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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
30 septembre 2010 (30.09.2010)

PCT

(10) Numéro de publication internationale
WO 2010/108994 A2

(51) Classification internationale des brevets :
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2010/053953

(22) Date de dépôt international :
25 mars 2010 (25.03.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
09 01441 26 mars 2009 (26.03.2009) FR
09 01442 26 mars 2009 (26.03.2009) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **TRUSTSEED** [FR/FR]; 23, avenue du Lieutel, F-78490 Galluis (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **BLOT-LEFEVRE, Eric** [FR/FR]; 53, Boulevard Victor Hugo, F-92200 Neuilly-sur-seine (FR).

(74) Mandataire : **NGUYEN-VAN-YEN, Christian**; Immeuble "Visium", 22, avenue Aristide Briand, F-94117 Arcueil Cedex (FR).

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

[Suite sur la page suivante]

(54) Title : METHOD AND DEVICE FOR ARCHIVING A DOCUMENT

(54) Titre : PROCEDE ET DISPOSTIF D'ARCHIVAGE D'UN DOCUMENT

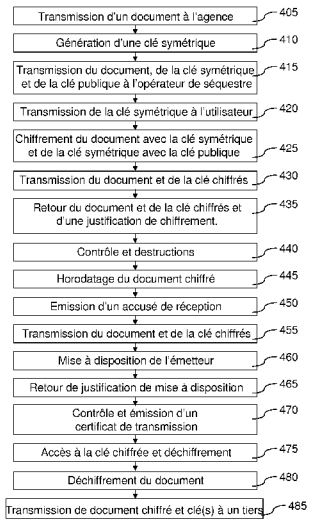

Figure 5

405 Send a document to the agency
410 Generate a symmetric key
415 Send the document, the symmetric key, and the public key to the receiving operator
420 Send the symmetric key to the user
425 Encrypt the document with a symmetric key, and encrypt the symmetric key with the public key
430 Send encrypted document and encrypted key
435 Return encrypted document and encrypted key and confirmation of the encryption
440 Check and destroy
445 Timestamp the encrypted document
450 Send confirmation of receipt
455 Send the encrypted document and encrypted key
460 Make available by sender
465 Return confirmation of making available
470 Check and send a transmission certificate
475 Access and decrypt the encrypted key
480 Decrypt the document
485 Send encrypted document and key(s) to a third party

(57) Abstract : The invention relates to a method for archiving a document, including: a step (225, 325, 425, 525) of encrypting the document with a symmetric key; a step (230, 330, 430, 530) of sending said encrypted document to an archiving operator; and a step of sending the symmetric key for encrypting said document to a receiving operator separate from the archiving operator. In certain embodiments, the method comprises a step (425, 525) of encrypting the symmetric key with a key consisting of a dual key comprising asymmetric keys. During the step of encrypting with the asymmetric key, the asymmetric key is that of the user having sent said document or that of the recipient of the document, depending on whether the method is used for personal archiving or for document transmission.

(57) Abrégé : Le procédé d'archivage d'un document comprend : - une étape (225, 325, 425, 525) de chiffrement du document avec une clé symétrique, - une étape (230, 330, 430, 530) de transmission dudit document chiffré à un opérateur d'archivage, - une étape de transmission de la clé symétrique de chiffrement dudit document à un opérateur de séquestre distinct de l'opérateur d'archivage. Dans des modes de réalisation, le procédé comporte une étape (425, 525) de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques. 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.

WO 2010/108994 A2

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

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport (règle 48.2.g))*

PROCEDE ET DISPOSITIF D'ARCHIVAGE 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, la présente invention divulgue un procédé d'archivage d'un document par un utilisateur comprenant une étape de chiffrement du document avec une clé symétrique et une étape de transmission dudit document chiffré à un opérateur d'archivage, caractérisé en ce qu'il comprend en outre une étape de transmission de la clé symétrique de chiffrement dudit document à un opérateur de séquestre distinct de l'opérateur d'archivage.

Avantageusement, le procédé de l'invention comprend en outre une étape de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques.

Avantageusement, le procédé de l'invention comprend une étape de génération de ladite clé symétrique pour chaque document à chiffrer.

Avantageusement, ladite clé symétrique est différente pour chaque document à chiffrer.

Avantageusement, 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.

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

Avantageusement, le procédé de l'invention comprend en outre une étape d'effacement du document chiffré et de conservation de la clé symétrique par le système informatique effectuant les étapes de chiffrement.

Avantageusement, le procédé de l'invention comprend en outre une étape de transmission par l'opérateur d'archivage à l'utilisateur du document chiffré, une étape de transmission par l'opérateur de séquestre audit utilisateur de la clé symétrique de chiffrement du document chiffré et une étape de déchiffrement par ledit utilisateur dudit document chiffré avec ladite clé symétrique.

Avantageusement, le procédé de l'invention comprend en outre une étape de transmission par l'opérateur d'archivage à un tiers habilité du document chiffré, une étape de transmission par l'opérateur de séquestre audit tiers habilité de la clé symétrique de chiffrement du document chiffré et une étape de déchiffrement par ledit tiers habilité dudit document chiffré avec ladite clé symétrique.

L'invention divulgue également un dispositif d'archivage d'un document par un utilisateur comprenant un module apte à chiffrer ledit document avec une clé symétrique et un module apte à transmettre ledit document chiffré à un opérateur d'archivage, caractérisé en ce qu'il comprend en outre un module de transmission de la clé symétrique de chiffrement dudit document à un opérateur de séquestre distinct de l'opérateur d'archivage.

Avantageusement, le dispositif de l'invention comprend en outre un module de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques.

Avantageusement, le dispositif de l'invention comprend en outre un moyen de génération de ladite clé symétrique pour chaque document à chiffrer.

Avantageusement, ladite clé symétrique est différente pour chaque document à chiffrer.

Avantageusement, le dispositif de l'invention comprend en outre un module apte à réaliser la transmission par l'opérateur d'archivage à l'utilisateur du document chiffré, un module apte à réaliser la transmission par l'opérateur de séquestre audit utilisateur de la clé symétrique de chiffrement du document chiffré et un module apte à réaliser le déchiffrement par ledit utilisateur dudit document chiffré avec ladite clé symétrique.

Avantageusement, le dispositif de l'invention comprend en outre un module apte à réaliser la transmission par l'opérateur d'archivage à un tiers habilité du document chiffré, un module apte à réaliser la transmission par l'opérateur de séquestre audit tiers habilité de la clé symétrique de chiffrement du document chiffré et un module apte à réaliser le déchiffrement par ledit tiers habilité dudit document chiffré avec ladite clé symétrique.

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 d'archivage d'un document par un utilisateur comprenant une étape (225, 325, 425, 525) de chiffrement du document avec une clé symétrique et une étape (230, 330, 430, 530) de transmission dudit document chiffré à un opérateur d'archivage, caractérisé en ce qu'il comprend en outre une étape de transmission de la clé symétrique de chiffrement dudit document à un opérateur de séquestre distinct de l'opérateur d'archivage.

2 – Procédé d'archivage selon la revendication 1, caractérisé en ce qu'il comprend en outre une étape (425, 525) de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques.

3 – Procédé d'archivage selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'il comprend une étape (410, 510) de génération de ladite clé symétrique pour chaque document à chiffrer.

4 - Procédé d'archivage selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ladite clé symétrique est différente pour chaque document à chiffrer.

5 – Procédé d'archivage selon l'une quelconque des revendications 1 à 4, 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.

6 – Procédé d'archivage selon l'une quelconque des revendications 1 à 4, 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.

7 – Procédé d'archivage selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comprend en outre 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.

8 - Procédé d'archivage selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comprend en outre une étape (255, 355, 455, 555) de transmission par l'opérateur d'archivage à l'utilisateur du document chiffré, une étape (275, 375, 475, 575) de transmission par l'opérateur de séquestre audit utilisateur de la clé symétrique de chiffrement du document chiffré et une étape (280, 380, 480, 580) de déchiffrement par ledit utilisateur dudit document chiffré avec ladite clé symétrique.

9 - Procédé d'archivage selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comprend en outre une étape (255, 355, 455, 555) de transmission par l'opérateur d'archivage à un tiers habilité du document chiffré, une étape (275, 375, 475, 575) de transmission par l'opérateur de séquestre audit tiers habilité de la clé symétrique de chiffrement du document chiffré et une étape (280, 380, 480, 580) de déchiffrement par ledit tiers habilité dudit document chiffré avec ladite clé symétrique.

10 - Dispositif d'archivage d'un document par un utilisateur comprenant un module apte à chiffrer ledit document avec une clé symétrique et un module apte à transmettre ledit document chiffré à un opérateur d'archivage, caractérisé en ce qu'il comprend en outre un module de transmission de la clé symétrique de chiffrement dudit document à un opérateur de séquestre distinct de l'opérateur d'archivage.

11 – Dispositif d'archivage selon la revendication 10, caractérisé en ce qu'il comprend en outre un module de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques.

12 – Dispositif d'archivage selon l'une quelconque des revendications 10 à 11, caractérisé en ce qu'il comprend en outre un moyen de génération de ladite clé symétrique pour chaque document à chiffrer.

13 – Dispositif d'archivage selon l'une quelconque des revendications 10 à 12, caractérisé en ce que ladite clé symétrique est différente pour chaque document à chiffrer.

14 – Dispositif d'archivage selon l'une quelconque des revendications 10 à 13, caractérisé en ce qu'il comprend en outre un module apte à réaliser la

transmission par l'opérateur d'archivage à l'utilisateur du document chiffré, un module apte à réaliser la transmission par l'opérateur de séquestre audit utilisateur de la clé symétrique de chiffrement du document chiffré et un module apte à réaliser le déchiffrement par ledit utilisateur dudit document chiffré avec ladite clé symétrique.

15 - Dispositif d'archivage selon l'une quelconque des revendications 10 à 13, caractérisé en ce qu'il comprend en outre un module apte à réaliser la transmission par l'opérateur d'archivage à un tiers habilité du document chiffré, un module apte à réaliser la transmission par l'opérateur de séquestre audit tiers habilité de la clé symétrique de chiffrement du document chiffré et un module apte à réaliser le déchiffrement par ledit tiers habilité dudit document chiffré avec ladite clé symétrique.

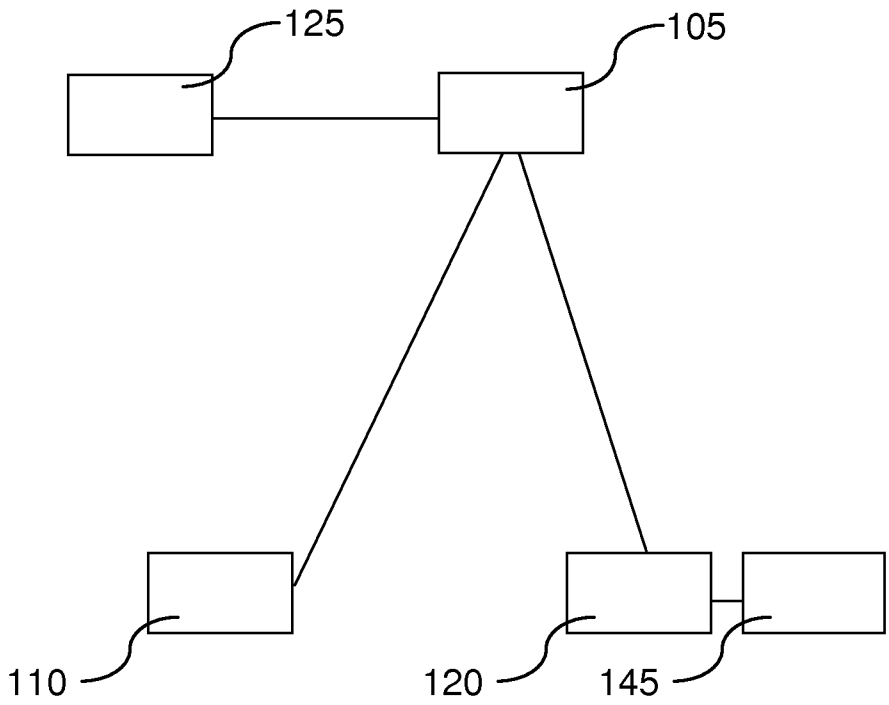

Figure 1

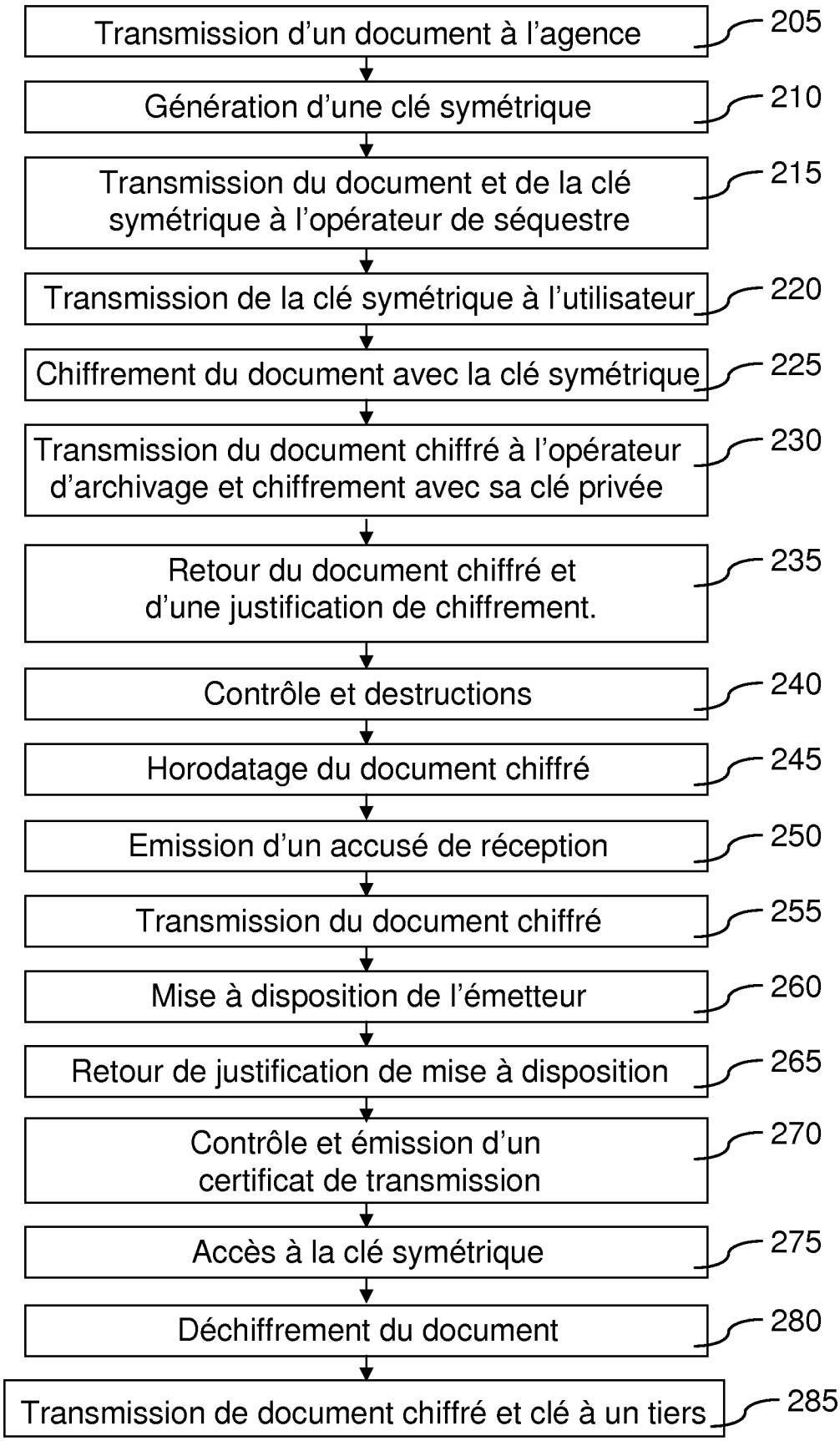
Transmission d'un document à l'agence
205
Génération d'une clé symétrique
210
Transmission du document et de la clé symétrique à l'opérateur de séquestre
215
Transmission de la clé symétrique à l'utilisateur
220
Chiffrement du document avec la clé symétrique
225
Transmission du document chiffré à l'opérateur 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

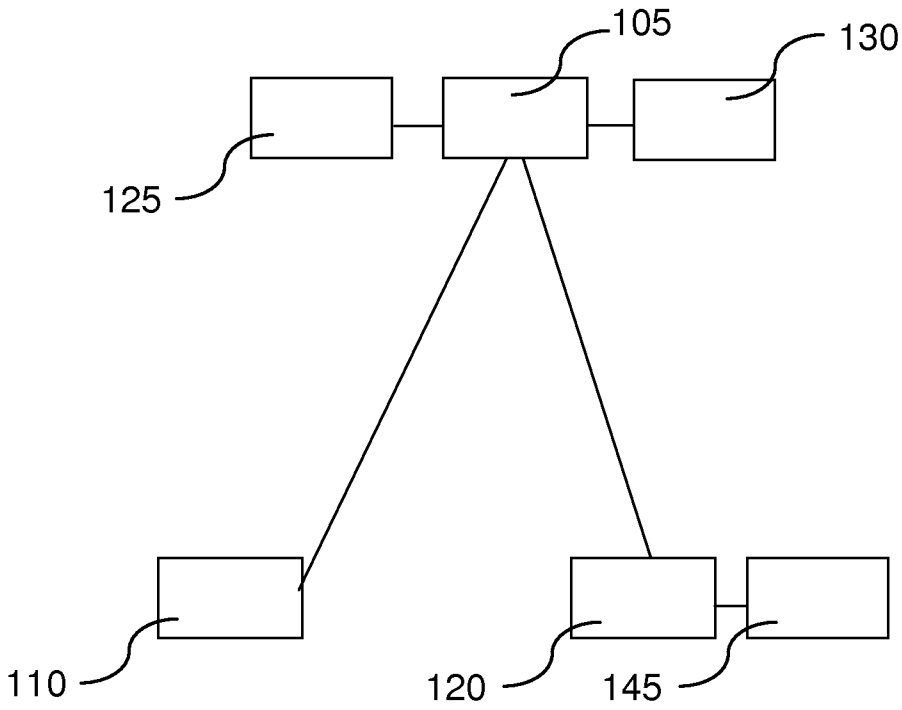

Figure 3

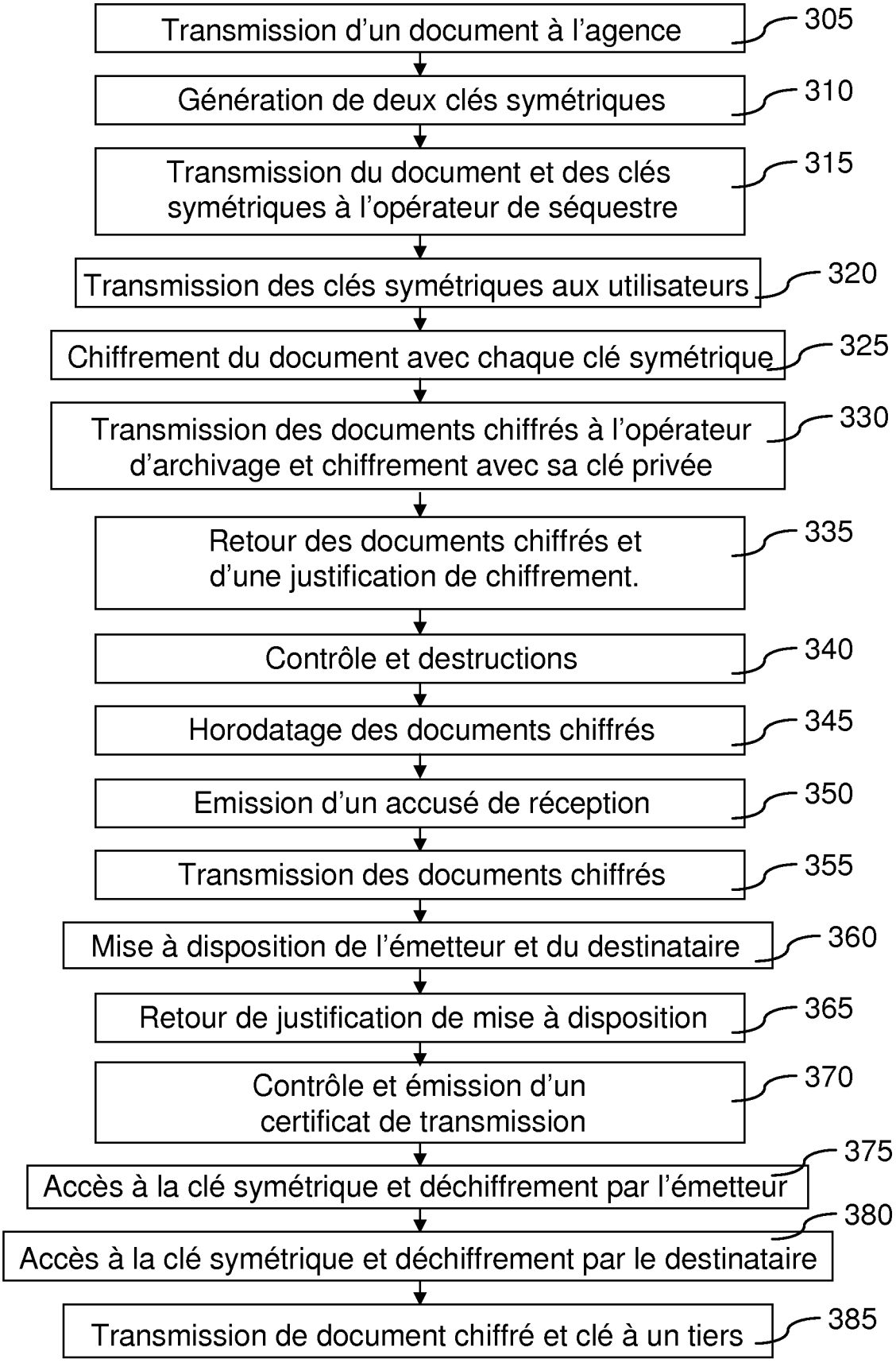
Transmission d'un document à l'agence
305
Génération de deux clés symétriques
310
Transmission du document et des clés symétriques à l'opérateur de séquestre
315
Transmission des clés symétriques aux utilisateurs
320
Chiffrement du document avec chaque clé symétrique
325
Transmission des documents chiffrés 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

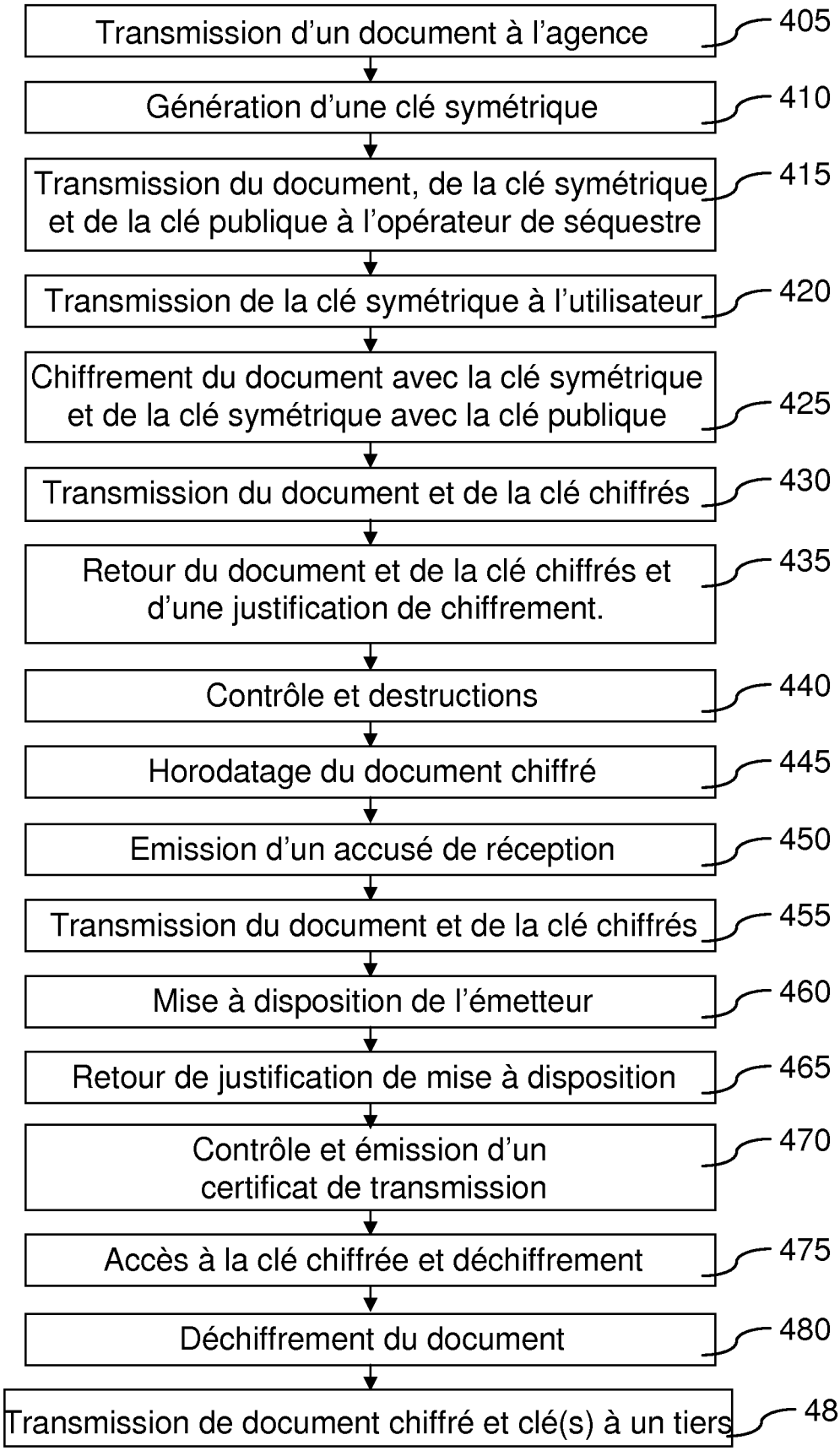
Transmission d'un document à l'agence
405
Génération d'une clé symétrique
410
Transmission du document, de la clé symétrique et de la clé publique à l'opérateur de séquestre
415
Transmission de la clé symétrique à l'utilisateur
420
Chiffrement du document avec la clé symétrique et de la clé symétrique 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

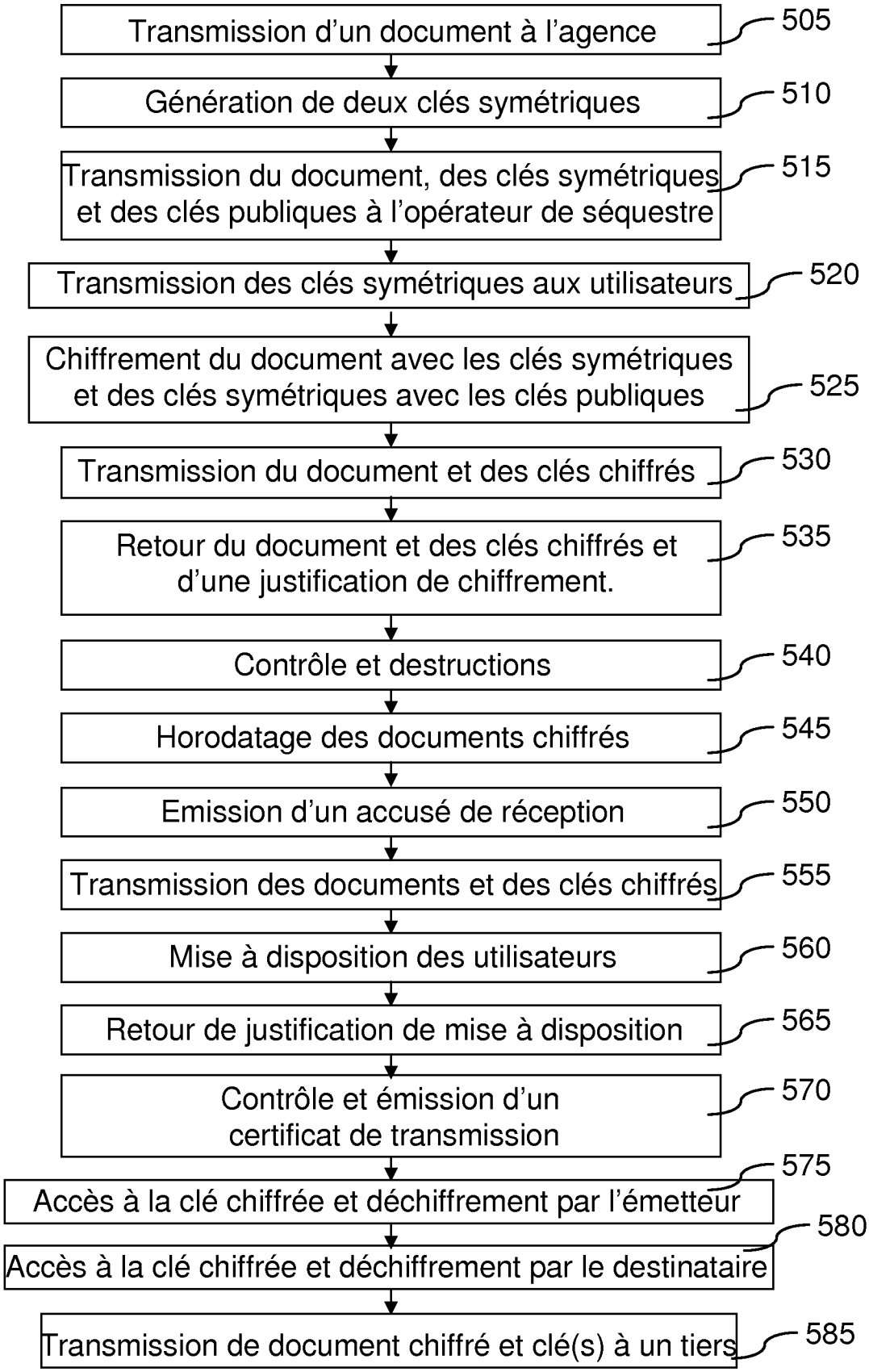
Transmission d'un document à l'agence
505
Génération de deux clés symétriques
510
Transmission du document, des clés symétriques et des clés publiques à l'opérateur de séquestre
515
Transmission des clés symétriques aux utilisateurs
520
Chiffrement du document avec les clés symétriques et des clés symétriques 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