(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
13 juillet 2006 (13.07.2006)

PCT

(10) Numéro de publication internationale
WO 2006/072690 A2

(51) Classification internationale des brevets :
H04L 29/06 (2006.01) *H04L 12/58* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2005/003215

(22) Date de dépôt international :
16 décembre 2005 (16.12.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0500139 5 janvier 2005 (05.01.2005) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **FRISCH, Laurent** [FR/FR]; 27, avenue d'Italie, F-75013 Paris (FR). **ARDITTI, David** [FR/FR]; 46 ter, rue Paul Vaillant Couturier, F-92140 Clamart (FR). **MATHIAS, Christophe** [FR/FR]; 7, avenue Eugénie, F-92210 Saint-Cloud (FR).

(74) Mandataire : **DAUDE, Delphine**; France Telecom, 38-40, rue du Général Leclerc, F-92794 Issy les Moulineaux Cedex 9 (FR).

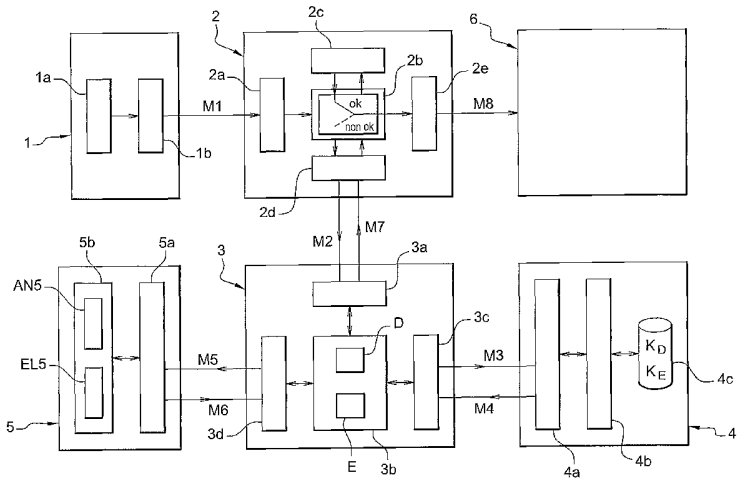
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC,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

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Suite sur la page suivante]

(54) **Title:** METHOD AND SYSTEM FOR TRANSMITTING AN ENCRYPTED SET OF DATA FROM AN ORIGINATOR DEVICE TO A RECIPIENT DEVICE

(54) **Titre :** PROCEDE ET SYSTEME DE TRANSMISSION D'UN ENSEMBLE DE DONNEES CHIFFRE DEPUIS UN DISPOSITIF EXPEDITEUR VERS UN DISPOSITIF DESTINATAIRE



(57) **Abstract:** The invention concerns transmission of an encrypted set of data from an originator device (1) to a recipient device (6). A first communication module transmits the encrypted set of data. A second communication module (3c) interfaces with a key repository module (4) to obtain at least one decryption key associated with the transmitted encrypted set of data. A module (D) decrypts the transmitted encrypted set of data using the obtained key. A first analyzing module (AN5) analyzes the decrypted set of data to detect whether the latter comprises an element unwanted by the recipient device (6). A third communication module (3a) transmits a message indicating whether the decrypted set of data comprises or not such an undesirable element. A second analyzing module (AN2) analyzes the transmitted message so that a fourth communication module (2e) transmits to the recipient device (6), either the encrypted set of data as initially transmitted by the originator device (1), or a warning message indicating that the encrypted set of data comprises an undesirable element.

[Suite sur la page suivante]

WO 2006/072690 A2

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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne la transmission d'un ensemble de données chiffré depuis un dispositif expéditeur (1) vers un dispositif destinataire (6). Un premier module de communication transmet l'ensemble de données chiffré. Un second module de communication (3c) dialogue avec un module (4) d'archivage de clés afin d'obtenir au moins une clé de déchiffrement associée à l'ensemble de données chiffré transmis. Un module (D) déchiffre l'ensemble de données chiffré transmis au moyen de la clé obtenue. Un premier module d'analyse (AN5) analyse l'ensemble de données déchiffré pour détecter si ce dernier comporte un élément non désiré par le dispositif destinataire (6). Un troisième module de communication (3a) transmet un message selon lequel l'ensemble de données déchiffré comporte ou ne comporte pas un tel élément non désiré. Un second module d'analyse (AN2) analyse le message transmis de telle façon qu'un quatrième module de communication (2e) transmette, en direction du dispositif destinataire (6), soit l'ensemble de données chiffré tel qu'émis initialement par le dispositif expéditeur (1), soit un message d'avertissement selon lequel l'ensemble de données chiffré comporte un élément non désiré.

Procédé et système de transmission d'un ensemble de données chiffré depuis un dispositif expéditeur vers un dispositif destinataire

La présente invention concerne un système de transmission d'un ensemble de données chiffré depuis un dispositif expéditeur vers un dispositif destinataire.

Par ensemble de données, on entend un document, un fichier, un message, etc...destiné à être transmis via un réseau de communication, tel qu'en particulier un réseau utilisant le protocole IP (de l'anglais Internet Protocol).

A l'heure actuelle, pour assurer la transmission, de façon confidentielle, d'un ensemble de données du type précité, par exemple un document électronique, on chiffre le texte du document. Cette opération consiste à appliquer une fonction mathématique avec des caractéristiques très particulières sur le texte. Cette fonction utilise une variable, la clé de chiffrement, qui est une suite de bits. Une fois le texte chiffré, il est illisible. Pour obtenir la version lisible, il faut le déchiffrer, c'est-à-dire appliquer une autre fonction mathématique, compatible avec la première, avec une autre variable, la clé de déchiffrement.

La valeur de la clé de déchiffrement dépend évidemment de la valeur de la clé de chiffrement et seul le possesseur de la clé de déchiffrement peut déchiffrer le texte. Lorsqu'un expéditeur désire transmettre un document confidentiel à un destinataire, via le réseau de communication précité, il chiffre le document sur son poste de travail avec une clé de chiffrement et il envoie la version chiffrée du document au destinataire. Ce dernier déchiffre le document sur son poste de travail avec la clé de déchiffrement, qu'il est le seul à connaître.

Un tel mode de transmission est mis en œuvre notamment dans le cadre de la dématérialisation des passations d'appels d'offre. Lorsqu'un organisme public lance un appel d'offres (préalable obligatoire à la conclusion d'un marché public), les entreprises candidates ont la faculté de retirer le dossier d'appel d'offres sous forme électronique, puis de déposer leurs offres en ligne.

Des dispositions législatives récentes encadrent, de façon assez

étroite, les conditions dans lesquelles le dépôt de ces offres peut s'effectuer.

En particulier :

- les entreprises candidates doivent signer électroniquement les documents qui contiennent leurs offres,

- si un document électronique qui contient une offre est considéré invalide par le dispositif destinataire, tel qu'en particulier un serveur appartenant à l'organisme public, le serveur rejette le document dès sa réception.

Un critère d'invalidité d'un tel document électronique pourrait par exemple s'appliquer lorsque le document électronique contient un élément non désiré par le dispositif destinataire.

Par élément non désiré, on entend notamment:

- une pièce jointe (fichier texte, image, multimédia ou autres) qui est envoyée par erreur depuis le dispositif expéditeur de l'entreprise candidate,

- un programme malveillant (virus, ver informatique ou autres) qui est contenu dans une pièce jointe, le terme "malveillant" signifiant que le programme se diffuse dans le dispositif destinataire dans le but d'entraîner le dysfonctionnement de ce dernier,

- une fonction interdite, telle que par exemple une "macro" permettant d'effectuer directement des commandes système, comme cela est possible dans Microsoft Word ou Microsoft Excel.

Si on considère qu'un document est invalide selon le critère ci-dessus, et que par ailleurs ce document est chiffré, le dispositif destinataire, en l'occurrence le serveur précité, n'est pas en mesure de le rejeter dès sa réception. En effet, la clé (éventuellement les clés) de déchiffrement du document n'est envoyée au serveur destinataire qu'au moment de l'ouverture officielle des appels d'offre.

En outre, il n'est pas souhaitable d'installer, dans le serveur précité, un module logiciel dédié à l'élimination des virus (notamment un anti-virus) qui sont susceptibles d'être contenus dans les documents chiffrés reçus par le serveur.

Une telle installation est en effet relativement lourde et entraînerait

nécessairement des problèmes d'efficacité et d'administrabilité du serveur (ex: obligation de mise à jour régulières des anti-virus du serveur).

Par ailleurs, les documents WO 01/63881, WO 99/05814, US 2002/0007453 et US 6 721 424 divulguent un système de transmission du type précité, dans lequel l'ensemble de données chiffré est, au cours de sa transmission, déchiffré, puis analysé, afin d'y détecter des éléments non désirés.

Un tel système comprend:

- un premier module de communication pour transmettre un ensemble de données chiffré émis par le dispositif expéditeur,
- un second module de communication pour dialoguer avec un module d'archivage de clés afin d'obtenir au moins une clé de déchiffrement qui est associée à l'ensemble de données chiffré transmis,
- un module de déchiffrement de l'ensemble de données chiffré transmis, au moyen de la clé de déchiffrement obtenue, pour obtenir un ensemble de données déchiffré,
- un module d'analyse pour analyser l'ensemble de données déchiffré afin de détecter si ce dernier comporte un élément non désiré par le dispositif destinataire.

L'inconvénient d'un tel système réside dans le fait que ce n'est pas l'ensemble de données chiffré initialement qui est reçu par le dispositif destinataire, mais un ensemble de données transformé, c'est-à-dire déchiffré, rechiffré, etc....

La présente invention a pour but de remédier aux inconvénients précités.

A cet effet, le système selon l'invention comprend :

- un troisième module de communication, pour transmettre un message selon lequel l'ensemble de données déchiffré comporte ou ne comporte pas un tel élément non désiré,
- un second module d'analyse pour analyser ledit message transmis,
- un quatrième module de communication pour transmettre en

direction du dispositif destinataire l'ensemble de données chiffré tel qu'émis initialement par le dispositif expéditeur, et, dans le cas où le message analysé par les seconds moyens d'analyse stipule que l'ensemble de données déchiffré comporte un tel élément non désiré, des informations selon lesquelles l'ensemble de données chiffré comporte cet élément non désiré.

Grâce à une telle configuration, le système selon l'invention permet d'éliminer, dans un ensemble de données chiffré qui est transmis à un dispositif destinataire, tout élément non désiré par ce dernier, avant même que le dispositif destinataire ne procède au déchiffrement de l'ensemble de données chiffré transmis.

Dans des modes de réalisation préférés du système selon l'invention, on a recours à l'une ou l'autre des dispositions suivantes :

- le système comprend en outre :
  - un module d'élimination pour supprimer, dans l'ensemble de données déchiffré, la totalité ou seulement une partie d'un élément non désiré susceptible d'être détecté par le premier module d'analyse,
  - un module de restitution pour reconstituer, à l'aide d'au moins une clé de chiffrement compatible avec la clé de déchiffrement, la totalité ou seulement une partie de l'ensemble de données chiffré transmis, à partir de l'ensemble de données déchiffré dans lequel le module d'élimination a supprimé la totalité ou seulement une partie de l'élément non désiré, la clé de chiffrement étant obtenue au préalable par le second module de communication, en plus de la clé de déchiffrement,
  - le troisième module de communication transmettant en outre l'ensemble de données chiffré reconstitué en totalité ou en partie,
  - et le quatrième module de communication transmettant en outre, en direction du dispositif destinataire, soit l'ensemble

de données chiffré transmis reconstitué en totalité, soit l'ensemble de données chiffré transmis reconstitué en partie.

- le second module de communication, les modules de déchiffrement et de restitution, le premier module d'analyse, le module d'élimination, ainsi que le troisième module de communication sont regroupés dans un seul dispositif,

- le module de communication, les modules de déchiffrement, de restitution et d'archivage, ainsi que le troisième module de communication, sont regroupés dans une infrastructure à clés publiques.

- le second module de communication, le premier module d'analyse, les modules de déchiffrement, d'élimination, de restitution et d'archivage, ainsi que le troisième module de communication, sont regroupés dans un seul dispositif.

Corrélativement, la présente invention concerne un procédé de transmission d'un ensemble de données chiffré depuis un dispositif expéditeur vers un dispositif destinataire, ledit procédé comprenant les étapes suivantes :

- a) transmission d'un ensemble de données chiffré depuis le dispositif expéditeur,

- b) dialogue avec un module d'archivage de clés afin d'obtenir au moins une clé de déchiffrement qui est associée à l'ensemble de données chiffré transmis,

- c) déchiffrement de l'ensemble de données chiffré transmis, au moyen de la clé de déchiffrement obtenue,

- d) analyse de l'ensemble de données déchiffré pour détecter si ce dernier comporte un élément non désiré par le dispositif destinataire.

Ledit procédé est remarquable en ce qu'il comprend en outre les étapes suivantes:

- e) transmission, en direction d'un module d'analyse, d'un message selon lequel l'ensemble de données déchiffré comporte ou ne comporte pas un tel élément non désiré,

- f) analyse du message transmis,

- g) transmission, en direction du dispositif destinataire, de l'ensemble de données chiffré tel qu'émis initialement par le dispositif expéditeur, et, dans le cas où le message analysé à l'étape f) stipule que l'ensemble de données déchiffré comporte un tel élément non désiré, des informations selon lesquelles l'ensemble de données chiffré comporte cet élément non désiré.

Les avantages particuliers du procédé de transmission étant identiques à ceux du système introduit précédemment, ils ne seront pas rappelés ici.

Dans un mode de réalisation préféré du procédé selon l'invention, on a recours à la disposition suivante :

- à l'étape b), au moins une clé de chiffrement est obtenue en plus de la clé de déchiffrement, la clé de chiffrement étant compatible avec la clé de déchiffrement,

- entre les étapes d) et e) ont lieu :

  - une étape de suppression, dans l'ensemble de données déchiffré, de la totalité ou seulement d'une partie de l'élément non désiré qui a été détecté au cours de l'étape d),
  - une étape de reconstitution, à l'aide d'au moins la clé de chiffrement obtenue, de la totalité ou seulement d'une partie de l'ensemble de données chiffré transmis, à partir de l'ensemble de données déchiffré dont la totalité ou seulement une partie de l'élément non désiré a été supprimée au cours de l'étape de suppression,

- en plus du message transmis à l'étape e), est transmis l'ensemble de données déchiffré, dont la totalité ou seulement une partie de l'élément non désiré a été supprimée au cours de l'étape de suppression,

- au cours de l'étape g) est transmis, en direction du dispositif destinataire, soit l'ensemble de données chiffré transmis reconstitué en totalité, soit l'ensemble de données chiffré transmis reconstitué en partie.

D'autres caractéristiques et avantages de l'invention apparaîtront au cours de la description suivante de deux de ses modes de réalisation, donné à titre d'exemple non limitatif, en regard de la figure 1 annexée qui représente l'architecture générale du système de transmission selon la présente invention.

Comme on peut le voir sur la figure 1, le système selon la présente invention comprend :

- un dispositif expéditeur 1, tel que par exemple un ordinateur appartenant à une entreprise candidate, dans le cadre d'une réponse à un appel d'offre,
- un dispositif de transmission 2, tel que par exemple un serveur,
- un dispositif de chiffrement/déchiffrement 3, tel que par exemple un serveur,
- un dispositif d'archivage 4, tel que par exemple un serveur,
- un dispositif de désinfection 5, tel que par exemple un serveur,
- un dispositif destinataire 6, tel que par exemple un serveur appartenant à un organisme public destiné à dépouiller des appels d'offre.

L'ordinateur 1 est destiné à transmettre au serveur 6 un ensemble de données chiffré, via un réseau public, par exemple du type Internet.

Dans l'exemple représenté, l'ensemble de données est un document électronique contenant l'appel d'offre.

L'ordinateur 1 comprend :

- une interface de communication 1a, notamment un navigateur Web, avec le serveur de transmission 2,
- une mémoire 1b dans laquelle est enregistré un document à transmettre, le document ayant été préalablement chiffré à l'aide d'une clé de chiffrement K_E, d'une façon connue en tant que telle. Un tel chiffrement est selon les cas, unique ou multiple (exemple: surchiffrement).

Le format du document chiffré obtenu est du type PKCS#7 (de l'anglais Public Key Cryptography Standards), CMS (de l'anglais Cryptographic Message Syntax), XML (de l'anglais Extensible Markup Language), PGP, etc....

Le serveur de transmission 2 comprend :

- une interface de communication 2a avec l'ordinateur 1,

- un module logiciel applicatif 2b relié à l'interface 2a et destiné à traiter les requêtes reçues par l'interface 2a,

- une mémoire 2c reliée au module applicatif 2b et destiné à stocker temporairement le document chiffré reçu,

- une interface de communication 2d avec le serveur de chiffrement/déchiffrement 3,

- une interface de communication 2e avec le dispositif destinataire 6.

Le serveur de chiffrement /déchiffrement 3 comprend :

- une interface de communication 3a avec le serveur de transmission 2,

- un module logiciel applicatif 3b relié à l'interface 3a et destiné à traiter les requêtes reçues par l'interface 3a,

- un module de déchiffrement D,

- un module de chiffrement E,

- une interface de communication 3c avec le serveur d'archivage 4,

- une interface de communication 3d avec le serveur de désinfection 5.

Le serveur d'archivage 4 comprend :

- une interface de communication 4a avec le serveur de chiffrement/chiffrement 3,

- un module logiciel applicatif 4b relié à l'interface 4a et destiné à traiter les requêtes reçues par l'interface 4a,

- une base de données 4c qui est reliée au module applicatif 4b et dans laquelle sont enregistrées une ou plusieurs clés de déchiffrement K_D qui sont compatibles respectivement avec la ou les clés de chiffrement K_E précitées.

Dans l'état de la technique, le serveur d'archivage 4 est plus connu sous le terme de serveur de séquestre et de recouvrement.

Le serveur de désinfection 5 comprend :

- une interface de communication 5a avec le serveur de chiffrement/déchiffrement 3,

- un module logiciel applicatif 5b relié à l'interface 5a et destiné à traiter les requêtes reçues par l'interface 5a,

- un module d'analyse AN5 destiné à détecter si le document déchiffré dans le serveur de chiffrement/déchiffrement 3 comporte un élément non désiré par le serveur destinataire 6,

- un module d'élimination EL5 destiné à supprimer, dans l'ensemble de données déchiffré, la totalité ou seulement une partie de l'élément non désiré susceptible d'être détecté par le module d'analyse AN5.

On va maintenant décrire en référence à la figure 1 le procédé de transmission conformément à la présente invention.

Dans un souci de simplification, on considérera que le document électronique transmis est associé à une seule clé de chiffrement K_E et à une seule clé de déchiffrement K_D.

Une entreprise, candidate dans le cadre d'un appel d'offre, se connecte auprès du serveur de transmission 2, au moyen de l'ordinateur 1, via un réseau public, tel que par exemple Internet.

Une fois la connexion établie, le navigateur 1a envoie alors en direction du serveur de transmission 2, via le réseau Internet, un message M1 comportant le document chiffré.

L'interface 2a reçoit le message M1 et le transmet au module applicatif 2b qui enregistre le document chiffré dans la mémoire 2c.

Le module applicatif 2b envoie en retour à l'interface 2d une copie du document chiffré.

L'interface 2d envoie alors, en direction du serveur de chiffrement/déchiffrement 3, un message M2 contenant le document chiffré, via un réseau privé, par exemple Intranet.

Au cours d'une première étape E1, l'interface de communication

3a du serveur de chiffrement/déchiffrement 3 reçoit le message M2 et le transmet au module applicatif 3b.

Au cours d'une seconde étape E2, le module applicatif 3b exécute un programme d'analyse du document chiffré reçu de façon à déterminer quelle est la clé de déchiffrement K_D compatible avec la clé de chiffrement K_E.

Au cours d'une troisième étape E3, l'interface de communication 3c émet, en direction du serveur d'archivage 4, un message M3 qui comprend une requête en recouvrement de la clé de déchiffrement K_D qui a été déterminée à l'étape E2.

L'interface de communication 4a du serveur d'archivage 4 reçoit le message M3 et le transmet au module applicatif 4b. Le module applicatif 4b extrait alors de la base de données 4c la clé de déchiffrement K_D demandée et la transmet à l'interface 4a. Cette dernière émet alors, en direction du serveur de chiffrement/déchiffrement 3, via le réseau Intranet, un message M4 contenant ladite clé de déchiffrement K_D.

Au cours d'une quatrième étape E4, l'interface de communication 3c du serveur 3 reçoit le message M4 et le transmet au module applicatif 3b. Au cours d'une cinquième étape E5, le module de déchiffrement D exécute un programme de déchiffrement du document chiffré reçu, à l'aide de la clé de déchiffrement K_D obtenue.

Au cours d'une sixième étape E6, l'interface de communication 3d émet, en direction du serveur de désinfection 5, via le réseau Intranet, un message M5 qui comprend une requête en désinfection du document déchiffré.

L'interface de communication 5a du serveur de désinfection 5 reçoit le message M5 et le transmet au module applicatif 5b. Le module d'analyse AN5 exécute un programme d'analyse du document déchiffré reçu pour détecter si ce dernier comporte un élément non désiré.

Si le module applicatif AN5 ne détecte pas un tel élément non désiré, l'interface de communication 5a émet, en direction du serveur de chiffrement/déchiffrement 3, via le réseau Intranet, un message M6 intitulé par exemple "document sain".

Si, en revanche, le module applicatif AN5 détecte un tel élément non désiré, l'interface de communication 5a émet, en direction du serveur de chiffrement/déchiffrement 3, via le réseau Intranet, un message M6 intitulé par exemple "document infecté".

Au cours d'une septième étape E7, l'interface de communication 3d reçoit le message M6 et le transmet au module applicatif 3b.

Au cours d'une huitième étape E8, le module 3b lance un programme d'analyse de l'intitulé du message M6 reçu.

Si l'intitulé du message M6 est "document sain", l'interface de communication 3a, au cours d'une neuvième étape E9.1, émet en direction du serveur de transmission 2, via le réseau Intranet, un message M7 intitulé par exemple "OK".

Si l'intitulé du message M6 est "document infecté", l'interface de communication 3a, au cours d'une huitième étape E9.2, émet en direction du serveur de transmission 2, via le réseau Intranet, un message M7 intitulé par exemple "non OK".

L'interface de communication 2a du serveur de transmission 2 reçoit le message M7 et le transmet au module applicatif 2b. Le module d'analyse AN2 analyse le message M7.

Si le message M7 reçu est intitulé "OK", le module applicatif 2b extrait le document chiffré de la mémoire 2c et le transmet à l'interface de communication 2e qui elle-même transmet, en direction du serveur destinataire 6, via le réseau Internet, un message M8 contenant ledit document chiffré extrait.

Si le message M7 reçu est intitulé " non OK", le module applicatif 2b extrait tout de même le document chiffré de la mémoire 2c et le transmet à l'interface de communication 2e qui elle-même transmet, en direction du serveur destinataire 6, via le réseau Internet, un message d'alerte M8 intitulé "document infecté" et contenant ledit document chiffré extrait.

Le serveur 6 reçoit alors le message M8 et le mémorise.

L'organisme public, détentrice du serveur 6, est ainsi en possession soit d'un document chiffré sain qui ne sera déchiffré

qu'ultérieurement, c'est à dire lors du dépouillement officiel des appels d'offre, soit d'un document chiffré infecté que l'organisme public ne prendra peut-être pas le risque de déchiffrer ultérieurement.

Selon une variante du système et du procédé qui viennent d'être décrits ci-dessus, la base de données 4c du serveur d'archivage 4 contient également la clé de chiffrement K_E compatible avec la clé de déchiffrement K_D. A cet effet, suite à la détermination, par le module applicatif 3b, de la clé de déchiffrement K_D, l'interface de communication 3c émet en direction du serveur d'archivage 4, au cours de l'étape E3 précitée, un message M3 qui comprend non seulement une requête en recouvrement de la clé de déchiffrement K_D, mais également une requête en recouvrement de la clé de chiffrement K_E.

L'interface de communication 4a du serveur d'archivage 4 reçoit le message M3 et le transmet au module applicatif 4b. Le module applicatif 4b extrait alors de la base de données 4c la clé de déchiffrement K_D et la clé de chiffrement K_E demandées et transmet ces dernières à l'interface 4a. L'interface 4a émet alors, en direction du serveur de chiffrement/déchiffrement 3, via le réseau Intranet, un message M4 contenant ladite clé de déchiffrement K_D et ladite clé de chiffrement K_E.

L'interface de communication 3c du serveur de chiffrement/déchiffrement 3 reçoit le message M4 et le transmet au module applicatif 3b. Le module de déchiffrement D exécute un programme de déchiffrement du document chiffré reçu, à l'aide de la clé de déchiffrement K_D obtenue.

Une fois cette étape terminée, l'interface de communication 3d émet, en direction du serveur de désinfection 5, un message M5 qui comprend une requête en désinfection du document déchiffré.

L'interface de communication 5a du serveur de désinfection 5 reçoit le message M5 et le transmet au module applicatif 5b. Le module d'analyse AN5 exécute le programme d'analyse précité, afin de détecter si le document déchiffré reçu comporte un élément non désiré.

Si le module d'analyse AN5 ne détecte pas un tel élément non

désiré, l'interface de communication 5a émet, en direction du serveur de chiffrement/déchiffrement 3, via le réseau Intranet, un message M6 intitulé par exemple "document sain".

Si, en revanche, le module d'analyse AN5 détecte un tel élément non désiré, le module d'élimination EL5 exécute un programme de désinfection, tel que par exemple un anti-virus, pour supprimer tout ou partie de l'élément non désiré. L'interface de communication 5a émet ensuite en direction du serveur de chiffrement/déchiffrement 3, via le réseau Intranet, un message M6 intitulé par exemple "document infecté" et comportant le document déchiffré débarrassé, en totalité ou en partie, de l'élément non désiré.

L'interface de communication 3d reçoit le message M6 et le transmet au module applicatif 3b. L'étape E8 précitée est alors effectuée mais diffère en ce sens que le programme effectue une analyse non seulement de l'intitulé du message M6 reçu, mais également du document déchiffré contenu dans le message M6 reçu.

Si l'intitulé du message M6 reçu est "document sain", l'étape E9.1 précitée est effectuée.

Si l'intitulé du message M6 reçu est "document infecté", et que le document déchiffré contenu dans le message M6 est débarrassé de l'élément non désiré, le module de chiffrement E lance un programme de rechiffrement du document déchiffré à l'aide de la clé K_E obtenue précédemment. L'interface de communication 3a émet alors en direction du serveur de transmission 2, via le réseau Intranet, un message M7 intitulé par exemple " non OK, SAIN " et comportant le document chiffré débarrassé de l'élément non désiré.

Si l'intitulé du message M6 reçu est "document infecté", et que le document déchiffré contenu dans le message M6 est débarrassé seulement en partie de l'élément non désiré, le module de chiffrement E lance un programme de rechiffrement du document déchiffré, à l'aide de clé K_E obtenue précédemment, de façon à reconstituer le document chiffré initial, seulement en partie, les parties infectées du document étant remplacées chacune par un message d'erreur. L'interface de communication 3a émet alors en direction du

serveur de transmission 2, via le réseau Intranet, un message M7 intitulé par exemple " non OK, INFECTÉ " et comportant le document chiffré reconstitué en partie.

L'interface de communication 2a du serveur de transmission 2 reçoit le message M7 et le transmet au module applicatif 2b. Le module d'analyse AN2 lance un programme d'analyse de l'intitulé du message M7.

Si le message M7 reçu est intitulé "OK", le module applicatif 2b extrait le document chiffré de la mémoire 2c et le transmet à l'interface de communication 2e qui elle-même transmet, en direction du serveur destinataire 6, via le réseau Internet, un message M8 contenant ledit document chiffré extrait.

Si le message M7 reçu est intitulé " non OK, SAIN", l'interface de communication 2e transmet en direction du serveur destinataire 6, via le réseau Internet, un message d'alerte M8 intitulé par exemple "document infecté" et contenant le document émis initialement par l'ordinateur 1.

L'interface de communication 2e transmet en outre en direction du serveur destinataire 6, via le réseau Internet, un message comportant le document chiffré reçu débarrassé de l'élément non désiré.

Si le message M7 reçu est intitulé "non OK, INFECTÉ", l'interface de communication 2e transmet en direction du serveur 6, via le réseau Internet, un message d'alerte M8 intitulé par exemple "document en partie infecté" et contenant le document émis initialement par l'ordinateur 1.

L'interface de communication 2e transmet en outre en direction du serveur destinataire 6, via le réseau Internet, un message comportant le document chiffré reçu débarrassé de l'élément non désiré.

La fin du procédé de transmission se déroule ensuite de la façon qui a été décrite ci-dessus en référence à la figure 1.

Dans l'exemple représenté, les connexions entre les différents dispositifs 1 à 6 sont par exemple de type http (de l'anglais Hyper Text Transfer Protocol). Plus spécifiquement, la connexion entre l'ordinateur 1 et le serveur de transmission 2, entre le serveur de transmission 2 et le serveur de chiffrement/déchiffrement 3, et entre le serveur de chiffrement/déchiffrement 3 et

le serveur d'archivage 4 est sécurisée. Dans l'exemple représenté, elle est de type https (de l'anglais Hyper Text Transfer Protocol Secure).

Selon une variante du système représenté sur la figure 1, les serveurs de chiffrement/déchiffrement 3 et de désinfection 5 sont regroupés au sein d'un unique et même serveur de façon à éviter la transmission en clair des documents déchiffrés.

Selon une autre variante du système représenté sur la figure 1, le système comprend une pluralité de serveurs de chiffrement/déchiffrement 3. A cet effet, le serveur de transmission 2 ou, en remplacement de ce dernier, un serveur proxy, comprend un module logiciel dans lequel est installé un programme chargé de décomposer le document chiffré en provenance de l'ordinateur 1 en plusieurs sous documents chiffrés, puis d'aiguiller chacun de ces sous documents en direction d'un serveur de chiffrement/déchiffrement 3 qui lui est associé.

Selon encore une autre variante du système représenté sur la figure 1, dans le cas où les clés de chiffrement sont des clés publiques encapsulées dans des certificats, ceux-ci étant gérés par une infrastructure à clé publique (ICP), le serveur d'archivage 4 fait partie intégrante de cette infrastructure.

Dans ces conditions, le serveur de chiffrement/déchiffrement 3 fait également partie intégrante de cette infrastructure de façon à ce que la transmission des clés séquestrées K_E ou K_D soit effectuée uniquement à l'intérieur de l'infrastructure et non vers un tiers qui n'en est pas le propriétaire.

L'avantage d'une telle infrastructure à clé publique est qu'elle permet d'ajouter des extensions aux certificats précités afin d'indiquer, pour un certificat donné:

- le ou les serveurs de chiffrement/déchiffrement 3 susceptibles d'analyser un document ou un sous document chiffré avec ce certificat,
- le ou les serveurs d'archivage 4 susceptibles de recouvrer la clé associée à ce certificat.

Il va de soi que le mode de réalisation et les variantes qui ont été

décrits ci-dessus ont été donnés à titre purement indicatif et nullement limitatif, et que de nombreuses modifications peuvent être facilement apportées par l'homme de l'art sans pour autant sortir du cadre de l'invention.

On pourrait par exemple imaginer que dans le cas où le module d'analyse AN2 analyse un message M7 intitulé " non OK", "non OK, SAIN" ou "non OK, INFECTÉ" il soit programmé pour que l'interface de communication 2a transmette en direction de l'ordinateur 1 et éventuellement du serveur destinataire 6, via le réseau Internet, un message d'alerte selon lequel le document chiffré à l'origine est infecté. En fonction du type de message M7 reçu, le message d'alerte pourrait contenir des précisions telles que la nature de l'élément non désiré qui a été détecté, la désignation des parties infectées du document chiffré transmis, etc....Le message d'alerte serait envoyé par exemple selon le protocole http, sous forme d'un courrier électronique, d'un message court, etc...

REVENDICATIONS

1. Système de transmission d'un ensemble de données chiffré depuis un dispositif expéditeur (1) vers un dispositif destinataire (6), ledit système comprenant :

- des premiers moyens de communication (2a, 2b, 2d) pour transmettre un ensemble de données chiffré émis par le dispositif expéditeur (1),
- des seconds moyens de communication (3c) pour dialoguer avec des moyens (4) d'archivage de clés afin d'obtenir au moins une clé de déchiffrement (K_D) qui est associée audit ensemble de données chiffré transmis,
- des moyens (D) de déchiffrement dudit ensemble de données chiffré transmis, au moyen de ladite clé de déchiffrement obtenue, pour obtenir un ensemble de données déchiffré,
- des premiers moyens d'analyse (AN5) pour analyser ledit ensemble de données déchiffré afin de détecter si ce dernier comporte un élément non désiré par le dispositif destinataire (6),

ledit système étant caractérisé en ce qu'il comprend en outre :

- des troisièmes moyens de communication (3a), pour transmettre un message selon lequel l'ensemble de données déchiffré comporte ou ne comporte pas un tel élément non désiré,
- des seconds moyens d'analyse (AN2) pour analyser ledit message transmis,
- des quatrièmes moyens de communication (2e) pour transmettre en direction du dispositif destinataire (6) :
  - soit ledit ensemble de données chiffré tel qu'émis initialement par le dispositif expéditeur (1), dans le cas où le message analysé par les seconds moyens d'analyse (AN2) stipule que l'ensemble de données déchiffré ne comporte pas un tel élément non désiré,
  - soit un message d'avertissement selon lequel l'ensemble de

données chiffré comporte un tel élément non désiré, dans le cas où le message analysé par les seconds moyens d'analyse (AN2) stipule que l'ensemble de données déchiffré comporte cet élément non désiré.

2. Système selon la revendication 1, comprenant en outre :

- des moyens d'élimination (EL5) pour supprimer, dans l'ensemble de données déchiffré, la totalité ou seulement une partie dudit élément non désiré susceptible d'être détecté par lesdits premiers moyens d'analyse (AN5),

- des moyens de restitution (E) pour reconstituer, à l'aide d'au moins une clé de chiffrement K_E compatible avec ladite clé de déchiffrement K_D , la totalité ou seulement une partie de l'ensemble de données chiffré transmis, à partir dudit ensemble de données déchiffré dans lequel lesdits moyens d'élimination (EL5) ont supprimé la totalité ou seulement une partie dudit élément non désiré, ladite clé de chiffrement étant obtenue au préalable par les seconds moyens de communication (3c) en plus de ladite clé de déchiffrement,

et dans lequel :

- lesdits troisièmes moyens de communication (3a) transmettent en outre l'ensemble de données chiffré reconstitué en totalité ou en partie,

- lesdits quatrièmes moyens de communication (2e) transmettent en direction du dispositif destinataire (6), en plus dudit message d'avertissement, soit l'ensemble de données chiffré transmis reconstitué en totalité, soit l'ensemble de données chiffré transmis reconstitué en partie.

3. Système selon la revendication 1 ou 2, dans lequel le message d'avertissement est accompagné du document tel que chiffré initialement par le dispositif expéditeur (1).

4. Système selon la revendication 1 ou 2, dans lequel lesdits seconds moyens de communication (3c), lesdits moyens de déchiffrement (D) et de restitution (E), lesdits premiers moyens d'analyse (AN5), lesdits moyens d'élimination (EL5), ainsi que lesdits troisièmes moyens de communication (3a), sont regroupés dans un seul dispositif.

5. Système selon la revendication 1 ou 2, dans lequel lesdits seconds

moyens de communication (3c), les moyens de déchiffrement (D), de restitution (E) et d'archivage (4), ainsi que lesdits troisièmes moyens de communication (3a), sont regroupés dans une infrastructure à clés publiques (ICP).

6. Système selon la revendication 1 ou 2, dans lequel lesdits seconds moyens de communication (3c), lesdits premiers moyens d'analyse (AN5), lesdits moyens de déchiffrement (D), d'élimination (EL5), d'archivage (4) et de restitution (E), ainsi que lesdits troisièmes moyens de communication (3a), sont regroupés dans un seul dispositif.

7. Procédé de transmission d'un ensemble de données chiffré depuis un dispositif expéditeur (1) vers un dispositif destinataire (6), ledit procédé comprenant les étapes suivantes :

- a) transmission d'un ensemble de données chiffré depuis le dispositif expéditeur (1),
- b) dialogue avec des moyens (4) d'archivage de clés afin d'obtenir au moins une clé de déchiffrement (K_D) qui est associée audit ensemble de données chiffré transmis,
- c) déchiffrement dudit ensemble de données chiffré transmis, au moyen de ladite clé de déchiffrement obtenue,
- d) analyse dudit ensemble de données déchiffré pour détecter si ce dernier comporte un élément non désiré par le dispositif destinataire (6),

ledit procédé étant caractérisé en ce qu'il comprend en outre les étapes suivantes:

- e) transmission d'un message selon lequel l'ensemble de données déchiffré comporte ou ne comporte pas un tel élément non désiré,
- f) analyse dudit message transmis,
- g) transmission, en direction du dispositif destinataire (6) :
  - soit dudit ensemble de données chiffré tel qu'émis initialement par le dispositif expéditeur (1), dans le cas où le message analysé par les seconds moyens d'analyse (AN2) stipule que l'ensemble de données déchiffré ne comporte pas un tel élément non désiré,

- soit d'un message d'avertissement selon lequel l'ensemble de données chiffré comporte un tel élément non désiré, dans le cas où le message analysé par les seconds moyens d'analyse (AN2) stipule que l'ensemble de données déchiffré comporte cet élément non désiré.

8. Procédé selon la revendication 7, au cours duquel :

- à l'étape b), au moins une clé de chiffrement K_E est obtenue en plus de ladite au moins une clé de déchiffrement K_D, ladite clé de chiffrement étant compatible avec la clé de déchiffrement,

- entre les étapes d) et e) ont lieu :

  - une étape de suppression, dans l'ensemble de données déchiffré, de la totalité ou seulement d'une partie dudit élément non désiré qui a été détecté au cours de l'étape d),
  - une étape de reconstitution, à l'aide de ladite au moins une clé de chiffrement obtenue à l'étape b), de la totalité ou seulement d'une partie de l'ensemble de données chiffré transmis, à partir dudit ensemble de données déchiffré dont la totalité ou seulement une partie dudit élément non désiré a été supprimée au cours de l'étape de suppression,

- en plus dudit message transmis à l'étape e), est transmis l'ensemble de données déchiffré, dont la totalité ou seulement une partie dudit élément non désiré a été supprimée au cours de ladite étape de suppression,

- au cours de l'étape g), en plus dudit message d'avertissement, est transmis en direction du dispositif destinataire (6), soit l'ensemble de données chiffré transmis reconstitué en totalité, soit l'ensemble de données chiffré transmis reconstitué en partie.

9. Procédé selon la revendication 7 ou 8, au cours duquel ledit message d'avertissement est accompagné du document tel que chiffré initialement par le dispositif expéditeur (1).

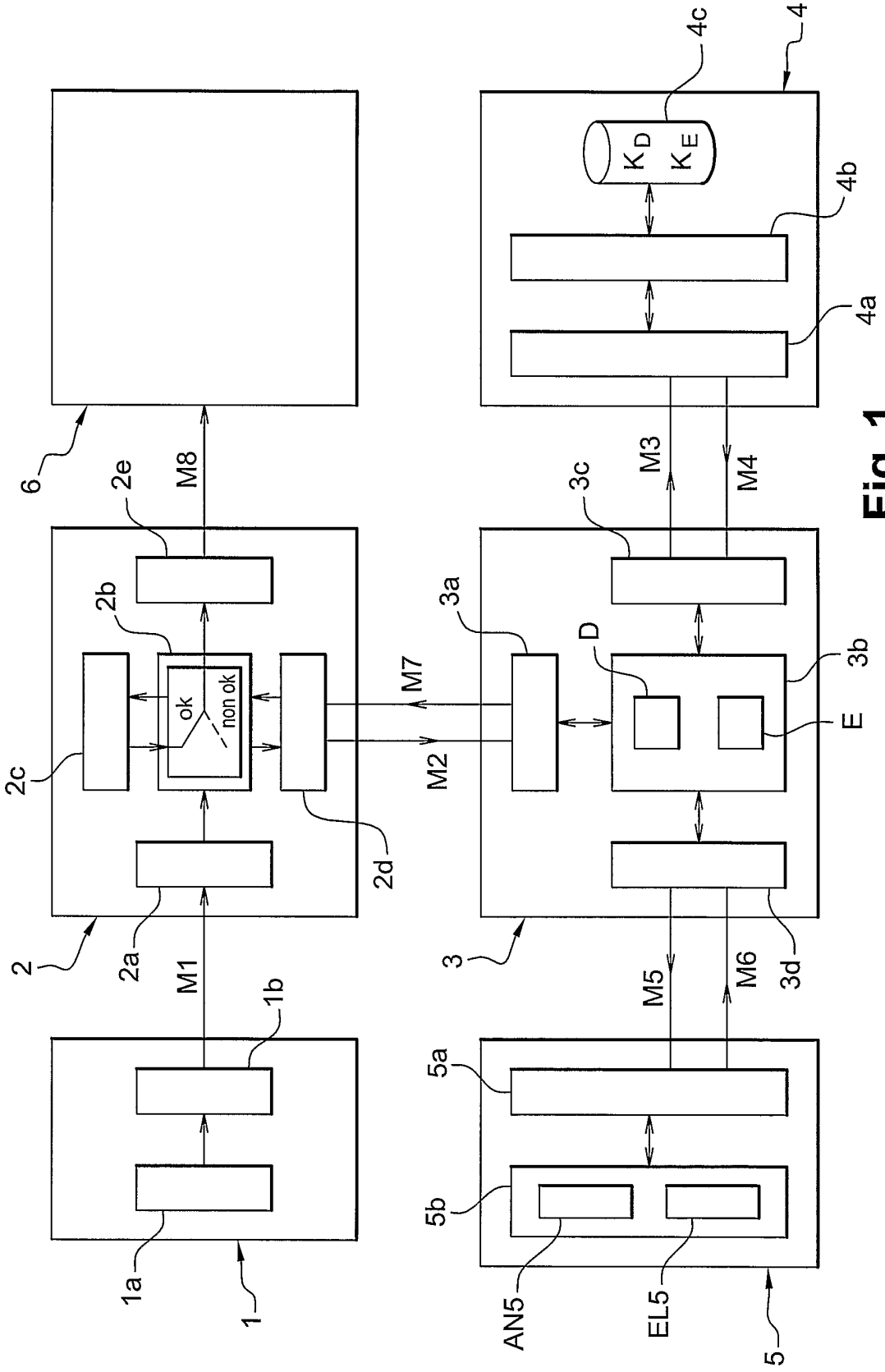

6
2e
M8
2b
ok
non ok
2c
2d
M7
M2
3a
D
3b
E
2
2a
M1
1b
1a
1
3
M5
M6
3d
5a
5b
AN5
EL5
5
3c
M3
M4
4c
4
K_D
K_E
4b
4a

Fig. 1