ROLAND PAU [FR]) 19 mai 2000 (2000-05-19) * page 4, ligne 5 - page 5, ligne 34 * * page 16, ligne 8 - page 20, ligne 27 *	1-10	

Date d'achèvement de la recherche	Examinateur
7 décembre 2009	Bec, Thierry

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0901441 FA 723141

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 07-12-2009
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
FR 2804561 A	03-08-2001	EP 1254534 A1	06-11-2002
		WO 0156222 A1	02-08-2001
		JP 2003521197 T	08-07-2003
		US 2003012387 A1	16-01-2003
WO 02093849 A	21-11-2002	CA 2386491 A1	16-11-2002
FR 2786049 A	19-05-2000	AUCUN	

EPO FORM P0465