(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 737 067**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **96 09087**

(51) **Int Cl⁶ : H 04 L 9/32**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 19.07.96.

(30) **Priorité** : 19.07.95 US 503984.

(43) **Date de la mise à disposition du public de la demande :** 24.01.97 Bulletin 97/04.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

(71) **Demandeur(s) :** *PREMENOS CORP* — US.

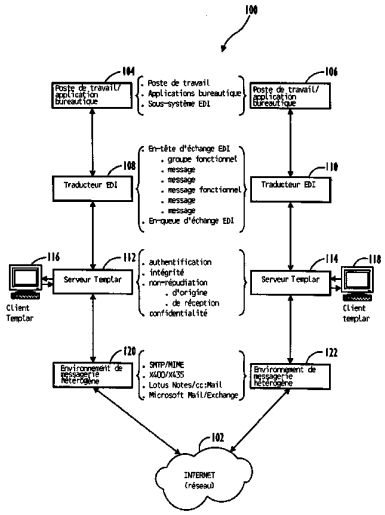
(72) **Inventeur(s) :** JENKINS LEW et PASETES EMMANUEL K.

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

(74) **Mandataire :** CABINET BEAU DE LOMENIE.

(54) SYSTEME ET PROCEDE PERMETTANT DE REALISER DES COMMUNICATIONS DU TYPE ECHANGE DE DONNEES ELECTRONIQUE SUR UN RESEAU OUVERT.

(57) L'invention concerne un système de télécommunications sur un réseau public ouvert (120, 102, 122) où sont échangées des communications d'échange EDI entre des ordinateurs émetteur (112) et récepteur (114), qui possèdent chacun une clé publique et une clé privée, la communication d'échange EDI possédant un message d'accusé de réception d'EDI. Le système comprend un moyen de calcul d'un premier code de hachage (MDS) pour ladite communication EDI venant de l'ordinateur émetteur, un moyen insérant ce code en un emplacement prédéterminé du message d'accusé de réception, un moyen de calcul d'un deuxième code de hachage du message d'accusé de réception qui crypte le deuxième code à l'aide de la clé privée de l'ordinateur émetteur, un moyen insérant ce deuxième code en un emplacement prédéterminé du message d'accusé de réception, un moyen qui transmet la communication EDI et le message d'accusé de réception numériquement signé audit ordinateur récepteur, et un moyen associé à l'ordinateur récepteur et servant à recevoir et traiter la communication EDI reçue et le message d'accusé de réception numériquement signé afin de fournir une authentification et une non-répudiation de la communication EDI par l'ordinateur émetteur, ledit moyen associé de l'ordinateur récepteur décryptant à l'aide de ladite clé publique de l'ordinateur émetteur le deuxième code de hachage crypté.



FR 2 737 067 - A1

La présente invention concerne des procédés et des systèmes permettant d'effectuer un EDI (échange de données électronique) dans des conditions de sécurité sur un réseau en système ouvert, par exemple le réseau INTERNET, et, plus particulièrement, un procédé et un système perfectionnée permettant d'assurer un système de messagerie EDI dans des conditions de sécurité sur un réseau ouvert qui emploie un schéma de cryptage par clés publique/privée du type RSA, afin de délivrer, de manière sûre, une authentification et une non-répudiation d'à la fois l'origine et la réception.

Les systèmes de télécommunications de sécurité à clés publiques/privées fonctionnant sur un réseau de type ouvert sont bien connus, comme décrit dans les brevets d'E.U.A n° 4 578 531, 4 471 164, 5 268 962, 5 142 577, 4 893 338, 5 222 140, 5 261 002, 5 073 934, 5 303 303, 5 297 208, 5 369 705, 5 351 293, 5 375 169, 5 224 166, 5 253 294 et 5 237 611. Le schéma de cryptage par clés publique/privée de type RSA est un système de codage par clé publique bien connu permettant de produire des messages de sécurité sur un réseau de type ouvert, comme le réseau INTERNET, et ce schéma est décrit dans divers brevets des E.U.A délivrés, comme les brevets des E.U.A n° 4 405 829, 4 424 414, 4 200 770, 4 218 582, 5 073 935 et 4 723 284 dont les contenus sont ici incorporés à titre de références. De plus, le concept de non-répudiation de l'origine est bien connu, comme décrit dans les brevets des E.U.A n° 5 226 709 et 5 367 573, ainsi que les systèmes dans lesquels des signatures numériques sont employées dans des systèmes codés par clés publique/privée tels que décrit dans les brevets des E.U.A n° 5 311 591, 5 214 702, 5 337 360, 4 868 877, 5 001 752, 5 005 200, 5 136 643, 5 018 196, 4 885 777, 4 267 782, 5 351 302, 5 208 858, 5 299 263, 5 142 578, 4 987 593, 4 991 210, 5 339 361, 5 373 558, 4 625 076 et le système Entrust commercialisé par la société Northern Telecom. En outre, divers autres systèmes de transmission de sécurité ont été mis au point au fur et à mesure des années dans le but d'essayer d'assurer des communications professionnelles sûres sur des réseaux publics/privés, comme décrit dans les brevets des E.U.A n° 5 369 702, 4 876 716, 5 199 074, 4 823 388, 5 268 962, 5 022 080, 5 136 646 et 5 204 961. De plus, l'utilisation de l'EDI (échange de données ou de documents électronique), pour transmettre des communications professionnelles d'égal à égal est bien connue dans la technique, comme décrit par exemple dans le brevet des E.U.A n° 5 202 977, cédé à la présente cessionnaire, ou dans le brevet des E.U.A ci-dessus mentionné n° 5 337 360. Toutefois, la demanderesse n'a eu connaissance d'aucune tentative aboutie d'utiliser le réseau INTERNET, ou tout autre réseau de

type ouvert largement accessible, comme des lignes téléphoniques ou un quelconque système TCP/IP (protocoles connus sous l'appellation de Transport Control Protocol/ Internet Protocol), dans lequel un système de codage par clé publique ou privée sûr, comme par exemple celui proposé par la société RSA, a été combiné avec succès à l'EDI de manière à fournir une authentification et une non-répudiation d'à la fois l'origine et la réception dans une transaction privée d'égal à égal sûre pouvant avoir lieu à tout moment sur le réseau de type ouvert sans être obligé de faire appel à la gestion de mots de passe, tout en procédant également à la vérification de l'intégrité du message. Ce système élimine la nécessité des réseaux à valeur ajoutée privés et des autres réseaux privés de tiers, tout en assurant la possibilité commerciale de transactions d'affaires privée faites d'égal à égal sur un réseau ouvert largement disponible à l'aide l'EDI. La certitude apportée quant à la non-répudiation et à l'authentification élimine la possibilité que l'autre partie nie que la transaction ait été approuvée et elle élimine tout doute concernant le contenu du document EDI ayant donné naissance à la transaction. L'aptitude du procédé et du système selon l'invention à fournir un système de messagerie EDI de sécurité en combinaison avec un système codé par clés publique/privée du type RSA permet de surmonter les inconvénients de la technique antérieure.

Le procédé et le système selon l'invention comprennent l'utilisation du message d'accusé de réception d'EDI, ou AUTACK, comme document pour fournir la signature numérique dans un système à clé publique/clé privée, où l'AUTACK est signé par un code de hachage crypté venant de la communication d'échange EDI, qui a été crypté à l'aide de la clé privée de l'émetteur, comme dans un système à clé publique/clé privée du type RSA, et ils constituent une amélioration par rapport à ces systèmes. Puisque l'AUTACK, ou accusé de réception fonctionnel, a été rendu hermétique à l'aide de la clé privée de l'émetteur de l'accusé de réception fonctionnel, c'est-à-dire le récepteur du message original, lorsque l'émetteur original décrypte le message AUTACK de réponse à l'aide de la clé publique du récepteur, il est assuré que le récepteur visé a émis réellement l'AUTACK de réponse, ou accusé de réception, de même qu'il est assuré de l'intégrité de la réception du fait que le code de hachage correct a été détecté.

On utilise de préférence le message AUTACK de l'EDI, par exemple le message AUTACK d'EDIFACT, qui est une norme internationale générique d'EDI pour l'administration, le commerce et les relations marchandes, pour délivrer, de manière sûre et voulue, une authentification, une non-répudiation de l'origine ou de la réception, et un accusé de réception ou un refus d'accuser la réception

relativement à une ou plusieurs enveloppes EDI, comme les enveloppes X.12 ou EDIFACT par exemple. Dans le procédé et le système présentement préférés de l'invention, au cours du processus d'authentification et de non-répudiation de l'origine, l'émetteur calcule un condensé de message, ou resserrement, voulu à partir de l'EDI, par exemple le MD5 (condensé de message, version 5) de la communication d'échange EDI tout entière, et insère la valeur correspondante dans le message AUTACK. L'émetteur calcule ensuite de préférence le MD5 du message AUTACK et signe numériquement l'AUTACK en cryptant le MD5 calculé à l'aide de la clé privée de l'émetteur, et il insère cette valeur dans le message AUTACK. Ainsi, l'AUTACK, ou message d'accusé de réception d'EDI, est de préférence utilisé pour produire la signature. Le récepteur, après réception du message, décrypte alors la communication d'échange EDI, si elle est cryptée, et calcule le MD5 de la communication d'échange EDI reçue. Si la non-répudiation d'origine est souhaitée, le récepteur décrypte alors le message AUTACK à l'aide de la clé publique de l'émetteur. La valeur obtenue à l'aide de ce décryptage est, dans cet exemple, le MD5 du message AUTACK. Le MD5 du message AUTACK est ensuite calculé et comparé avec la valeur décryptée. Si les deux valeurs sont égales, l'intégrité de l'AUTACK est vérifiée et la non-répudiation de l'origine est établie. On compare ensuite le MD5 de la communication d'échange EDI avec le MD5 de l'échange EDI qui a été inséré dans l'AUTACK et, si tous deux sont égaux, alors l'intégrité de l'échange EDI est vérifiée, et la non-répudiation de l'origine est établie.

Pour établir ensuite la non-répudiation de la réception, alors, après vérification de l'intégrité et de l'authenticité de la communication d'échange EDI reçue de la manière ci-dessus décrite, un nouvel AUTACK, ou AUTACK de réponse, est créé par peuplement de tous les segments et de tous les éléments de la manière appropriée, le MD5 calculé est numériquement signé à l'aide de la clé privée du récepteur, le MD5 numériquement signé est inséré dans l'AUTACK de réponse, des segments appropriés de l'AUTACK de réponse sont peuplés, et l'AUTACK de réponse ainsi préparé est transmis à l'émetteur. Dès réception de cet AUTACK de réponse, l'émetteur de l'original vérifie alors la signature numérique venant du récepteur de son message original en décryptant celui-ci à l'aide de la clé publique du récepteur. La valeur obtenue suite à ce décryptage et le MD5 de l'AUTACK de réponse reçu. L'émetteur original, qui a reçu l'AUTACK de réponse de la part du récepteur de ce message, calcule alors le MD5 de l'AUTACK de réponse reçu et, si le MD5 calculé est égal au MD5 décrypté, l'intégrité de

l'AUTACK est préservée et la non-répudiation d'origine de l'AUTACK est établie. De plus, si le MD5 contenu dans le segment particulier de l'AUTACK reçu, où il a été inséré par l'émetteur, est égal au MD5 de l'échange EDI précédemment transmis et que l'accusé de réception est positif, ce qui peut être déduit du contrôle du code de sécurité du message AUTACK, alors ce qui suit est implicite pour l'établissement de la non-répudiation de la réception : la communication d'échange EDI considérée est connue à la fois de l'émetteur et du récepteur puisque le MD5 de la communication d'échange EDI et le numéro d'échange sont contenus dans le message AUTACK et ont été dûment reconnus, l'intégrité et l'authenticité de la communication d'échange EDI, au moment de la réception, ont été vérifiées, et le récepteur ne nie pas avoir reçu la communication d'échange EDI considérée.

La capacité de négocier ou de conclure des affaires sur une base égalitaire en utilisant un réseau public ouvert, comme le réseau INTERNET, sans qu'il soit besoin de gérer des mots de passe, peut être contrôlée, dans toute la mesure voulue, par les participants à la négociation via l'utilisation d'accords de partenaires de négociation pour fournir une certification par échange de clés ou via la confiance faite à l'autorité d'un certificat qui délivre et vérifie des trajets de clés publiques/privées. Ainsi, des transaction privées et sûres, faisant l'objet d'une authentification et d'une non-répudiation d'à la fois l'origine et la réception, en même temps que d'une vérification dans l'intégrité du message, et utilisant une EDI, peuvent être menés sur un réseau de télécommunications ouvert.

La description suivante, conçue à titre d'illustration de l'invention, vise à donner une meilleure compréhension de ses caractéristiques et avantages ; elle s'appuie sur les dessins annexés, parmi lesquels :

la figure 1 est un organigramme fonctionnel pouvant être associé au procédé et au système présentement préférés de l'invention, permettant d'effectuer une EDI de sécurité sur un réseau ouvert, comme le réseau INTERNET, afin de fournir l'intégrité, l'authentification, la non-répudiation de l'origine et du récepteur, ainsi que la confidentialité, à l'aide de l'EDI ;

la figure 2 est un organigramme fonctionnel de la partie du procédé et du système de la figure 1 assurant l'authentification et la non-répudiation de l'origine à l'aide du message AUTACK d'EDIFACT ;

la figure 3 est un organigramme fonctionnel, analogue à celui de la figure 2, de la partie du procédé et du système de la figure 1 assurant la non-répudiation du récepteur, à l'aide du message AUTACK d'EDIFACT ;

la figure 4 est un organigramme fonctionnel montrant la réception de messages de sécurité sur le réseau INTERNET selon le procédé et le système présentement préférés de l'invention ;

la figure 5 est un organigramme fonctionnel, analogue à celui de la figure 4, montrant l'émission de messages de sécurité sur le réseau INTERNET selon le procédé du système présentement préféré de l'invention ;

la figure 6 est un organigramme fonctionnel, analogue à celui de la figure 4, montrant la gestion de partenaires de négociation selon le procédé et le système présentement préférés de l'invention ;

la figure 7 est un organigramme fonctionnel, analogue à celui de la figure 4, montrant la gestion de listes de contrôle de connexion selon le procédé et le système présentement préférés de l'invention ;

la figure 8 est un organigramme fonctionnel, analogue à celui de la figure 4, montrant la gestion d'opérations de suivis selon le procédé et le système présentement préférés de l'invention ;

la figure 9 est un organigramme fonctionnel, analogue à celui de la figure 4, montrant la surveillance de travaux selon le procédé et le système présentement préférés de l'invention ;

la figure 10 est un diagramme fonctionnel de l'organisation du système employé pour mettre en oeuvre le procédé présentement préféré de l'invention ;

les figures 11 à 13 comprennent respectivement un organigramme fonctionnel, analogue à celui de la figure 4, montrant l'ensemble du procédé et du système présentement préférés des figures 1 à 10, où la figure 11 illustre la vérification du certificat, la figure 12 illustre le traitement de la TPA, et la figure 13 illustre le traitement par clé publique/clé privée ;

la figure 14 est une représentation simplifiée d'un affichage d'écran d'ordinateur typique selon le procédé et le système présentement préférés de l'invention, montrant les diverses options fonctionnelles devant être commandées par les utilisateurs pour assurer un système de messagerie de sécurité sur le réseau INTERNET, selon le procédé et le système présentement préférés de l'invention ;

les figures 15 à 21 sont des représentations simplifiées, analogues à celle de la figure 14, d'affichages d'écrans d'ordinateur typiques selon l'option PROFIL DES PARTENAIRES DE NEGOCIATION, présentée sur l'affichage d'écran de la figure 14 ;

les figures 22 à 28 sont des représentations simplifiées, analogues à celle de la figure 14, d'affichages d'écrans d'ordinateur typiques selon l'option

ACCORDS DE PARTENAIRES DE NEGOCIATION, présentée sur l'affichage d'écran de la figure 14, où la figure 28 illustre l'affichage d'écran RETRANSMISSION VERS L'EXTERIEUR, associée à l'envoi de messages électroniques de sécurité selon le procédé et le système présentement préférés de l'invention ;

les figures 29 à 33 sont des représentations simplifiées, analogues à celle de la figure 14, d'affichages d'écrans d'ordinateur typiques selon l'option GESTION DE CLES, présentée sur l'affichage d'écran de la figure 14 ; et

les figures 34 à 41 sont des représentations simplifiées, analogues à celle de la figure 14, d'affichages d'écrans d'ordinateur typiques selon l'option SUIVIS, présentée sur l'affichage d'écran de la figure 14, les figures 35 à 38 illustrant plus spécialement le suivi d'échanges et les figures 39 à 41 illustrant plus spécialement le suivi d'une liste de contrôle de connexion.

On va maintenant se reporter de manière plus détaillée aux dessins et, pour commencer, à la figure 1, qui montre l'organigramme fonctionnel du système 100 présentement préféré de l'invention, servant à assurer, dans des conditions de sécurité, un échange de données électronique (EDI) sur un réseau ouvert classique, comme le réseau INTERNET 102 offert sur le marché commercial. Le procédé et le système préférés selon l'invention sont mis en oeuvre dans un système qui est réalisé sous la marque déposée TEMPLAR, appartenant à la société cessionnaire. Comme cela sera expliqué de façon plus détaillée ci-après, en liaison avec les figures 2 à 41, le procédé et le système présentement préférés de l'invention fournissent l'intégrité, l'authentification, la non-répudiation d'à la fois l'origine et la réception, et la confidentialité, lorsqu'on utilise un EDI. Ceci est de préférence réalisé au moyen du message d'accusé de réception de l'EDI, ou l'AUTACK, comme document servant à offrir une signature numérique dans un système à clé publique/clé privée, qui est de préférence un système employant le schéma classique de cryptage par clé publique/clé privée RSA, comme le schéma de cryptage décrit dans les brevets des E.U.A n° 4 405 828, 4 424 414, 4 200 770 et 4 218 582, dont les contenus sont ici incorporés, dans leur totalité, à titre de références. Comme cela sera décrit de façon plus détaillée ci-après, l'AUTACK est de préférence rendu hermétique ou est signé à l'aide d'une signature numérique qui est de préférence créée par cryptage du MD5 (condensé de message, version 5) de l'AUTACK avec la clé privée du créateur de l'AUTACK, à savoir la clé privée de l'émetteur dans le processus préféré d'authentification et de non-répudiation de l'origine, comme illustré sur la figure 2, ou avec la clé privée du récepteur dans le

processus préféré de non-répudiation de la réception, comme représenté sur la figure 3. La signature numérique est ensuite insérée de préférence en une position prédéterminée de l'AUTACK et est émise à destination de l'autre partie de la transaction. Puisque l'AUTACK a été rendu hermétique à l'aide de la clé privée de l'émetteur de l'AUTACK, lorsque le récepteur de cet AUTACK décrypte l'AUTACK à l'aide de la clé publique de l'émetteur de cet AUTACK, il est assuré que le récepteur voulu de son message a réellement envoyé cet AUTACK, de même qu'il est assuré de l'intégrité de la réception du fait que le bon code de hachage (connu également sous l'appellation "code hash") a été détecté de la manière qui sera décrite ultérieurement. Selon l'invention, la clé secrète cryptée utilisée pour crypter le message ainsi que le message lui-même sont contenus dans le message PKCS.

Le MD5 est une valeur classique que l'on peut obtenir dans un message EDI en effectuant un "hachage" classique d'une certaine quantité, par exemple un échange EDI. Il existe une très faible probabilité pour que les MD5 de deux documents différents quelconques soient identiques et, par conséquent, le MD5 est de préférence utilisé pour établir l'intégrité d'échanges EDI selon le procédé présentement préféré de l'invention.

Comme cela est bien connu des utilisateurs de l'EDI, un message AUTACK est une norme UN/EDIFACT servant à donner une authentification et un accusé de réception. Selon le procédé et le système présentement préférés de l'invention, l'AUTACK consiste de préférence en l'USH, ou en-tête de sécurité, l'USB, l'USX servant à identifier le message, l'USY servant à maintenir les informations de sécurité sur le message considéré, l'USR, et quelques autres segments classiques que l'on trouve normalement dans un AUTACK.

De préférence, des informations telles que le type de réponse, l'étendue de l'application de sécurité, et la fonction de sécurité sont codés dans le segment USH. A titre d'exemple, le deuxième élément du segment USH peut contenir de préférence la valeur 2, ou quelques autres valeurs désignées, si l'AUTACK doit servir comme document vérifiant la non-répudiation de l'origine, ayant par exemple une cinquième zone de valeur 2, ou quelque autre valeur désignée, si un accusé de réception est demandé. Le segment USX contient de préférence le numéro d'échange de l'échange EDI considéré, ce qui lie le message considéré à l'AUTACK, et le segment USR est de préférence un support de résultat de sécurité et contient le MD5 numériquement signé de l'AUTACK, selon l'invention.

Comme on peut le voir également sur la figure 1, si l'on suppose qu'une transaction d'affaires à deux parties seulement, ayant lieu entre deux parties qui ont passé un accord de partenaires de négociation, chacune des parties possède un poste de travail d'ordinateur classique 104, 106, par exemple RS/6000, HP/9000 et SOLARIS ; un traducteur EDI classique 108, 110 ; un serveur logiciel/matériel intégré classique 112, 114, qui a été programmé pour fonctionner selon le procédé du système préféré de l'invention et qui contient des terminaux d'affichage d'ordinateur classiques 116, 118, pouvant fonctionner dans un environnement du type WINDOWS de Microsoft ou X-WINDOWS sous UNIX, servant à afficher des messages et des choix en fonction du procédé préféré de l'invention, ainsi que des messages et des documents transmis via l'EDI sur le réseau INTERNET 102 pour mettre en oeuvre le procédé de l'invention, les serveurs 112, 114 étant en mesure de réaliser les opérations voulues d'authentification, d'intégrité, de non-répudiation de l'origine et de la réception, et de confidentialité, selon l'invention. Comme représenté, les serveurs 112, 114 communiquent classiquement sur le réseau ouvert, par exemple le réseau INTERNET 102, via un environnement de messagerie hétérogène 120, 122, par exemple une messagerie employant SMPT/MIME, X400/X435, LOTUS NOTES/cc:MAIL, et, ou bien, MICROSOFT MAIL/EXCHANGE. Les serveurs 112, 114 sont de préférence des ordinateurs classiques, qui ont été classiquement programmés en C++, de manière à mettre en oeuvre le procédé présentement préféré de l'invention, et sont de préférence destinés à fonctionner sur l'une des plates-formes UNIX suivantes : AIX, HPUX, SUN OS, ou bien SOLARIS.

Sont énumérés ci-après, dans le tableau A, les divers scénarios qu'un programmeur ordinaire pourra facilement utiliser pour créer la programmation nécessaire, en langage C++, lequel est un langage de programmation orienté vers l'exécution, pour faire fonctionner les serveurs 112, 114 afin qu'ils mettent en oeuvre le procédé présentement préféré de l'invention. Comme on pourra le constater, les différents scénarios se rapportent respectivement aux questions suivantes : émettre un document EDI, réémettre un document EDI, recevoir un document EDI valable, recevoir un accusé de réception AUTACK, recevoir la nouvelle clé publique d'un partenaire de négociation, distribuer sa propre nouvelle clé publique à des partenaires de négociation reliés, activer le menu principal de gestion de certificats, créer sa propre paire de clés clé privée/clé publique, modifier un certificat (sa propre paire de clés publique/privée), retirer sa propre paire de clés privée/publique, copier sa propre clé publique dans un fichier du disque, imprimer

son propre certificat de clé publique, sauvegarder sa propre clé privée/publique sur un fichier du disque, restaurer sa propre clé privée/publique à partir du fichier du disque pour remplacer la clé privée/publique existante, restaurer sa propre clé privée/publique à partir du fichier du disque pour avoir une nouvelle clé, activer le menu principal de gestion de clés publiques de partenaires de négociation, ajouter une clé publique de partenaire de négociation, modifier la clé publique d'un partenaire de négociation, retirer la clé publique d'un partenaire de négociation, copier la clé publique d'un partenaire de négociation à partir d'un fichier du disque pour remplacer la clé publique existante d'un partenaire de négociation, copier la clé publique d'un partenaire de négociation à partir d'un fichier du disque pour avoir une nouvelle clé, activer le menu principal de gestion d'accords de partenaires de négociation, ajouter un accord de partenaires de négociation, modifier l'accord de partenaires de négociation, retirer l'accord de partenaires de négociation, copier l'accord de partenaires de négociation sur un fichier du disque, copier l'accord de partenaires de négociation à partir d'un fichier du disque, "ficeler" (assembler en paquets) selon MIME (le système de messagerie MIME classique), "déficeler" (désassembler les paquets) selon MIME, ficeler selon PKCS (PKCS classique), déficeler selon PKCS, travailler avec l'enregistrement des suivis, surveiller les travaux des serveurs, recevoir un document EDI non valable ayant un problème d'intégrité, recevoir un AUTACK ayant un problème d'intégrité, recevoir un message non admis, recevoir un échange EDI sans AUTACK tout en attendant une non-répudiation d'origine, et recevoir un AUTACK non attendu.

Envoyer un document EDI

Tableau A Scénarios

Initiateur	Action	Participant
traducteur EDI	demander d'envoyer un train EDI	agent d'authentification
agent d'authentification	obtenir l'ID de l'émetteur et du récepteur	enveloppe d'échange EDI
agent d'authentification	créer un enregistrement de suivis	enregistrement de suivis
agent d'authentification	créer une liste de contrôle de commencement d'événement	liste de contrôle
agent d'authentification	demander le procédé de calcul de condensé et l'adresse de destination du partenaire de négociation, l'adresse source, le procédé de non-répudiation de réception (NNR), de non-répudiation d'origine (NRO) de confidentialité et de transfert	accord de partenaires de négociation
agent d'authentification	obtenir un condensé d'identification	échange EDI
échange EDI	obtenir le procédé de condensé d'identification	configuration
échange EDI	calculer le condensé de l'échange EDI	calculateur de condensé
agent d'authentification	vérifier que le condensé d'identification et de numéro de commande est unique	liste de suivis
agent d'authentification	créer l'AUTACK	AUTACK
AUTACK	obtenir l'identification (ID) de clé privée, la NRR, la NRO, le contrôle d'intégrité, le procédé de condensé	accord de partenaires de négociation
AUTACK	obtenir la clé privée	répertoire de clés
AUTACK	obtenir le condensé d'intégrité	échange EDI
AUTACK	calculer son propre condensé	calculateur de condensé
AUTACK	signer le condensé de l'AUTACK	BSAFE
agent d'authentification	créer une enveloppe d'AUTACK	enveloppe de UNB
agent d'authentification	crypter l'échange EDI	PKCS
agent d'authentification	combiner l'échange EDI et l'AUTACK en un corps de message codé MIME (partiels MIME multiples)	ficeleur MIME
agent d'authentification	envoyer l'échange codé au partenaire de négociation	fonction sendmail
agent d'authentification	mettre à jour l'enregistrement de suivis avec la date et l'heure de l'envoi, l'emplacement du corps de message, l'ID de l'émetteur et du récepteur, la NRO et le condensé d'intégrité, l'ID de la clé privée, l'ID de la clé publique, le condensé d'identification	enregistrement de suivis
agent d'authentification	créer une liste de contrôle de messages envoyés	liste de contrôle
agent d'authentification	renvoyer un code de retour réussi et l'ID de l'enregistrement de suivis au traducteur EDI	agent d'authentification

2737067

Ré-envoyer un document EDI

Initiateur	Action	Participant
surveillant de ré-émission	demander l'état d'accusé de réception	enregistrement de suivis
surveillant de ré-émission	demander l'action de ré-émission	accord de partenaires de négociation
surveillant de ré-émission	demander de ré-envoyer l'échange EDI	agent d'authentification
agent d'authentification	demander l'emplacement du corps de message	enregistrement de suivis
agent d'authentification	envoyer l'échange codé au partenaire de négociation	fonction sandmail
agent d'authentification	mettre à jour l'enregistrement de suivis à l'aide de la date et de l'heure du ré-envoi	enregistrement de suivis
agent d'authentification	créer une liste de contrôle de messages ré-envoyés	liste de contrôle

Recevoir un document EDI valable

Initiateur	Action	Participant
ficeleur MIME	informer de l'arrivée de messages	ficeleur MIME
agent d'authentification	créer une rubrique de liste de messages bien reçus	liste de contrôle
agent d'authentification	valider le message reçu contenu dans un échange EDI	échange EDI
agent d'authentification	créer un enregistrement de suivis	enregistrement de suivis
agent d'authentification	obtenir l'ID de l'émetteur et du récepteur	enveloppe de l'échange EDI
agent d'authentification	obtenir un accord de partenaires de négociation avec l'ID de l'émetteur et du récepteur	accord de partenaires de négociation
agent d'authentification	obtenir le condensé de l'échange et le condensé signé, ainsi que le procédé de calcul de condensé	AUTACK
AUTACK	obtenir l'ID de la clé publique	accord de partenaires de négociation
AUTACK	obtenir la clé publique du partenaire de négociation	répertoire de clés
répertoire de clés	lire la dernière clé publique effective	répertoire de clés
AUTACK	décrypter le condensé signé	BSAFE
agent d'authentification	calculer le condensé de l'échange EDI	échange EDI
agent d'authentification	comparer le condensé calculé de l'échange EDI avec le condensé contenu dans l'AUTACK, vérifier que le condensé de l'AUTACK partiel est le même que le condensé signé décrypté contenu dans l'AUTACK	AUTACK
agent d'authentification	obtenir le condensé de l'identification	échange EDI
échange EDI	obtenir le procédé de condensé d'identification	configuration
échange EDI	calculer le condensé de l'échange EDI	calculateur de condensé
agent d'authentification	vérifier que le condensé de l'identification et du numéro de commande est unique	liste de suivis
agent d'authentification	créer une rubrique de liste d'échanges EDI bien reçus	liste de contrôle
agent d'authentification	obtenir la non-répudiation de la réception	accord de partenaires de négociation
agent d'authentification	créer un accusé de réception AUTACK, un numéro de commande	AUTACK
AUTACK	obtenir l'ID de la clé privée	accord de partenaires de négociation

Recevoir un document EDI valable (suite)

Initiateur	Action	Participant
AUTACK	obtenir la clé privée	répertoire de clés
AUTACK	signer le condensé	BSAFE
agent d'authentification	créer une rubrique de liste de demande d'envoi AUTACK	liste de commande
agent d'authentification	créer un corps de message codé MIME AUTACK	ficeleur MIME
agent d'authentification	envoyer l'AUTACK codé au partenaire de négociation	fonction sandmail
agent d'authentification	mettre à jour l'enregistrement de suivis avec la date et l'heure d'envoi d'AUTACK, l'emplacement du corps de message, l'ID de l'émetteur et du récepteur, le condensé	enregistrement de suivis
agent d'authentification	créer une rubrique de liste d'AUTACK envoyé	liste de contrôle
agent d'authentification	obtenir l'action de post-traitement d'acheminement vers l'intérieur	accord de partenaires de négociation
agent d'authentification	écrire les données EDI dans un fichier ou répertoire spécifié	agent d'authentification
agent d'authentification	exécuter l'instruction de post-traitement (p. ex. faire intervenir le traducteur EDI)	agent d'authentification

Recevoir un accusé de réception AUTACK

Initiateur	Action	Participant
ficeleur MIME	informer de l'arrivée de messages	ficeleur MIME
agent d'authenti–fication	obtenir des listes de parties de corps MIME	ficeleur MIME
agent d'authenti–fication	valider le message reçu contenu dans un AUTACK	échange AUTACK
agent d'authenti–fication	obtenir l'ID de l'émetteur et du récepteur	enveloppe d'échange AUTACK
agent d'authenti–fication	obtenir le drapeau NRR, l'ID de la clé publique	accord de partenaires de négociation
agent d'authenti–fication	vérifier la signature de l'émetteur	BSAFE
agent d'authenti–fication	obtenir le condensé de l'intégrité et du numéro de commande de l'échange	AUTACK
agent d'authenti–fication	mettre la jour la date et l'heure de l'accusé de réception reçu de l'échange envoyé	enregistrement de suivis

2737067

Recevoir une nouvelle clé publique de partenaire de négociation

Initiateur	Action	Participant
ficeleur MIME	informer de l'arrivée de messages	ficeleur MIME
agent d'authenti–fication	obtenir la liste des parties de corps MIME	ficeleur MIME
agent d'authenti–fication	valider le message reçu contenu dans un certificat	certificat
agent d'authenti–fication	obtenir le nom distinctif, le qualificateur et l'ID du partenaire de négociation	certificat
agent d'authenti–fication	obtenir l'adresse de messagerie électronique pour la clé publique de l'équipe de gestion de certificat	répertoire de clés
agent d'authenti–fication	vérifier la signature	BSAFE
agent d'authenti–fication	enregistrer l'arrivée des certificats	liste de contrôle
agent d'authenti–fication	créer un enregistrement de suivis avec certificat de type	enregistrement de suivis
agent d'authenti–fication	informer l'utilisateur de l'arrivée du certificat	agent d'authentification
utilisateur	vérifier avec le partenaire de négociation que le certificat est correct	utilisateur
utilisateur	sélectionner pour mettre à jour le certificat dans l'enregistrement de suivis	utilisateur
UI	obtenir le certificat	enregistrement de suivis
UI	ajouter au certificat un nouveau numéro de série	répertoire de clés
UI	modifier la date expirée du précédent certificat	répertoire de clés
UI	enregistrer la mise à jour du certificat	liste de contrôle
UI	modifier l'état de l'enregistrement de suivis pour tenir compte de la mise à jour	enregistrement de suivis

Distribuer sa propre nouvelle clé publique à des partenaires de négociation reliés

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton de gestion de certificat	utilisateur
UI	obtenir une liste de paires de clés – ID de clés	répertoire de clés
UI	afficher la liste des paires de clés sur l'écran	UI
utilisateur	sélectionner le certificat à distribuer	utilisateur
utilisateur	faire intervenir la fonction de distribution	utilisateur
UI	obtenir une liste de partenaires de négociation utilisant ce certificat	accord de partenaires de négociation
UI	obtenir l'adresse de messagerie électronique du partenaire de négociation	partenaire de négociation
UI	afficher la liste des partenaires de négociation et des adresses de messagerie électronique	UI
utilisateur	sélectionner ou désélectionner le partenaire de négociation	utilisateur
utilisateur	modifier l'adresse de messagerie électronique	utilisateur
utilisateur	ajouter une nouvelle adresse de messagerie électronique	utilisateur
utilisateur	faire intervenir le processus de distribution	utilisateur
UI	créer le certificat (X.509 ou PKCS?)	répertoire de clés
UI	coder le certificat en format MIME	ficeleur MIME
UI	envoyer le certificat codé MIME	fonction sandmail
UI	créer une rubrique d'enregistrement de clé envoyée	liste de contrôle

2737067

Activer le menu principal de gestion de certificats

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton de gestion de certificats	utilisateur
UI	obtenir une liste de paires de clés – ID de clés	répertoire de clés
UI	afficher la liste des paires de clés sur l'écran	UI

Créer sa propre paire de clés, clé privée/clé publique

L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton de création de paires de clés	utilisateur
UI	afficher un écran afin d'accepter l'ID de clé, la date effective, le nom distinctif et l'adresse de messagerie électronique	UI
utilisateur	introduire l'ID de clé, la date effective, le nom et l'adresse de messagerie électronique	utilisateur
UI	créer la paire de clés	répertoire de clés
répertoire de clés	obtenir la longueur de la clé	configuration
répertoire de clés	obtenir la valeur de départ de production de la clé	générateur de valeur de départ
répertoire de clés	produire la paire de clés privée et publique	BSAFE
répertoire de clés	s'assurer que la clé publique n'existe pas	base de données de répertoire de clés
répertoire de clés	obtenir la clé de chiffrage interne	configuration
répertoire de clés	chiffrer la clé privée	BSAFE
répertoire de clés	affecter 1 au numéro de série	répertoire de clés
répertoire de clés	écrire la paire de clés	base de données
répertoire de clés	renvoyer la paire de clés	répertoire de clés
UI	mettre à jour la liste des clés	UI

2737067

Modifier le certificat (sa propre paire de clés privée/publique)
L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	sélectionner une paire de clés à modifier	utilisateur
utilisateur	faire intervenir le bouton de modification du certificat	utilisateur
UI	afficher un écran afin de modifier la date effective, le nom et l'adresse de messagerie électronique	utilisateur
utilisateur	modifier les champs	utilisateur
utilisateur	faire intervenir le bouton de création de nouvelles clés	utilisateur
UI	re-produire la paire de clés	répertoire de clés
répertoire de clés	affecter un nouveau numéro de série	répertoire de clés
répertoire de clés	obtenir la valeur de départ de production de la clé	générateur de valeur de départ
répertoire de clés	obtenir la longueur de la clé	configuration
répertoire de clés	produire la paire de clés privée et publique	BSAFE
répertoire de clés	s'assurer que la clé publique n'existe pas	base de données de répertoire de clés
répertoire de clés	obtenir la clé de chiffrage interne	configuration
répertoire de clés	crypte la clé privée	BSAFE
répertoire de clés	écrire la nouvelle paire de clés	base de données de répertoire de clés
répertoire de clés	renvoyer la paire de clés	répertoire de clés
UI	mettre à jour la liste des clés	UI

2737067

Retirer sa propre paire de clés privée/publique

L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	sélectionner une paire de clés à retirer	utilisateur
utilisateur	faire intervenir le bouton de retrait de la paire de clés	utilisateur
UI	vérifier si la paire de clés est utilisée dans l'un quelconque des accords de partenaires de négociation	accord de partenaires de négociation
UI	afficher le message de confirmation	UI
utilisateur	confirmer le retrait de la paire de clés	utilisateur
UI	retirer la paire de clés	répertoire de clés
répertoire de clés	désactiver la paire de clés	base de données de répertoire de clés
UI	repérer la paire de clés comme étant désactivée sur l'écran	UI

Copier sa propre clé publique sur un fichier du disque

L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	sélectionner une clé	utilisateur
utilisateur	faire intervenir la fonction de copie sur disque	utilisateur
UI	afficher un écran afin de demander le nom du fichier de sortie	UI
utilisateur	introduire le nom du fichier	utilisateur
UI	afficher un écran de confirmation de remplacement	UI
utilisateur	sélectionner afin d'écraser le fichier existant	utilisateur
UI	délivrer le certificat en format X.509 au fichier du disque	répertoire de clés
UI	afficher un message d'achèvement	UI
UI	réafficher la liste	UI

2737067

Imprimer son propre certificat de clé publique

L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	sélectionner une clé	utilisateur
utilisateur	faire intervenir la fonction imprimer le certificat	utilisateur
UI	obtenir le certificat sous un format lisible par les êtres humains	répertoire de clés
répertoire de clés	formater le nom distinctif, la clé publique, la date effective, la référence (ID de clé), le numéro de série, l'algorithme de signature, la signature du certificat, la version, l'émetteur et l'adresse de messagerie électronique	répertoire de clés
UI	délivrer le certificat à l'imprimante par défaut du système	UI
UI	réafficher la liste	UI

Sauvegarder sa propre clé privée/publique sur un fichier de disque

L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	sélectionner une clé	utilisateur
utilisateur	faire intervenir la fonction de sauvegarde sur disque	utilisateur
UI	afficher un écran afin de demander le nom du fichier de sortie	UI
utilisateur	introduire le nom du fichier	utilisateur
UI	afficher un écran de confirmation de remplacement	UI
utilisateur	sélectionner afin d'écraser le fichier existant	utilisateur
UI	délivrer la paire de clés, le nom distinctif, la clé privée, publique, la date effective, la référence (ID de clé), le numéro de série, l'algorithme du condensé, le condensé, la version, l'émetteur et l'adresse de messagerie électronique au fichier	répertoire de clés
UI	afficher un message d'achèvement	UI
UI	réafficher la liste	UI

2737067

Restaurer sa propre clé privée/publique à partir du fichier de disque pour remplacer la clé existante
L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	sélectionner une clé	utilisateur
utilisateur	faire intervenir la fonction restauration à partir du disque	utilisateur
UI	afficher un écran pour demander le nom du fichier d'entrée	UI
utilisateur	introduire le nom du fichier	utilisateur
UI	afficher une confirmation de remplacement et sauvegarder l'écran de la paire de clés	UI
utilisateur	sélectionner afin d'écraser la clé existante et introduire le nom du fichier de sauvegarde	utilisateur
UI	créer une rubrique d'enregistrement	liste de contrôle
UI	délivrer la paire de clés existantes, le nom distinctif, la clé privée, publique, la date effective, la référence (ID de clé), le numéro de série, l'algorithme du condensé, le condensé, la version, l'émetteur et l'adresse de messagerie électronique au fichier de sauvegarde	répertoire de clés
UI	remplacer la paire de clés	répertoire de clés
répertoire de clés	lire l'information relative à la clé dans le fichier	répertoire de clés
répertoire de clés	mettre à jour l'information relative à clé	base de données
UI	afficher un message d'achèvement	UI
UI	réafficher la liste	UI

Restaurer sa propre clé privée/publique à partir d'un fichier de disque pour avoir une nouvelle clé
L'utilisateur a besoin de faire entrer et d'activer le menu principal de gestion de certificats avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	faire intervenir la fonction restauration à partir du disque	utilisateur
UI	afficher un écran pour demander l'ID de clé et le nom du fichier d'entrée	UI
utilisateur	introduire l'ID de clé et le nom du fichier	utilisateur
répertoire de clés	lire l'information relative à la clé dans le fichier	répertoire de clé
répertoire de clés	calculer le condensé du certificat	calculateur de condensé
répertoire de clés	vérifier le bon accord du condensé	répertoire de clés
répertoire de clés	écrire l'information relative à la clé	base de données
UI	ajouter la paire de clés à la liste	UI
UI	réafficher la liste	UI

Activer le menu principal de gestion de clés publiques de partenaires de négociation

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton des clés des partenaires de négociation	utilisateur
UI	obtenir une liste de clés publiques de partenaires de négociation	répertoire de clés
UI	afficher la liste des clés publiques des partenaires de négociation sur l'écran	UI

Ajouter une clé publique d'un partenaire de négociation

L'utilisateur doit introduire et activer le menu principal de gestion des certificats publics des partenaires de négociation avant d'obtenir cette fonction.

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton d'addition de la clé publique d'un partenaire de négociation	utilisateur
UI	afficher l'écran d'addition de clé publique de partenaire de négociation	UI
utilisateur	sélectionner pour ajouter la clé à partir d'un fichier de disque	utilisateur
UI	afficher un écran afin d'introduire le nom de fichier	UI
utilisateur	introduire le nom de fichier	utilisateur
UI	lire l'adresse de messagerie électronique, la date effective, la clé publique, le numéro de téléphone, l'adresse postale	fichier de clés publiques
UI	afficher la clé publique	UI
utilisateur	introduire le nom de société du partenaire de négociation	utilisateur
UI	afficher la nouvelle clé publique de la liste sur l'écran	UI

Modifier la clé publique d'un partenaire de négociation

L'utilisateur doit introduire et activer le menu principal de gestion des certificats publics des partenaires de négociation avant d'obtenir cette fonction.

Initiateur	Action	Participant
utilisateur	sélectionnner une clé publique à modifier	utilisateur
utilisateur	faire intervenir le bouton de changement de clé publique	utilisateur
UI	obtenir l'information relative à la clé publique	répertoire de clés
UI	afficher la clé publique du partenaire de négociation sur l'écran	UI
utilisateur	modifier la date effective et la clé publique	utilisateur
UI	mettre à jour la clé publique	répertoire de clés
UI	ajouter à la nouvelle clé publique le nouveau numéro de série	répertoire de clés
UI	afficher la nouvelle clé publique de la liste sur l'écran	UI

Retirer la touche publique d'un partenaire de négociation

L'utilisateur doit introduire et activer le menu principal de gestion de certificats publics des partenaires de négociation avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	sélectionnner une clé publique à retirer	utilisateur
utilisateur	faire intervenir le bouton de retrait de clé publique	utilisateur
UI	obtenir l'information relative à la clé publique	répertoire de clés
UI	afficher l'écran d'addition de clé publique de partenaire de négociation	UI
UI	afficher l'écran de confirmation	UI
utilisateur	confirmer le retrait	utilisateur
UI	désactiver la clé publique	répertoire de clés
UI	retirer la clé publique de la liste sur l'écran	UI

Copier la clé publique d'un partenaire de négociation à partir d'un fichier de disque pour remplacer la clé existante

L'utilisateur doit introduire et activer le menu principal de gestion de certificats avant d'obtenir cette fonction. On suppose que le fichier est en format X.509.

Initiateur	Action	Participant
utilisateur	sélectionner une clé publique	utilisateur
utilisateur	faire intervenir la fonction de restauration à partir du disque	utilisateur
UI	afficher un écran pour demander le nom du fichier d'entrée	UI
utilisateur	introduire le nom du fichier	utilisateur
UI	afficher une confirmation de remplacement et sauvegarder l'écran de la paire de clés	UI
utilisateur	sélectionner pour écraser la clé existante et introduire le nom du fichier de sauvegarde	utilisateur
UI	créer une rubrique d'enregistrement	liste de contrôle
UI	délivrer la clé existante, le nom distinctif, la clé publique, la date effective, la référence (l'ID de clé), le numéro de série, l'algorithme du condensé, le condensé, la version, l'émetteur et l'adresse de messagerie électronique au fichier de sauvegarde	répertoire de clés
UI	remplacer la clé	répertoire de clés
répertoire de clés	lire l'information relative à la clé sur le fichier	répertoire de clés
répertoire de clés	mettre à jour l'information relative à la clé	base de données
UI	afficher un message d'achèvement	UI
UI	réafficher la liste	UI

Copie de la clé publique d'un partenaire de négociation sur le fichier de disque pour obtenir une nouvelle clé

L'utilisateur doit introduire et activer le menu principal de gestion de certificats avant d'obtenir cette fonction. On suppose que le fichier est en format X.509.

Initiateur	Action	Participant
utilisateur	faire intervenir la fonction de restauration à partir du disque	utilisateur
UI	afficher un écran pour demander l'ID de clé et le nom du fichier d'entrée	UI
utilisateur	introduire l'ID de clé et le nom du fichier	utilisateur
répertoire de clés	lire l'information relative à la clé dans le fichier	répertoire de clés
répertoire de clés	calculer le condensé de certificat	calculateur de condensé
répertoire de clés	vérifier le bon accord du condensé	répertoire de clés
répertoire de clés	écrire l'information relative à la clé	base de données
UI	ajouter la clé à la liste	UI
UI	réafficher la liste	UI

Activer le menu principal de gestion des accords de partenaires de négociation

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton d'accord de partenaires de négociation	utilisateur
UI	obtenir une liste d'accords de partenaires de négociation	liste des accords de partenaires de négociation
UI	afficher la liste des accords de partenaires de négociation sur l'écran	UI

2737067

Ajouter un accord de partenaires de négociation

L'utilisateur doit introduire et activer le menu principal de gestion des partenaires de négociation avant d'obtenir cette fonction

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton d'addition d'accord de partenaires de négociation	utilisateur
UI	afficher un écran d'accord de partenaires de négociation afin d'accepter un ID de partenaire de négociation local et de certificat ; un ID de partenaire de négociation éloigné et de certificat	UI
utilisateur	faire intervenir l'addition d'un nouveau partenaire de négociation local	utilisateur
UI	afficher un écran d'addition de partenaire de négociation	UI
utilisateur	introduire le nom, le contact, l'adresse de messagerie électronique du contact, le téléphone, le fax, l'adresse, le nom complet, un commentaire	utilisateur
UI	vérifier que le partenaire de négociation n'existe pas	liste des partenaires de négociation
UI	ajouter le partenaire de négociation	liste des partenaires de négociation
UI	afficher le partenaire de négociation local sur l'écran	UI
utilisateur	introduire le type d'enveloppe, les séparateurs, le qualificateur et l'ID	utilisateur
utilisateur	faire intervenir l'addition d'un nouveau partenaire de négociation éloigné	utilisateur
UI	afficher un écran d'addition de partenaire de négociation	UI
utilisateur	introduire le nom, le contact, l'adresse de messagerie électronique du contact, le téléphone, le fax, l'adresse, le nom complet, un commentaire	utilisateur
UI	vérifier que le partenaire de négociation n'existe pas	liste des partenaires de négociation
UI	ajouter le partenaire de négociation	liste des partenaires de négociation
UI	afficher le partenaire de négociation éloigné sur l'écran	UI
utilisateur	faire intervenir le bouton d'acheminement vers l'intérieur	utilisateur
UI	afficher l'écran d'informations d'acheminement vers l'intérieur	UI
utilisateur	introduire des informations d'acheminement vers l'intérieur : état ; sécurité, NRO, NRR et confidentiel ; fichier de réception de données EDI, instruction d'exécution après réception	utilisateur
UI	vérifier les informations d'acheminement vers l'intérieur	acheminement vers l'intérieur
UI	ajouter l'acheminement vers l'intérieur	acheminement vers l'intérieur

Ajouter un accord de partenaires de négociation (suite)

Initiateur	Action	Participant
utilisateur	faire intervenir le bouton d'acheminement vers l'extérieur	utilisateur
UI	afficher l'écran d'informations d'acheminement vers l'extérieur	UI
utilisateur	introduire des informations de transport, récepteur MIME et adresse de messagerie électronique de l'émetteur, dimension maximale du message, jeu de caractères	utilisateur
utilisateur	introduire sécurité, NRO, NRR, confidentiel	utilisateur
utilisateur	introduire intervalle de ré-émission et action	utilisateur
UI	vérifier les informations d'acheminement vers l'extérieur	acheminement vers l'extérieur
UI	ajouter l'acheminement vers l'extérieur	acheminement vers l'extérieur
UI	réafficher l'écran principal d'accord de partenaires de négociation	UI
utilisateur	sélectionner pour sauvegarder l'accord des partenaires de négociation	utilisateur
UI	ajouter l'accord des partenaires de négociation	liste des accords des partenaires de négociation

Modifier un accord de partenaires de négociation

L'utilisateur doit introduire et activer le menu principal de gestion de partenaires de négociation avant d'obtenir cette fonction.

Initiateur	Action	Participant
utilisateur	sélectionner l'accord de partenaires de négociation à modifier	utilisateur
utilisateur	faire intervenir le bouton de modification d'accord de partenaires de négociation	utilisateur
UI	obtenir l'accord de partenaires de négociation sélectionné	liste d'accords de partenaires de négociation
UI	obtenir des informations, partenaires de négociation local et éloigné, informations vers l'intérieur et vers l'extérieur	accord de partenaires de négociation
UI	afficher les informations relative à l'accord de partenaires de négociation sur l'écran et ne pas permettre de modifier les partenaires de négociation local et éloigné	UI
utilisateur	demander de modifier l'information relative au partenaire de négociation local	utilisateur
UI	obtenir des informations sur le partenaire de négociation local	partenaire de négociation
UI	afficher les informations relatives au partenaire de négociation sur l'écran	UI
utilisateur	modifier l'adresse de messagerie électronique du partenaire de négociation	utilisateur
UI	mettre à jour le partenaire de négociation	partenaire de négociation
UI	afficher l'écran d'accord de partenaires de négociation	UI
utilisateur	sélectionner pour modifier le partenaire de négociation éloigné	UI
UI	obtenir des informations sur le partenaire de négociation éloigné	partenaire de négociation
UI	afficher sur l'écran l'information relative au partenaire de négociation	UI
UI	afficher l'écran d'accord de partenaires de négociation	UI
utilisateur	modifier l'adresse du partenaire de négociation	utilisateur
UI	mettre à jour le partenaire de négociation	partenaire de négociation
UI	afficher l'écran d'accord de partenaires de négociation	UI
utilisateur	modifier les informations d'acheminement vers l'intérieur et vers l'extérieur	utilisateur
utilisateur	sélectionner pour mettre à jour l'accord de partenaires de négociation	utilisateur
UI	mettre à jour l'accord de partenaires de négociation	liste des partenaires de négocation

Retirer un accord de partenaires de négociation

L'utilisateur doit introduire et activer le menu principal de gestion des partenaires de négociation pour obtenir cette fonction.

Initiateur	Action	Participant
utilisateur	sélectionner l'accord de partenaires de négociation à retirer	utilisateur
utilisateur	faire intervenir le bouton de retrait d'accord de partenaires de négociation	utilisateur
UI	obtenir l'accord de partenaires de négociation sélectionné	liste d'accords de partenaires de négociation
UI	obtenir des informations, partenaires de négociation local et éloigné	accord de partenaires de négociation
UI	afficher sur l'écran des informations relatives à l'accord des partenaires de négociation	UI
UI	afficher l'écran de confirmation	UI
utilisateur	confirmer le retrait	utilisateur
UI	retirer l'accord de partenaires de négociation	liste d'accords de partenaires de négociation
UI	retirer l'accord de la liste sur l'écran	UI
UI	réafficher la nouvelle liste sur l'écran	UI

Copie d'un accord de partenaires de négociation sur un fichier de disque

L'utilisateur doit introduire et activer le menu principal d'accord de partenaires de négociation avant d'obtenir cette fonction.

Initiateur	Action	Participant
utilisateur	sélectionner l'accord de partenaires de négociation	utilisateur
utilisateur	faire intervenir la fonction de copie sur disque	utilisateur
UI	afficher un écran pour demander le nom du fichier de sortie	UI
utilisateur	introduire le nom du fichier	utilisateur
UI	afficher un écran de confirmation de remplacement	UI
utilisateur	sélectionner pour écraser le fichier existant	utilisateur
UI	délivrer l'accord de partenaires de négociation au fichier sous la forme d'une table à deux dimensions	accord de partenaires de négociation
UI	afficher un message d'achèvement	UI
UI	réafficher la liste	UI

Copie d'un accord de partenaires de négociation à partir d'un fichier de disque

L'utilisateur doit introduire et activer le menu principal d'accord de partenaires de négociation avant d'obtenir cette fonction.

Initiateur	Action	Participant
utilisateur	faire intervenir la fonction de copie à partir du disque	utilisateur
UI	afficher un écran pour demander le nom du fichier d'entrée	UI
utilisateur	introduire le nom du fichier	utilisateur
UI	afficher un écran de confirmation de remplacement	UI
utilisateur	sélectionner pour écraser l'accord de partenaires de négociation existant	utilisateur
UI	remplacer l'accord de partenaires de négociation	accord de partenaires de négociation
accord de partenaires de négociation	lire dans le fichier des informations relatives à l'accord de partenaires de négociation	accord de partenaires de négociation
accord de partenaires de négociation	mettre à jour les informations relatives à l'accord de partenaires de négociation	base de données
UI	afficher un message d'achèvement	UI
UI	réafficher la liste	UI

Ficeler (assembler en paquets) selon MIME

Initiateur	Action	Participant
agent d'authen-tification	créer un objet MIME avec un échange EDI, un AUTACK, un accord de partenaires de négociation	ficeleur MIME
ficeleur MIME	obtenir qualificateur et ID de l'émetteur et du récepteur	échange EDI
ficeleur MIME	obtenir l'adresse de messagerie électronique d'origine et de destination, la taille partielle MIME maximale	accord de partenaires de négociation
ficeleur MIME	obtenir le procédé de cryptage de sécurité des partenaires de négociation (par exemple DES ou RC4), l'ID de la clé publique du partenaire de négociation, le drapeau de confidentialité	accord de partenaires de négociation
ficeleur MIME	envelopper l'échange EDI dans une enveloppe PKCS	enveloppeur PKCS
ficeleur MIME	créer une partie de corps EDI pour l'échange EDI traité par PKCS	partie de corps MIME
ficeleur MIME	créer une partie de corps AUTACK	partie de corps MIME
ficeleur MIME	créer un en-tête MIME à partir de l'adresse de messagerie électronique et à destination de celle-ci	en-tête MIME
ficeleur MIME	créer des partiels MIME à partir de l'en-tête MIME et des parties de corps MIME	message MIME
ficeleur MIME	renvoyer le message MIME à l'agent d'authentification	ficeleur MIME

Déficeler (désassembler les paquets) selon MIME

Initiateur	Action	Participant
fonction sendmail	créer un cas de partiel MIME	ficeleur MIME
ficeleur MIME	enregistrer l'arrivée d'un partiel	liste de contrôle
ficeleur MIME	assembler des partiels	ficeleur MIME
ficeleur MIME	enregistrer tous les partiels reçus	liste de contrôle
ficeleur MIME	déballer les parties de corps traitées par PKCS	désenveloppeur PKCS
ficeleur MIME	informer l'agent d'identification de l'arrivée d'un message	ficeleur MIME
agent d'authentification	obtenir l'adresse de messagerie électronique d'origine et de destination	ficeleur MIME
ficeleur MIME	obtenir sécurité TP (partenaire de négociation)	accord de partenaires de négociation
agent d'authentification	obtenir la liste des parties de corps	message MIME
agent d'authentification	obtenir la partie de corps AUTACK	message MIME
agent d'authentification	obtenir l'échange EDI	message MIME
agent d'authentification	poursuivre avec les autres traitements	agent d'authentification

Ficeler (assembler en paquets) selon PKCS

Initiateur	Action	Participant
ficeleur MIME	créer un échange EDI traité par PKCS	ficeleur PKCS
ficeleur PKCS	obtenir le qualificateur et l'ID de l'émetteur et du récepteur	échangeur EDI
ficeleur PKCS	obtenir le procédé de cryptage et l'ID de la clé publique du partenaire de négociation (par exemple DES ou RC4)	accord de partenaires de négociation
ficeleur PKCS	obtenir la clé publique du partenaire de négociation	répertoire de clés
ficeleur PKCS	obtenir une clé DES aléatoire	crypteur DES
ficeleur PKCS	crypter l'échange EDI	crypteur DES
ficeleur PKCS	crypter la clé DES	BSAFE
ficeleur PKCS	créer la partie de corps MIME traitée par PKCS à l'aide de la clé DES cryptée et de l'échange EDI	partie de corps MIME
ficeleur PKCS	renvoyer l'échange EDI traité par PKCS	ficeleur PKCS

Déficeler (désassembler les paquets) selon PKCS

Initiateur	Action	Participant
ficeleur MIME	déballer une partie de corps traitée par PKCS	ficeleur PKCS
ficeleur PKCS	obtenir l'ID de la clé publique du partenaire de négocation	accord de partenaires de négociation
ficeleur PKCS	obtenir la clé publique du partenaire de négociation	répertoire de clés
ficeleur PKCS	faire accorder le certificat présent dans l'enveloppe avec le certificat présent dans le répertoire de clés	clé publique du partenaire de négociation
ficeleur PKCS	obtenir l'échangeur EDI traité par PKCS	partie de corps traitée par PKCS
ficeleur PKCS	décrypter la clé DES	BSAFE
ficeleur PKCS	décrypter l'échange EDI crypté	crypteur DES
ficeleur PKCS	renvoyer l'échangeur EDI au ficeleur MIME	ficeleur PKCS

Travailler avec un enregistrement de suivis

Initiateur	Action	Participant
utilisateur	faire intervenir la fonction de travail avec l'enregistrement de suivis	utilisateur
UI	demander les critères de sélection, étendue des données, émetteur/ récepteur, ID d'enregistrement des suivis, état, type de données, numéro de commande d'échange (sensible au type de données et ne s'appliquant qu'aux données EDI)	UI
utilisateur	introduire des critères, par exemple l'étendue des données	utilisateur
UI	obtenir une liste d'enregistrement de suivis qui se trouvent à l'intérieur de l'étendue spécifiée des données	enregistrement de suivis
enregistrement de suivis	interroger la base de données	base de données
UI	afficher une liste d'enregistrement de suivis	UI
utilisateur	faire intervenir la visualisation de détail d'un train EDI	utilisateur
UI	obtenir le détail	enregistrement de suivis
UI	afficher le détail du train EDI	UI
utilisateur	faire intervenir la ré-émission d'un échange	utilisateur
UI	ré-émettre l'échange	agent d'authentification
UI	réafficher le détail	UI
utilisateur	fermer	utilisateur
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	sélectionner pour ré-émettre un train EDI	utilisateur
UI	ré-émettre le train	agent d'authentification
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	retraiter un train vers l'extérieur	utilisateur
UI	retraiter un train vers l'extérieur (à partir du début)	agent d'authentification
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	retraiter un train vers l'intérieur	utilisateur
UI	retraiter un train vers l'intérieur (à partir du début)	agent d'authentification
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	continuer à partir de la dernière action	utilisateur

Travailler avec un enregistrement de suivis (suite)

Initiateur	Action	Participant
UI	continuer la dernière action	agent d'authentification
agent d'authentification	obtenir l'état	enregistrement de suivis
agent d'authentification	continuer le traitement en fonction de l'état	agent d'authentification
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	répéter la dernière action d'un train vers l'intérieur réussi, c'est-à-dire retraduire	utilisateur
UI	répéter la dernière action	agent d'authentification
agent d'authentification	obtenir l'état	enregistrement de suivis
agent d'authentification	répéter la dernière action	agent d'authentification
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	sélectionner pour imprimer un groupe d'enregistrement de suivis	utilisateur
UI	obtenir des informations de résumé d'enregistrement de suivis	enregistrement de suivis
UI	formater le rapport	UI
UI	imprimer le rapport	Imprimante
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	laisser un train EDI de maintien	utilisateur
UI	modifier l'état de l'enregistrement de suivis à laisser	enregistrement de suivis
UI	traiter le train EDI	agent d'authentification
UI	réafficher la liste d'enregistrement de suivis	UI
utilisateur	sélectionner pour afficher le contenu d'un message reçu	utilisateur
UI	obtenir le contenu du message	enregistrement de suivis
enregistrement de suivis	obtenir le contenu du message	fichier de message
UI	afficher le message	UI
utilisateur	fermer	utilisateur
UI	réafficher la liste d'enregistrement de suivis	UI

Surveiller les travaux du serveur

Initiateur	Action	Participant
utilisateur	faire intervenir la fonction de travail avec surveillance des travaux du serveur	utilisateur
UI	obtenir des informations sur les travaux du serveur	système d'exploitation placé sur le serveur
UI	afficher le nom et l'état des travaux du serveur	UI
utilisateur	sélectionner pour rafraîchir l'état	utilisateur
UI	obtenir des informations sur les travaux du serveur	système d'exploitation placé sur le serveur
UI	afficher le nom et l'état des travaux du serveur	UI
utilisateur	sélectionner pour faire commencer un travail du serveur, par exemple "guardian"	utilisateur
UI	faire commencer le travail du serveur	configuration du travail
configuration du travail	faire commencer le travail	système d'exploitation placé sur le serveur
UI	obtenir des informations sur les travaux du serveur	système d'exploitation placé sur le serveur
UI	afficher le nom et l'état des travaux du serveur	UI

Recevoir un document EDI non valable ayant un problème d'intégrité

On suppose que le début du scénario est le même que celui appelé "recevoir un document EDI valable". Après avoir vérifié que le condensé de l'AUTACK partiel est le même que le condensé signé décrypté contenu dans l'AUTACK, l'agent d'authentification découvre que le condensé contenu dans l'AUTACK ne s'accorde pas avec le condensé de l'échange EDI

Initiateur	Action	Participant
agent d'authentification	créer un enregistrement d'erreur d'intégrité d'échange à l'aide des informations suivantes : condensé de l'AUTACK, condensé de l'échange EDI, numéro de commande de l'AUTACK, le numéro de commande de l'échange, nom du partenaire de négociation, ID d'enregistrement de suivis	liste de contrôle
agent d'authentification	mettre à jour l'état de l'enregistrement de suivis sur l'erreur d'intégrité d'échange	enregistrement de suivis
agent d'authentification	obtenir l'adresse de messagerie électronique locale	accord de partenaires de négociation
agent d'authentification	formater un message électronique d'erreur d'intégrité d'échange à l'aide des informations suivantes : timbre temporel, condensé de l'AUTACK, condensé de l'échange EDI, numéro de commande de l'AUTACK, numéro de commande de l'échange, nom du partenaire de négociation, ID d'enregistrement de suivis	agent d'authentification
agent d'authentification	envoyer le message électronique	fonction sendmail
agent d'authentification	obtenir la date et l'heure de la création de l'échange EDI	échange EDI
agent d'authentification	formater un AUTACK négatif, le condensé se trouvant dans l'AUTACK reçu	AUTACK
agent d'authentification	créer un échange AUTACK	échange AUTACK
agent d'authentification	coder l'AUTACK négatif dans le format MIME	ficeleur MIME
agent d'authentification	envoyer l'AUTACK négatif codé au partenaire de négociation	fonction sendmail
agent d'authentification	mettre à jour l'état de l'enregistrement de suivis sur l'erreur d'intégrité d'échange à l'aide de l'AUTACK négatif envoyé	enregistrement de suivis
agent d'authentification	enregistrer l'événement constitué par l'AUTACK négatif envoyé	liste de contrôle

Recevoir un AUTACK ayant un problème d'intégrité

On suppose que le début du scénario est le même que celui appelé "recevoir un document EDI valable". L'agent d'authentification découvre que le condensé de l'AUTACK partiel n'est pas le même que le condensé signé décrypté contenu dans l'AUTACK.

Initiateur	Action	Participant
agent d'authentification	créer un enregistrement d'erreur d'intégrité d'AUTACK à l'aide des informations suivantes : condensé signé de l'AUTACK partiel se trouvant dans l'AUTACK, condensé signé décrypté de l'AUTACK partiel contenu dans l'AUTACK, condensé calculé de l'AUTACK partiel, numéro de commande de l'AUTACK, nom du partenaire de négociation, clé publique du partenaire de négociation, ID d'enregis-trement de suivis	liste de contrôle
agent d'authentification	mettre à jour l'état de l'enregistrement de suivis sur l'erreur d'intégrité AUTACK	enregistrement de suivis
agent d'authentification	obtenir l'adresse de messagerie électronique locale	accord de partenaires de négociation
agent d'authentification	formater un message électronique d'erreur d'intégrité d'AUTACK à l'aide des informations suivantes : timbre temporel, condensé signé de l'AUTACK partiel contenu dans l'AUTACK, condensé signé décrypté de l'AUTACK partiel contenu dans l'AUTACK, condensé calculé de l'AUTACK partiel, numéro de commande de l'AUTACK, nom du partenaire de négociation, clé publique du partenaire de négociation, ID d'enregistrement de suivis	agent d'authentification
agent d'authentification	envoyer le message électronique	fonction sendmail

2737067

Recevoir un message non admis

On suppose que le début du scénario est le même que celui appelé "réception d'un document EDI valable". L'agent d'authentification découvre que le message n'est pas un document EDI, n'est pas un AUTACK et n'est pas un certificat

Initiateur	Action	Participant
agent d'authentification	transférer le message non admis dans un fichier	fichier de transfert
fichier de transfert	obtenir le répertoire du fichier de transfert	configuration
fichier de transfert	produire un nom de fichier de transfert unique	fichier de transfert
fichier de transfert	délivrer le message non admis au fichier de transfert	fichier de transfert
agent d'authentification	créer un enregistrement d'erreur de message non admis reçu à l'aide des informations suivantes : adresse de messagerie électronique de l'émetteur et du récepteur, sujet, ID du message électronique, nom du fichier de transfert	liste de contrôle
agent d'authentification	mettre à jour l'état de l'enregistrement de suivis sur le message non admis reçu, sauvegarder le nom du fichier de transfert	enregistrement de suivis
agent d'authentification	obtenir l'adresse de messagerie électronique locale	accord de partenaires de négociation
agent d'authentification	formater un message électronique d'erreur de message non admis reçu à l'aide des informations suivantes : adresse de messagerie électronique de l'émetteur et du récepteur, sujet, ID du message électronique, nom du fichier de transfert	agent d'authentification
agent d'authentification	envoyer le message électronique	fonction sendmail

2737067

Recevoir un échange EDI sans AUTACK tandis qu'on attend une non-répudiation d'origine

On suppose que le début du scénario est le même que celui intitulé "recevoir un document EDI valable". L'agent d'authentification découvre qu'il n'y a pas d'AUTACK dans le message

Initiateur	Action	Participant
agent d'authentification	transférer l'échange EDI à un fichier	fichier de transfert
fichier de transfert	obtenir le répertoire du fichier de transfert	configuration
fichier de transfert	produire un nom de fichier de transfert unique	fichier de transfert
fichier de transfert	délivrer l'échange EDI au fichier de transfert	fichier de transfert
agent d'authentification	créer un enregistrement d'erreur d'AUTACK non reçu à l'aide des informations suivantes : timbre temporel, numéro de commande d'échange, nom du partenaire de négociation, ID d'enregistrement de suivis, nom du fichier de transfert	liste de contrôle
agent d'authentification	mettre à jour l'état de l'enregistrement de suivis sur l'AUTACK non reçu, sauvegarder le nom du fichier de transfert	enregistrement de suivis
agent d'authentification	obtenir l'adresse électronique locale	accord de partenaires de négociation
agent d'authentification	formater un message électronique d'erreur d'AUTACK non reçu à l'aide des informations suivantes : timbre temporel, numéro de commande d'échange, nom du partenaire de négociation, ID d'enregistrement de suivis, nom du fichier de transfert	agent d'authentification
agent d'authentification	envoyer le message électronique	fonction sendmail

2737067

Recevoir un AUTACK non attendu

On suppose que le début du scénario est le même que celui intitulé "recevoir un document EDI valable". L'agent d'authentification découvre qu'il y a un AUTACK dans le message, mais que l'accord des partenaires de négociation ne spécifie aucune non-répudiation d'origine.

Initiateur	Action	Participant
agent d'authentification	transférer l'échange EDI à un fichier	fichier de transfert
fichier de transfert	obtenir le répertoire du fichier de transfert	configuration
fichier de transfert	produire un nom de fichier de transfert unique	fichier de transfert
fichier de transfert	délivrer l'EDI au fichier de transfert	fichier de transfert
agent d'authentification	transférer l'échange AUTACK à un fichier	fichier de transfert
fichier de transfert	obtenir le répertoire du fichier de transfert	configuration
fichier de transfert	produire un nom de fichier de transfert unique	fichier de transfert
fichier de transfert	délivrer l'AUTACK au fichier de transfert	fichier de transfert
agent d'authentification	créer un enregistrement d'erreur d'AUTACK non attendu à l'aide des informations suivantes : timbre temporel, numéro de commande d'échange, nom du partenaire de négociation, ID d'enregistrement de suivis, noms des fichiers de transfert	liste de contrôle
agent d'authentification	mettre à jour l'état de l'enregistrement de suivis sur l'AUTACK non attendu, sauvegarder les noms des fichiers de transfert	enregistrement de suivis
agent d'authentification	obtenir l'adresse de messagerie électronique locale	accord de partenaires de négociation
agent d'authentification	formater un message électronique d'erreur d'AUTACK non attendu à l'aide des informations suivantes : timbre temporel, numéro de commande d'échange, nom du partenaire d'échange, ID d'enregistrement de suivis, noms des fichiers de transfert	agent d'authentification
agent d'authentification	envoyer le message électronique	fonction sendmail

Les figures 14 à 41 illustrent les divers affichages d'écran, dans un environnement du type WINDOWS classique, qui peuvent de préférence être réalisés sur les écrans d'ordinateur typiques 116 et 118 associés aux serveurs 112 et 114 pour la mise en oeuvre du procédé ci-dessus exposé, sous commande du programme qui a été basé sur les scénarios du tableau A. La figure 14 montre l'écran général qui est présenté aux parties, présentes sur le réseau, qui ont droit de prendre part, d'égal à égal, d'ordinateur à ordinateur, à des transactions EDI d'affaires via le réseau INTERNET. Comme représenté à titre d'exemple sur la figure 14, l'utilisateur peut se voir offrir, par exemple, de choisir entre des fenêtres se rapportant respectivement à PROFILS DE PARTENAIRES DE NEGOCIATION, ACCORDS DE PARTENAIRES DE NEGOCIATION, GESTION DE CLES, et SUIVIS, dans l'environnement WINDOWS classique qui est de préférence employé.

Les figures 15 à 21 illustrent divers affichages sur écran d'ordinateur qui pourront être présentés à l'utilisateur après sélection de la fenêtre PROFILS DE PARTENAIRES DE NEGOCIATION de l'affichage d'écran de la figure 14. La figure 15 montre un ensemble de trois partenaires de négociation possibles, identifié par CISCO, SEARS, et MOI, où MOI représente l'utilisateur lui-même. La figure 16 montre une boîte de dialogue possible permettant de créer le profil d'un partenaire de négociation directement sur l'écran d'ordinateur 116, 118. De même, la figure 17 illustre une boîte de dialogue possible permettant de créer une information relative au contact, pour le partenaire de négociation, directement sur l'écran d'ordinateur 116, 118. La figure 18 illustre une boîte de dialogue possible permettant de créer une information relative au qualificateur EDI directement sur l'écran d'ordinateur 116, 118. La figure 19 illustre une boîte de dialogue possible pour des clés liées de partenaires de négociation qui sont affichées et peuvent être modifiées directement sur l'écran d'ordinateur 116, 118, présentant deux options se rapportant à LIER et DELIER, un bouton IMPRIMER étant également présent. La figure 20 illustre l'affichage d'écran d'ordinateur 116, 118 dans le cas où l'option LIER LES CLES a été sélectionnée sur l'affichage de la figure 19 afin de lier une clé particulière à un partenaire de négociation particulier. La figure 21 illustre l'affichage d'écran d'ordinateur 116, 118 se rapportant à un AJOUT DE CLE permettant, par exemple, d'afficher un certificat formaté qui peut être lié au partenaire de négociation tout comme la clé.

Les figures 22 à 28 illustrent divers affichages sur écran d'ordinateur, qui peuvent être présentés à l'utilisateur après sélection de la fenêtre ACCORDS

DE PARTENAIRES DE NEGOCIATION sur l'affichage d'écran de la figure 14. La figure 22 montre un ensemble des trois mêmes partenaires de négociation que ceux identifiés sur la figure 15. La figure 23 illustre une boîte de dialogue permettant de créer, dans l'exemple précédent, un accord de partenaires de négociation entre l'utilisateur MOI, qui est l'ID local, et SEARS, qui est l'ID éloigné, directement sur l'écran d'ordinateur 116, 118. La figure 24 illustre une boîte de dialogue permettant de créer les instructions d'acheminement vers l'intérieur relatives à l'accord de partenaires de négociation, directement sur l'écran d'ordinateur 116, 118. De même, les figures 25 à 27 illustrent diverses boîtes de dialogue permettant de créer les instructions d'acheminement vers l'extérieur relatives à l'accord de partenaires de négociation, directement sur l'écran d'ordinateur 116, 118. La figure 28 illustre une boîte de dialogue permettant de sélectionner la ré-émission vers l'extérieur, directement sur l'écran d'ordinateur 116, 118.

Les figures 29 à 33 illustrent divers affichages sur écran d'ordinateur qui peuvent être présentés à l'utilisateur après sélection de la fenêtre GESTION DE CLES sur l'affichage d'écran de la figure 14. La figure 29 montre de nouveau un ensemble des trois mêmes partenaires de négociation, comme présenté sur la figure 15. La figure 30 illustre une boîte de dialogue possible associée à l'ID de clé locale, la figure 31 illustre une boîte de dialogue possible associée à l'ID de clé éloignée, la figure 32 illustre une boîte de dialogue possible associée à des détails relatifs à la clé, et la figure 33 illustre une boîte de dialogue possible associée à l'exportation de la clé publique vers un autre fichier.

Les figures 34 à 41 illustrent divers affichages sur écran d'ordinateur qui peuvent être présentés à l'utilisateur après sélection de la fenêtre SUIVIS sur l'affichage d'écran de la figure 14. La figure 34 illustre un affichage d'écran sur l'écran d'ordinateur 116, 118 où deux messages EDI ont été envoyés, un entre SEARS et CISCO, et un entre MOI et EUX, par exemple. La figure 35 illustre un affichage possible sur l'écran d'ordinateur 116, 118 concernant les échanges entre les partenaires de négociation et elle montre la non-répudiation de l'AUTACK de réception, illustrant l'état de l'AUTACK sur l'écran d'ordinateur 116, 118 selon l'invention. La figure 36 illustre un affichage possible sur l'écran d'ordinateur 116, 118, concernant les données EDI après que la boîte de dialogue VISUALISER LES DONNEES EDI a été sélectionné sur l'affichage d'écran de la figure 35. Les figures 37 à 38 illustrent des affichages d'écran possibles sur l'écran d'ordinateur 116, 118 permettant de sélectionner des critères de suivis. La figure 39 illustre un affichage

d'écran possible sur l'écran d'ordinateur 116, 118 concernant une liste de contrôle, les figures 40 à 41 illustrant des affichages d'écran possibles sur l'écran d'ordinateur 116, 118, qui permettent de sélectionner des critères de choix pour la liste de contrôle.

On se reporte maintenant à la figure 2, où est présenté le processus préféré d'authentification et de non-répudiation d'origine selon le procédé présentement préféré de l'invention. Comme on peut le voir sur la figure 2, le bloc 200 représente un échange EDI typique selon l'invention. Le bloc 202 représente l'action préférée du serveur situé à l'extrémité émetteur relativement à cet échange EDI selon le procédé de l'invention. Comme représenté, le serveur du côté émetteur calcule de préférence le MD5 (condensé de message, version 5) relatif à l'échange EDI tout entier, par exemple depuis l'ISA jusqu'au dernier caractère de l'IEA (appelé MD5EDIINTERCHANGE). Cette valeur est alors de préférence insérée en une position prédéterminée du message AUTACK, de préférence le deuxième élément du segment USY du message AUTACK. Le serveur de l'émetteur calcule de préférence alors le MD5 du message AUTACK, par exemple de préférence depuis le premier caractère de l'USH jusqu'au premier caractère de l'UST. Le serveur de l'émetteur signe de préférence alors l'AUTACK en cryptant le MD5 à l'aide de la clé privée de l'émetteur. Cette valeur calculée est ensuite de préférence insérée en une position prédéterminée de l'AUTACK, par exemple de préférence comme premier élément du segment USR du message AUTACK. Le bloc 204 représente un message AUTACK typique selon le procédé préféré de l'invention après que le serveur de l'émetteur a effectué l'action illustrée sur le bloc 202. L'AUTACK 204 est de préférence alors émis à destination du serveur du récepteur, où l'action du récepteur et la vérification effectuée par celui-ci, comme présenté dans le bloc 206, ont de préférence lieu. Si l'échange EDI est crypté, alors le serveur du récepteur décrypte de préférence celui-ci et calcule le MD5 de l'échange EDI reçu. En supposant que la non-répudiation d'origine soit souhaitée ou demandée, le serveur du récepteur décrypte de préférence alors, en utilisant la clé publique de l'émetteur, le contenu du premier élément du segment USR du message AUTACK 204, lequel est l'emplacement où le serveur de l'émetteur a inséré le MD5 de l'AUTACK. La valeur ainsi obtenue par le décryptage du MD5 du message AUTACK, dans l'exemple indiqué ci-dessus, depuis le premier caractère de l'USH jusqu'au premier caractère de l'UST. Le serveur du récepteur calcule de préférence alors le MD5 message AUTACK et compare le MD5 calculé avec la valeur du MD5 obtenue par décryptage du contenu du premier élément du

segment USR du message AUTACK. Si les deux valeurs du MD5 sont égales, alors le serveur du récepteur sait que l'intégrité de l'AUTACK a été préservée et que la non-répudiation de l'origine est établie. Le serveur du récepteur compare de préférence alors le MD5 de l'échange EDI avec le MD5 du segment USY du message AUTACK, lequel est l'emplacement ou le serveur de l'émetteur a inséré le MD5 de l'échange EDI, et, si les deux valeurs de MD5 sont égales, le serveur du récepteur sait que l'intégrité de l'échange EDI a été préservée, que l'authenticité est vérifiée et que la non-répudiation d'origine est établie.

On se reporte maintenant à la figure 3, qui présente le processus préféré de non-répudiation de la réception selon le procédé présentement préféré de l'invention. Comme on peut le voir sur le bloc 208, l'action du serveur du récepteur visant à vérifier l'intégrité et l'authenticité de l'échange EDI reçu est de préférence comme décrit ci-dessus en liaison avec le bloc 206 de la figure 2. Après cela, le serveur du récepteur crée de préférence un nouvel AUTACK, comme le message AUTACK représenté dans le bloc 210, et il transmet ce nouvel AUTACK 210 au serveur de l'émetteur afin qu'il soit vérifié par le serveur de l'émetteur original, comme représenté par le bloc 212. Ainsi qu'on peut le voir sur la figure 3, lors de la création du nouvel AUTACK, le serveur du récepteur peuple de préférence tous les segments et éléments de la manière appropriée, par exemple tous les segments et éléments allant jusqu'à UST, inclusivement. Le serveur du récepteur calcule de préférence alors le MD5 du nouvel AUTACK, par exemple depuis l'USH jusqu'au premier caractère de l'UST, et il signe le MD5 calculé à l'aide de la clé privée du récepteur. Le serveur du récepteur insère de préférence alors le MD5 signé numériquement en un emplacement prédéterminé du nouvel AUTACK, par exemple le premier élément du segment USR. Le serveur du récepteur peuple de préférence alors les segments UNT et UNZ du nouvel AUTACK de la manière appropriée et émet le nouvel AUTACK préparé à destination du serveur de l'émetteur original. Le serveur de l'émetteur original vérifie de préférence alors la signature numérique du nouvel AUTACK reçu en la décryptant à l'aide de la clé publique du récepteur, la valeur obtenue par ce décryptage étant le MD5 du nouvel AUTACK reçu. Le serveur de l'émetteur original calcule alors le MD5 du nouvel AUTACK reçu et le compare avec la valeur du MD5 obtenue à partir du processus de décryptage. Si les deux valeurs du MD5 sont identiques, alors le serveur de l'émetteur original sait que l'intégrité du nouvel AUTACK est préservée et que la non-répudiation d'origine du nouvel AUTACK est établie. Le serveur de l'émetteur de l'origine sait également que, si le MD5 contenu dans le segment USY

du nouvel AUTACK reçu, selon l'exemple ci-dessus, est égal au MD5 de l'échange EDI précédemment émis et que l'accusé de réception est positif (ceci étant de préférence obtenu par contrôle du code de sécurité du nouveau message AUTACK), alors l'échange EDI considéré est reconnu à la fois du côté l'émetteur et de celui du récepteur puisque le MD5 de l'échange EDI et le numéro d'échange sont contenus dans le message AUTACK et ont été dûment reconnus. De plus, l'intégrité et l'authenticité de l'échange EDI, au moment de la réception, ont été vérifiées et le serveur du récepteur n'a pas nié avoir reçu l'échange EDI en question.

On se reporte maintenant aux figures 4 et 5, qui représentent un organigramme de traitement du procédé présentement préféré de réception et d'émission de messages électroniques, respectivement, selon l'invention. De ce point de vue, le dispositif de commande, noté TEMPLAR, servant à mettre en oeuvre le procédé présentement préféré de l'invention est de préférence situé entre le système de messagerie classique et la table bidimensionnelle EDI spécifiée de l'utilisateur dans les système d'émission et de réception, le système classique SENDMAIL fourni avec le système d'exploitation X-WINDOWS d'UNIX ou WINDOWS de MICROSOFT étant de préférence utilisé pour envoyer et recevoir des messages, le message qui est envoyé et reçu étant de préférence conforme à la norme MIME, le système PKCS étant de préférence utilisé pour crypter et décrypter des parties de corps codées par MIME. De préférence, les identificateurs MIME ne sont pas cryptés. Comme noté ci-dessus, le message AUTACK de EDIFACT est de préférence utilisé pour délivrer de manière sûre une authentification, une non-répudiation de l'origine et, ou bien, de la réception, et un accusé de réception ou un non-accusé de réception se rapportant à une ou plusieurs enveloppes X-12 ou EDIFACT. De préférence, des enveloppes EDI multiples sont vues comme un seul bloc de données dans le système selon l'invention. De préférence, si un message AUTACK reçu ne satisfait pas une intégrité de message, l'accusé de réception n'est pas renvoyé à l'émetteur original du message, bien que, si cela est souhaitable, il soit possible de facilement modifier le système pour l'obtenir.

On se reporte maintenant aux figures 6 à 9, qui représentent des organigrammes se rapportant à la gestion de partenaires de négociation, à la gestion de listes de contrôle, à la gestion d'opérations de suivis et la surveillance de travaux, respectivement, selon le procédé présentement préféré de l'invention. Ces organigrammes s'expliquent d'eux-mêmes lorsqu'on les envisage en liaison avec la

discussion précédente, et, dans un souci de brièveté, on ne les décrira pas de manière plus détaillée. Toutefois, le lecteur voudra bien admettre que leur contenu est incorporé dans cette description.

La figure 10 est un diagramme fonctionnel montrant l'organisation du procédé présentement préféré de l'invention, tel que représenté par le scénario du tableau A et la précédente description, et on ne le décrira pas de manière plus détaillée. Le lecteur voudra toutefois bien considérer que son contenu est intégré dans la description.

Enfin, les figures 11 à 13 représentent un organigramme du procédé présentement préféré de l'invention en liaison avec la description précédente, où la figure 11 illustre diverses opérations de vérification de l'intégrité de l'AUTACK, de l'échange EDI et du certificat, NRO représentant la non-répudiation d'origine, tandis que NRR représente la non-répudiation de réception. La figure 12 illustre la partie du procédé se rapportant au traitement de la TPA. La figure 13 illustre la partie du procédé de l'invention qui est appliquée au traitement des clés publiques et privées, de même TPA, dans la mise en oeuvre du procédé de l'invention tel que ci-dessus décrit.

Par conséquent, en utilisant le message AUTACK comme document se rapportant à la signature numérique, laquelle est effectuée sur la base d'un système de clés publiques/privées, comme par exemple le système du type RSA, on réalise un système de messagerie efficace et d'une haute sécurité pour effectuer des échanges EDI sur un réseau ouvert, par exemple le réseau INTERNET, dans lequel système des partenaires de négociation peuvent facilement obtenir, de manière sûre, la vérification et l'authentification ainsi que la non-répudiation d'à la fois l'origine et la réception, qui sont toutes importantes, pour des transitions d'affaires électroniques rapides s'étendant sur une zone géographique largement étendue dans laquelle un réseau ouvert constitue le moyen de télécommunications le plus normal.

Bien entendu, l'homme de l'art sera en mesure d'imaginer, à partir du système et du procédé dont la description vient d'être donnée à titre simplement illustratif et nullement limitatif, diverses variantes et modifications ne sortant pas du cadre de l'invention.

REVENDICATIONS

1. Système de télécommunications permettant d'interconnecter sélectivement une pluralité d'ordinateurs (112, 114) sur un réseau public ouvert (120, 102, 122) sur lequel lesdits ordinateurs échangent des messages numériques de sécurité entre un ordinateur émetteur (112) et un ordinateur récepteur (114) de ladite pluralité d'ordinateurs, ledit ordinateur émetteur ayant une première clé publique associée et une première clé privée associée, ledit ordinateur récepteur ayant une deuxième clé publique associée et une deuxième clé privée associée, lesdits messages numériques comprenant une communication d'échange EDI, ou échange de données électronique, entre ledit ordinateur émetteur et ledit ordinateur récepteur, ladite communication d'échange EDI ayant un message d'accusé de réception d'EDI associé ; caractérisé en ce qu'il comprend :

un moyen servant à calculer un premier code de hachage pour ladite communication d'échange d'EDI venant dudit ordinateur émetteur ;

un moyen servant à insérer ledit premier code de hachage en un emplacement prédéterminé dudit message d'accusé de réception d'EDI associé ;

un moyen servant à calculer un deuxième code de hachage dudit message d'accusé de réception d'EDI associé ;

un moyen servant à signer numériquement ledit message d'accusé de réception d'EDI associé, ledit moyen de signature numérique du message comprenant un moyen qui crypte ledit deuxième code de hachage à l'aide de ladite clé privée de l'ordinateur émetteur ;

un moyen servant à insérer ledit deuxième code de hachage en un emplacement prédéterminé dudit message d'accusé de réception d'EDI associé ;

un moyen servant à transmettre ladite communication d'échange EDI en même temps que ledit message d'accusé de réception d'EDI associé qui était numériquement signé audit ordinateur récepteur sur ledit réseau public ouvert ; et

un moyen associé audit ordinateur récepteur et servant à recevoir et à traiter ladite communication d'échange EDI reçue et ledit message d'accusé de réception d'EDI numériquement signé afin de fournir une authentification et une non-répudiation de ladite communication d'échange EDI venant dudit ordinateur émetteur, ledit moyen comprenant un moyen qui décrypte à l'aide de ladite clé publique de l'ordinateur émetteur ledit deuxième code de hachage crypté ; de sorte que des communications d'échange EDI privées sûres peuvent avoir lieu sur un

réseau public ouvert tout en assurant l'authentification et la non-répudiation desdites communications EDI

2. Système selon la revendication 1, caractérisé en ce que ledit moyen associé audit ordinateur récepteur comprend en outre un moyen servant à calculer un troisième code de hachage dudit message d'accusé de réception d'EDI reçu ; et un moyen servant à comparer ledit troisième code de hachage avec ledit deuxième code de hachage décrypté provenant dudit message d'accusé de réception d'EDI reçu, ledit moyen de comparaison comprenant un moyen qui produit une indication de l'intégrité dudit message d'accusé de réception d'EDI et de la non-répudiation de l'origine lorsque ledit deuxième code de hachage décrypté et ledit troisième code de hachage sont en accord.

3. Système selon la revendication 2, caractérisé en ce que ledit moyen associé audit ordinateur récepteur comprend en outre un moyen servant à calculer un quatrième code de hachage de ladite communication d'échange EDI reçue ; et un moyen servant à comparer ledit quatrième code de hachage de ladite communication d'échange EDI reçue avec ledit premier code de hachage se trouvant dans ledit message d'accusé de réception d'EDI reçu, ledit moyen de comparaison comprenant un moyen qui produit une indication de l'intégrité et de la vérification de l'authenticité de ladite communication d'échange EDI et de la non-répudiation de l'origine lorsque les premier et quatrième codes de hachage sont en accord.

4. Système selon la revendication 3, caractérisé en ce que ledit moyen associé audit ordinateur récepteur comprend en outre un moyen servant à créer un message d'accusé de réception d'EDI de réponse et à transmettre ledit message d'accusé de réception d'EDI de réponse audit ordinateur émetteur sur ledit réseau public ouvert, ledit moyen de création de message d'accusé de réception d'EDI de réponse comprenant un moyen servant à calculer un cinquième code de hachage dudit message d'accusé de réception d'EDI de réponse et à signer numériquement ledit cinquième code de hachage par cryptage dudit cinquième code de hachage à l'aide de ladite clé privée de l'ordinateur récepteur ; et un moyen servant à insérer ledit cinquième code de hachage numériquement signé en un emplacement prédéterminé dudit message d'accusé de réception d'EDI de réponse transmis.

5. Système selon la revendication 4, caractérisé en ce qu'il comprend en outre un moyen associé audit ordinateur émetteur et servant à recevoir ledit message d'accusé de réception d'EDI de réponse transmis, et à décrypter à l'aide de ladite clé publique de l'ordinateur récepteur ledit cinquième code de hachage crypté afin de vérifier ladite signature numérique dudit message d'accusé de

réception d'EDI de réponse ; et un moyen servant à calculer un sixième code de hachage dudit message d'accusé de réception d'EDI de réponse de réponse reçu ; et un moyen servant à comparer ledit sixième code de hachage avec ledit cinquième code de hachage décrypté, ledit moyen de comparaison comprenant un moyen qui fournit une indication de l'intégrité dudit message d'accusé de réception d'EDI de réponse reçue et de la non-répudiation de l'origine dudit message d'accusé de réception d'EDI de réponse ; de sorte que la non-répudiation de la réception de ladite communication d'échange EDI est établie par ledit ordinateur émetteur.

6. Système selon la revendication 5, où ledit moyen servant à créer ledit message d'accusé de réception d'EDI de réponse comprend en outre un moyen servant à insérer ledit quatrième code de hachage en un emplacement prédéterminé dudit message d'accusé de réception d'EDI de réponse transmis, et ledit moyen associé audit ordinateur émetteur comprend en outre un moyen servant comparer ledit quatrième code de hachage se trouvant dans ledit message d'accusé de réception d'EDI de réponse reçu avec ledit premier code de hachage, ledit moyen de comparaison fournissant une indication de l'intégrité et de l'authenticité dudit échange EDI lorsque lesdits premier et quatrième codes de hachage sont en accord.

7. Système selon la revendication 6, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

8. Système selon la revendication 7, caractérisé en ce que ledit message d'accusé de réception d'EDI de réponse comprend un message AUTACK.

9. Système selon la revendication 8, caractérisé en ce que chacun desdits codes de hachage comprend un MD5, ou condensé de message version 5.

10. Système selon la revendication 9, caractérisé en ce que lesdites clés publiques et privées comprennent un système de télécommunications cryptographique de type RSA.

11. Système selon la revendication 10, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

12. Système selon la revendication 1, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

13. Système selon la revendication 1, caractérisé en ce que ledit moyen associé audit ordinateur récepteur comprend en outre un moyen servant à créer un message d'accusé de réception d'EDI de réponse et à transmettre ledit message d'accusé de réception d'EDI de réponse audit ordinateur émetteur sur ledit réseau public ouvert, ledit moyen de création de message d'accusé de réception d'EDI de réponse comprenant un moyen servant à calculer un troisième code de hachage

dudit message d'accusé de réception d'EDI de réponse et à signer numériquement ledit troisième code de hachage en cryptant ledit troisième code de hachage à l'aide de ladite clé privée de l'ordinateur récepteur ; et un moyen servant à insérer ledit troisième code de hachage signé numériquement en un emplacement prédéterminé dudit message d'accusé de réception d'EDI de réponse transmis.

14. Système selon la revendication 13, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

15. Système selon la revendication 14, caractérisé en ce qu'il comprend en outre un moyen associé avec ledit ordinateur émetteur et servant à recevoir ledit message d'accusé de réception d'EDI de réponse transmis et à décrypter à l'aide de ladite clé publique de l'ordinateur récepteur ledit troisième code de hachage crypté afin de vérifier ladite signature numérique dudit message d'accusé de réception de débit de réponse ; et un moyen servant à calculer un quatrième code de hachage dudit message d'accusé de réception d'EDI de réponse de réponse reçu ; un moyen servant à comparer ledit quatrième code de hachage avec ledit troisième code de hachage ; et un moyen servant à comparer ledit quatrième code de hachage avec ledit troisième code de hachage décrypté, ledit moyen de comparaison comprenant un moyen qui fournit une indication de l'intégrité dudit message d'accusé de réception d'EDI de réponse reçu et de la non-répudiation d'origine dudit message d'accusé de réception d'EDI de réponse ; de sorte que la non-répudiation de réception de ladite communication d'échange EDI est établie par ledit ordinateur émetteur.

16. Système selon la revendication 13, caractérisé en ce qu'il comprend en outre un moyen associé audit ordinateur émetteur et servant à recevoir ledit message d'accusé de réception d'EDI de réponse transmis et à décrypter à l'aide de ladite clé publique de l'ordinateur récepteur ledit troisième code de hachage crypté afin de vérifier ladite signature numérique dudit message d'accusé de réception d'EDI de réponse ; et un moyen servant à calculer un quatrième code de hachage dudit message d'accusé de réception d'EDI de réponse de réponse reçu ; et un moyen servant à comparer ledit quatrième code de hachage avec ledit troisième code de hachage décrypté, ledit moyen de comparaison comprenant un moyen qui fournit une indication de l'intégrité dudit message d'accusé de réception d'EDI de réponse reçu et de la non-répudiation d'origine dudit message d'accusé de réception d'EDI de réponse ; de sorte que la non-répudiation de réception de ladite communication d'échange EDI est établie par ledit ordinateur émetteur.

17. Système selon la revendication 4, caractérisé en ce que ledit moyen servant à créer ledit message d'accusé de réception d'EDI de réponse comprend en outre un moyen servant à insérer ledit quatrième code de hachage en un emplacement prédéterminé dudit message d'accusé de réception d'EDI de réponse transmis, et ledit moyen associé audit ordinateur émetteur comprend en outre un moyen servant à comparer ledit quatrième code de hachage contenu dans ledit message d'accusé de réception d'EDI de réponse reçu avec ledit premier code de hachage, ledit moyen de comparaison fournissant une indication de l'intégrité et de l'authenticité dudit échange EDI lorsque lesdits premier et quatrième codes de hachage sont en accord.

18. Système selon la revendication 1, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUDACK.

19. Système selon la revendication 18, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

20. Système selon la revendication 19, caractérisé en ce que chacun desdits codes de hachage comprend un MD5, ou condensé de message version 5.

21. Système selon la revendication 1, caractérisé en ce que chacun desdits codes de hachage comprend un MD5, ou condensé de message version 5.

22. Système selon la revendication 21, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

23. Système selon la revendication 21, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

24. Système selon la revendication 23, caractérisé en ce que lesdites clés publiques et privées comprennent un système de télécommunications cryptographique du type RSA.

25. Système selon la revendication 24, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

26. Système selon la revendication 1, caractérisé en ce que lesdites clés publiques et privées comprennent un système de télécommunications cryptographique du type RSA.

27. Système selon la revendication 26, en ce que ledit réseau public ouvert comprend le réseau INTERNET.

28. Système selon la revendication 13, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

29. Système selon la revendication 28, caractérisé en ce que ledit message d'accusé de réception d'EDI de réponse comprend un message AUTACK.

30. Système selon la revendication 13, caractérisé en ce que ledit message d'accusé de réception d'EDI de réponse comprend un message AUTACK.

31. Système selon la revendication 1, caractérisé en ce qu'il comprend un moyen servant à produire une communication d'accord de partenaires de négociation entre ledit ordinateur émetteur et ledit ordinateur récepteur, ledit ordinateur émetteur et ledit ordinateur récepteur comprenant des partenaires de négociation, ladite communication d'accord de partenaires de négociation comprenant lesdites clés publiques contenues dans ladite communication d'échange EDI afin de permettre auxdits partenaires de négociation de se fournir mutuellement des certifications.

32. Système selon la revendication 31, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

33. Système selon la revendication 32, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

34. Système selon la revendication 31, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

35. Procédé permettant d'interconnecter sélectivement une pluralité d'ordinateurs sur un réseau public ouvert afin d'effectuer un échange par ordinateurs de messages numériques de sécurité privés entre un ordinateur émetteur et un ordinateur récepteur appartenant à ladite pluralité d'ordinateurs, ledit ordinateur émetteur ayant une première clé publique associé et une première clé privée associée, ledit ordinateur récepteur ayant une deuxième clé publique associée et une deuxième clé privée associée, lesdits messages numériques comprenant une communication d'échange EDI entre ledit ordinateur émetteur et ledit ordinateur récepteur, ladite communication d'échange EDI ayant un message d'accusé de réception d'EDI associé, ledit procédé étant caractérisé en ce qu'il comprend les opérations suivantes : signer numériquement ledit message d'accusé de réception d'EDI associé à l'aide de ladite clé privée de l'ordinateur émetteur ; transmettre ladite communication d'échange EDI en même temps que ledit message d'accusé de réception d'EDI associé numériquement signé audit ordinateur récepteur sur ledit réseau public ouvert ; et traiter ledit message d'accusé de réception d'EDI numériquement signé reçu afin de fournir une authentification et une non-répudiation de ladite communication d'échange EDI provenant dudit ordinateur émetteur, ladite opération de traitement comprenant l'opération qui consiste à traiter ledit message d'accusé de réception d'EDI associé numériquement signé reçu à l'aide de ladite clé publique de l'ordinateur émetteur ; si bien que des

communications d'échange d'EDI privées sûres peuvent avoir lieu sur un réseau public ouvert tout en fournissant une authentification et une non-répudiation desdites communications EDI à l'aide dudit message d'accusé de réception d'EDI associé.

36. Procédé selon la revendication 35, où ledit réseau publique ouvert comprend le réseau INTERNET.

37. Procédé selon la revendication 36, caractérisé en ce qu'il comprend les opérations consistant à : créer un message d'accusé de réception d'EDI de réponse venant dudit ordinateur récepteur ; signer numériquement ledit message d'accusé de réception d'EDI de réponse à l'aide de ladite clé privée de l'ordinateur récepteur ; transmettre ledit message d'accusé de réception d'EDI de réponse numériquement signé audit ordinateur émetteur sur ledit réseau public ouvert, ledit ordinateur émetteur recevant ledit message d'accusé de réception d'EDI de réponse numériquement signé ; et traiter ledit message d'accusé de réception d'EDI de réponse numériquement signé reçu en fournissant une non-répudiation de réception de ladite communication d'échange EDI par ledit ordinateur émetteur, ladite opération de traitement comprenant l'opération qui consiste à traiter le message d'accusé de réception d'EDI de réponse numériquement signé reçu à l'aide de ladite clé publique de l'ordinateur récepteur ; si bien que la non-répudiation de réception de ladite communication d'échange EDI est établie par ledit ordinateur émetteur.

38. Procédé selon la revendication 35, caractérisé en ce qu'il comprend en outre les opérations suivantes : créer un message d'accusé de réception d'EDI de réponse venant dudit ordinateur récepteur ; signer numériquement ledit message d'accusé de réception d'EDI de réponse à l'aide de ladite clé privée de l'ordinateur récepteur ; transmettre ledit message d'accusé de réception d'EDI de réponse numériquement signé audit ordinateur émetteur sur ledit réseau public ouvert, ledit ordinateur émetteur recevant ledit message d'accusé de réception d'EDI de réponse numériquement signé ; et traiter ledit message d'accusé de réception d'EDI de réponse numériquement signé reçue en fournissant une non-répudiation de réception de ladite communication d'échange EDI par ledit ordinateur émetteur, ladite opération de traitement comprenant l'opération qui consiste à traiter ledit message d'accusé de réception d'EDI de réponse numériquement signé reçu à l'aide de ladite clé publique de l'ordinateur récepteur ; si bien que la non-répudiation de réception de ladite communication d'échange EDI est établie par ledit ordinateur émetteur.

39. Procédé selon la revendication 38, caractérisé en ce que ladite opération de traitement comprend en outre l'opération consistant à produire la non-répudiation d'origine dans ledit ordinateur récepteur à partir dudit message d'accusé de réception d'EDI reçu.

40. Procédé selon la revendication 39, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

41. Procédé selon la revendication 35, caractérisé en ce que ladite opération de traitement comprend en outre l'opération qui consiste à produire la non-répudiation d'origine dans ledit ordinateur récepteur à partir dudit message d'accusé de réception d'EDI reçu.

42. Procédé selon la revendication 35, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

43. Procédé selon la revendication 38, caractérisé en ce que ledit message d'accusé de réception d'EDI de réponse comprend un message AUTACK.

44. Procédé selon la revendication 43, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

45. Procédé selon la revendication 35, caractérisé en ce que lesdites clés publiques et privées comprennent un système de télécommunications cryptographique du type RSA.

46. Procédé selon la revendication 45, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

47. Procédé selon la revendication 45, caractérisé en ce que ledit message d'accusé de réception d'EDI comprend un message AUTACK.

48. Procédé selon la revendication 47, caractérisé en ce qu'il comprend les opérations suivantes : créer un message d'accusé de réception d'EDI de réponse venant dudit ordinateur récepteur ; signer numériquement ledit message d'accusé de réception d'EDI de réponse à l'aide de ladite clé privée de l'ordinateur récepteur ; transmettre ledit message d'accusé de réception d'EDI de réponse numériquement signé audit ordinateur émetteur sur ledit réseau public ouvert, ledit ordinateur émetteur recevant ledit message d'accusé de réception d'EDI de réponse numériquement signé ; et traiter ledit message d'accusé de réception d'EDI de réponse numériquement signé reçu en fournissant la non-répudiation de réception de ladite communication d'échange EDI par ledit ordinateur émetteur, ladite opération de traitement comprenant l'opération qui consiste à traiter ledit message d'accusé de réception d'EDI de réponse numériquement signé reçu à l'aide de ladite

clé publique de l'ordinateur récepteur ; si bien que la non-répudiation de réception de ladite communication d'échange EDI est établie par ledit ordinateur émetteur.

49. Procédé selon la revendication 48, caractérisé en ce que ledit message d'accusé de réception d'EDI de réponse comprend un message AUTACK.

50. Procédé selon la revendication 49, caractérisé en ce que ledit réseau public ouvert comprend le réseau INTERNET.

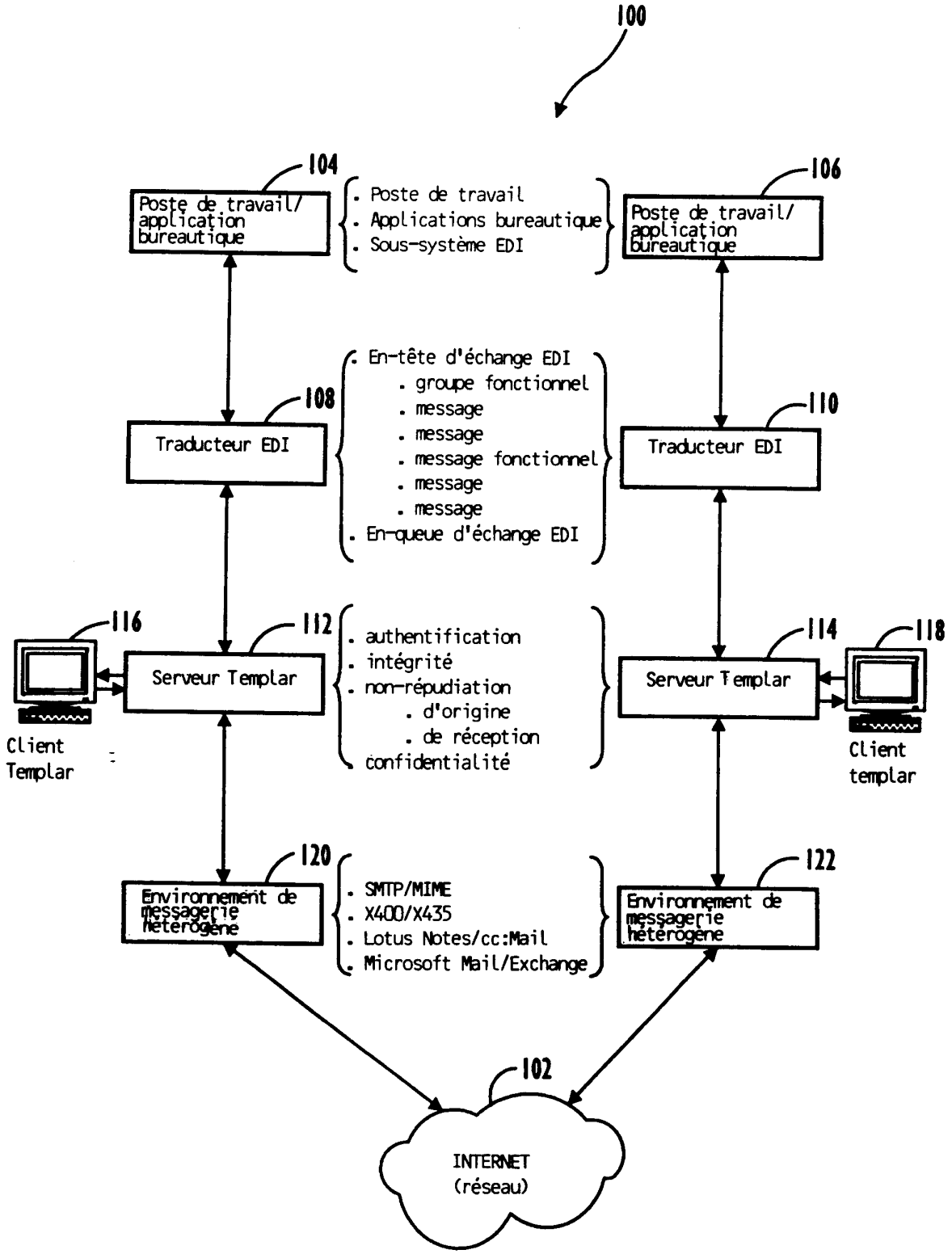

100
104
Poste de travail/ application bureautique
. Poste de travail
. Applications bureautique
. Sous-système EDI
106
Poste de travail/ application bureautique
108
Traducteur EDI
. En-tête d'échange EDI
. groupe fonctionnel
. message
. message
. message fonctionnel
. message
. message
. En-queue d'échange EDI
110
Traducteur EDI
116
112
Serveur Templar
. authentification
. intégrité
. non-répudiation
. d'origine
. de réception
. confidentialité
114
Serveur Templar
118
Client Templar
Client templar
120
Environnement de messagerie hétérogène
. SMTP/MIME
. X400/X435
. Lotus Notes/cc:Mail
. Microsoft Mail/Exchange
122
Environnement de messagerie hétérogène
102
INTERNET
(réseau)

FIG. 1

Processus d'authentification et de non-répudiation d'origine

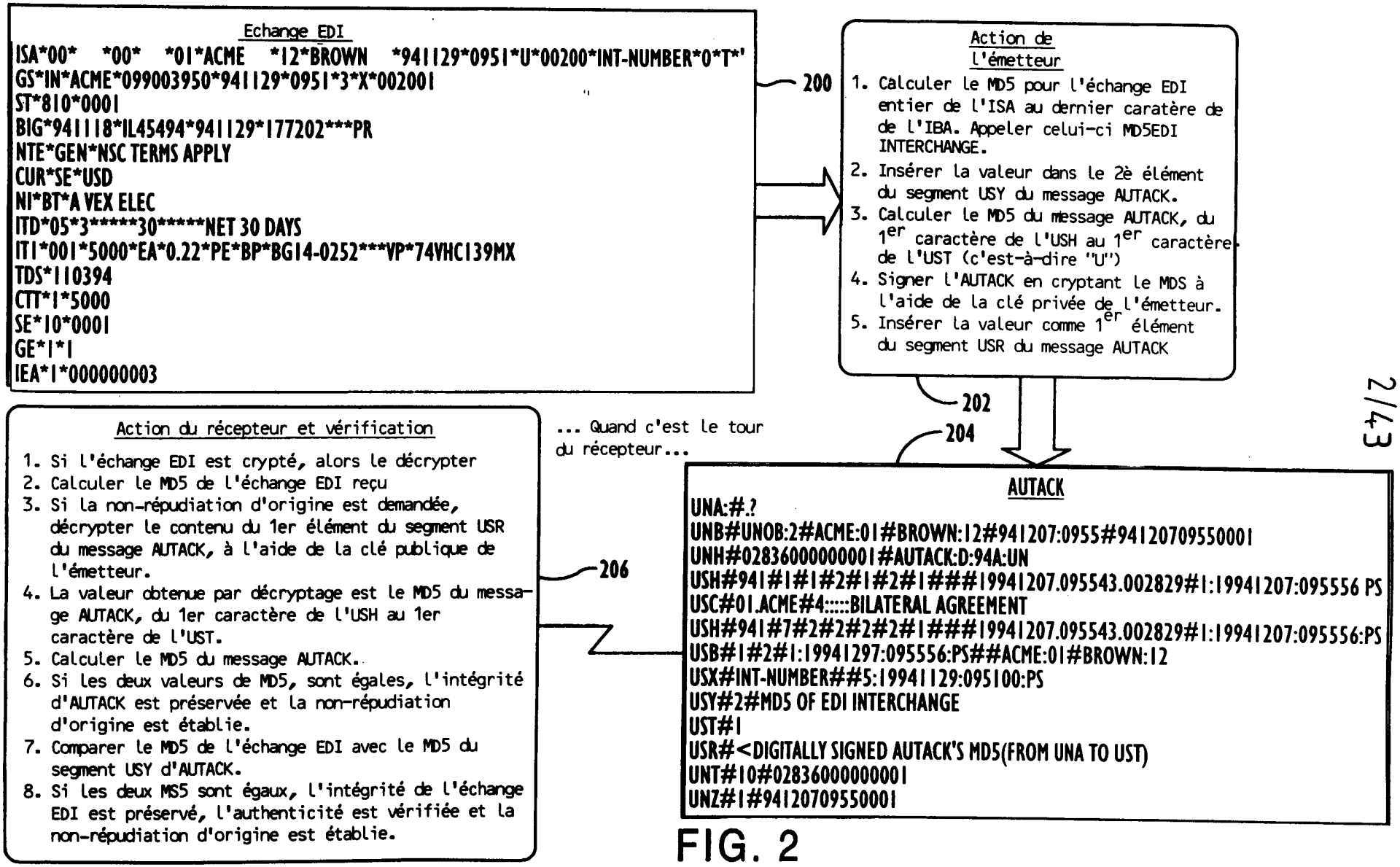


FIG. 2

Processus de non-répudiation de réception

Action du récepteur

1. Comme décrit sur la figure 2, vérifier l'intégrité et l'authenticité de l'échange EDI reçu
2. Créer un nouvel AUTACK, comme suit :
   a) peupler tous les segments et éléments jusqu'à UST inclusivement comme approprié ;
   b) signer le MD5 calculé avec la clé privée du récepteur (le MD5 est calculé de l'USH au 1er caractère de l'UST, c'est-à-dire à 'U'.) ;
   c) insérez le MD5 signé numériquement dans le 1er élément du segment USR ;
   d) peupler les segments UNT comme approprié.
3. Transmettre l'AUTACK préparé à l'émetteur

208

AUTACK

```
UNA:#.?
UNB#UNOB:2#ACME:01#BROWN:12#941207:0955#94120709550001
UNH#02836000000001#AUTACK:D:94A:UN
USH#941#1#1#2#1#2#1###19941207.095543.002829#1:19941207:095556:PS
USC#01.ACME#4:::::BILATERAL AGREEMENT
USH#941#7#2#2#2#2#1###19941207.095543.002829#1:19941207:095556:PS
USB#1#2#1:19941297:095556:PS##ACME#01#BROWN:12
USX#INT-NUMBER##5:19941129:095100:PS
USY#2#MD5 OF EDI INTERCHANGE
UST#1
USR#<AUTACK'S MD5 DIGITALLY SIGNED BY RECEIVER (MD5
COMPUTED FROM USH TO THE FIRST CHR. OF UST)
UNT#10#02836000000001
UNZ#1#94120709550001
```

210

... Quand c'est le tour de l'émetteur ... 212

Vérification par l'émetteur de l'original

1. Vérifier la signature numérique en la décryptant avec la clé publique du récepteur. La valeur obtenue le décryptage est le MD5 de l'AUTACK reçu.
2. Calculer le MD5 de l'AUTACK reçu. Si le MD5 est égal au MD5 décrypté, l'intégrité de l'AUTACK est préservée et la non-répudiation d'origine de l'AUTACK est établie.
3. Si le MD5 contenu dans le segment USY de l'AUTACK reçu est égal au MD5 de l'échange EDI précédemment transmis et si l'accusé de réception est positif (déduit du contrôle du code de sécurité de l'AUTACK) alors ceci entraîne ce qui suit :
   a) l'échange EDI en question est reconnu pour l'émetteur et le récepteur, puisque le MD5 de l'échange EDI et le numéro de l'échange sont contenus dans l'AUTACK et ont été dûment reconnus ;
   b) l'intégrité et l'authenticité de l'échange EDI au moment de la réception ont été vérifiées ;
   c) le récepteur ne nie pas avoir reçu l'échange EDI en question.

FIG. 3

2737067

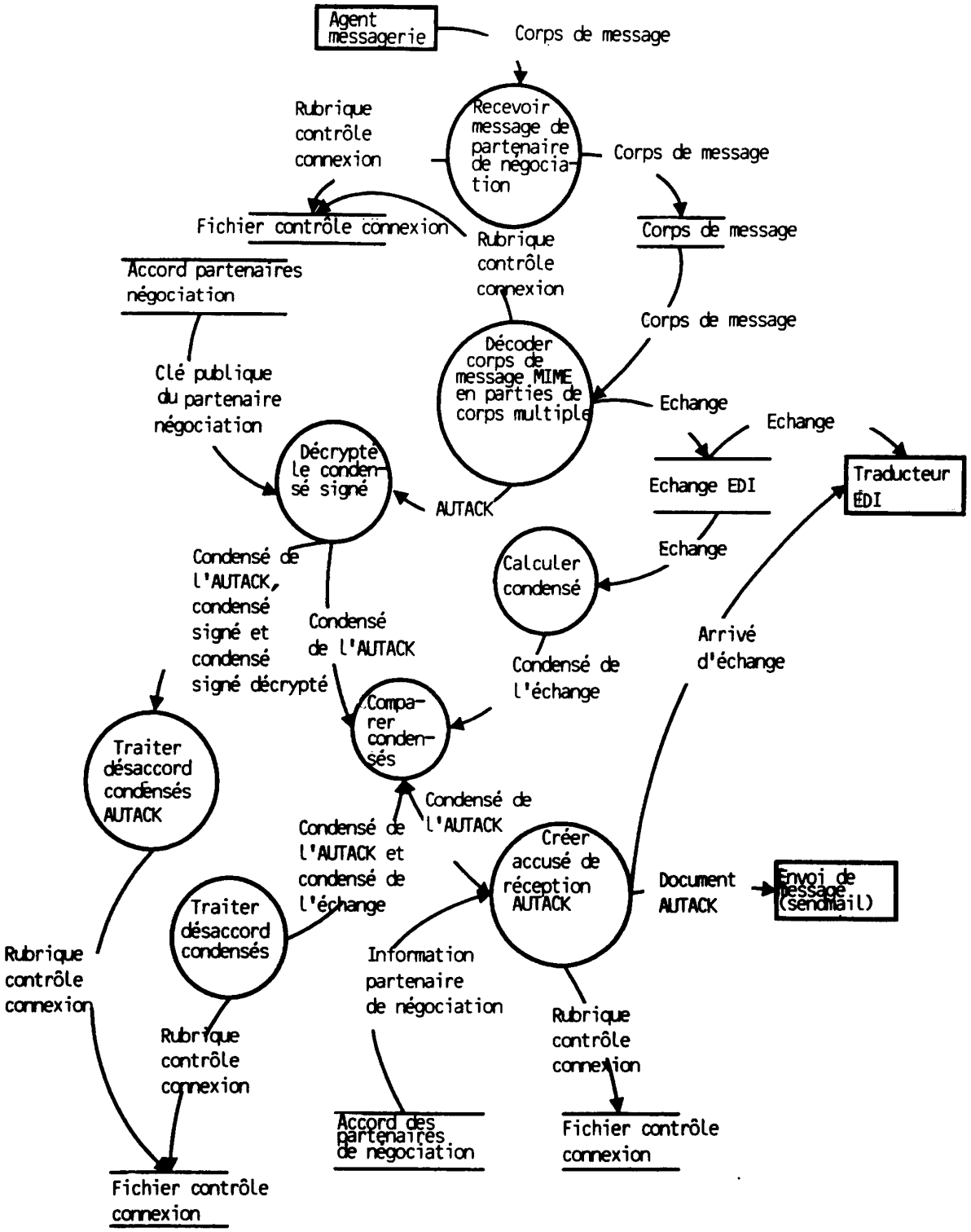

Agent messagerie
Corps de message
Recevoir message de partenaire de négociation
Rubrique contrôle connexion
Corps de message
Fichier contrôle connexion
Rubrique contrôle connexion
Corps de message
Accord partenaires négociation
Corps de message
Décoder corps de message MIME en parties de corps multiple
Clé publique du partenaire négociation
Echange
Echange
Décrypte le condensé signé
Echange EDI
Traducteur EDI
AUTACK
Echange
Condensé de l'AUTACK, condensé signé et condensé signé décrypté
Calculer condensé
Condensé de l'AUTACK
Arrivé d'échange
Condensé de l'échange
Comparer condensés
Traiter désaccord condensés AUTACK
Condensé de l'AUTACK
Condensé de l'AUTACK et condensé de l'échange
Créer accusé de réception AUTACK
Document AUTACK
Envoi de message (sendmail)
Traiter désaccord condensés
Rubrique contrôle connexion
Information partenaire de négociation
Rubrique contrôle connexion
Rubrique contrôle connexion
Accord des partenaires de négociation
Fichier contrôle connexion
Fichier contrôle connexion

FIG. 4

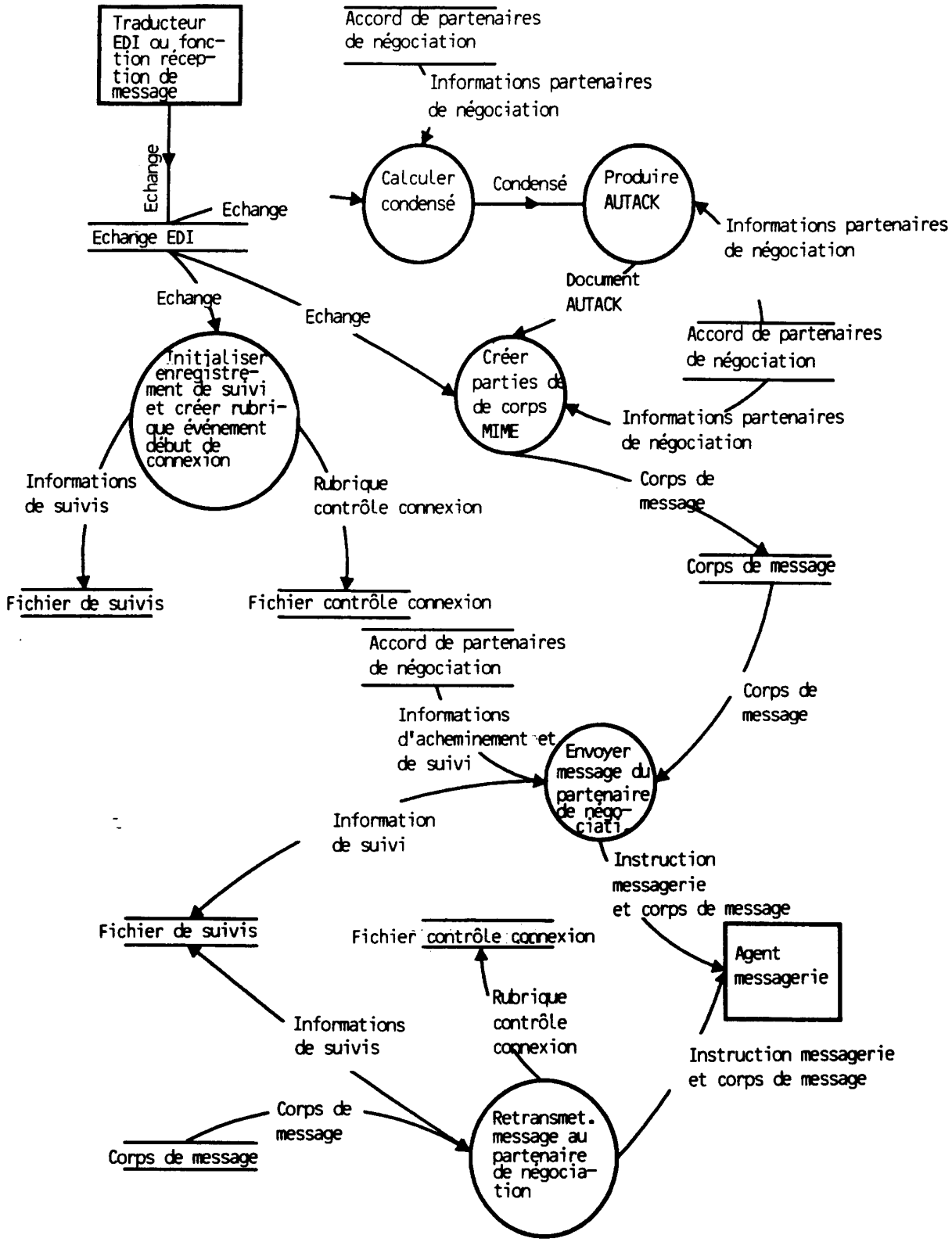

Traducteur EDI ou fonction réception de message
Accord de partenaires de négociation
Informations partenaires de négociation
Echange
Echange
Echange EDI
Calculer condensé
Condensé
Produire AUTACK
Informations partenaires de négociation
Document AUTACK
Echange
Echange
Initialiser enregistrement de suivi et créer rubrique événement début de connexion
Créer parties de de corps MIME
Accord de partenaires de négociation
Informations partenaires de négociation
Informations de suivis
Rubrique contrôle connexion
Corps de message
Corps de message
Fichier de suivis
Fichier contrôle connexion
Accord de partenaires de négociation
Informations d'acheminement et de suivi
Envoyer message du partenaire de négociati.
Corps de message
Information de suivi
Instruction messagerie et corps de message
Fichier de suivis
Fichier contrôle connexion
Agent messagerie
Rubrique contrôle connexion
Informations de suivis
Instruction messagerie et corps de message
Corps de message
Corps de message
Retransmet. message au partenaire de négociation

FIG. 5

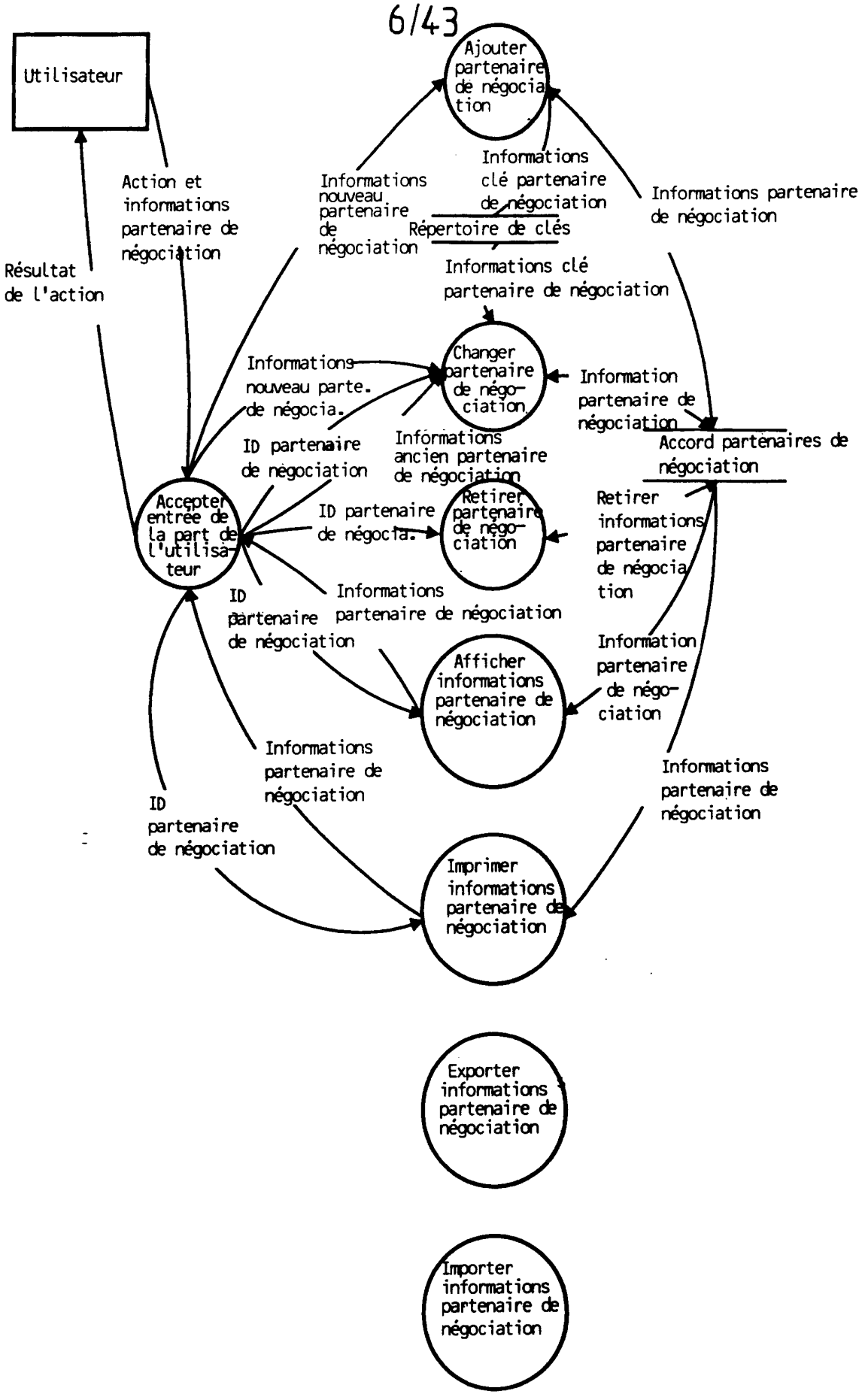

Utilisateur
Ajouter partenaire de négociation
Action et informations partenaire de négociation
Informations nouveau partenaire de négociation
Informations clé partenaire de négociation
Répertoire de clés
Informations partenaire de négociation
Résultat de l'action
Informations clé partenaire de négociation
Changer partenaire de négociation
Informations nouveau parte. de négocia.
Information partenaire de négociation
Accord partenaires de négociation
ID partenaire de négociation
Informations ancien partenaire de négociation
Accepter entrée de la part de l'utilisateur
ID partenaire de négocia.
Retirer partenaire de négociation
Retirer informations partenaire de négociation
Informations partenaire de négociation
ID partenaire de négociation
Information partenaire de négociation
Afficher informations partenaire de négociation
Informations partenaire de négociation
Informations partenaire de négociation
ID partenaire de négociation
Imprimer informations partenaire de négociation
Exporter informations partenaire de négociation
Importer informations partenaire de négociation

FIG.6

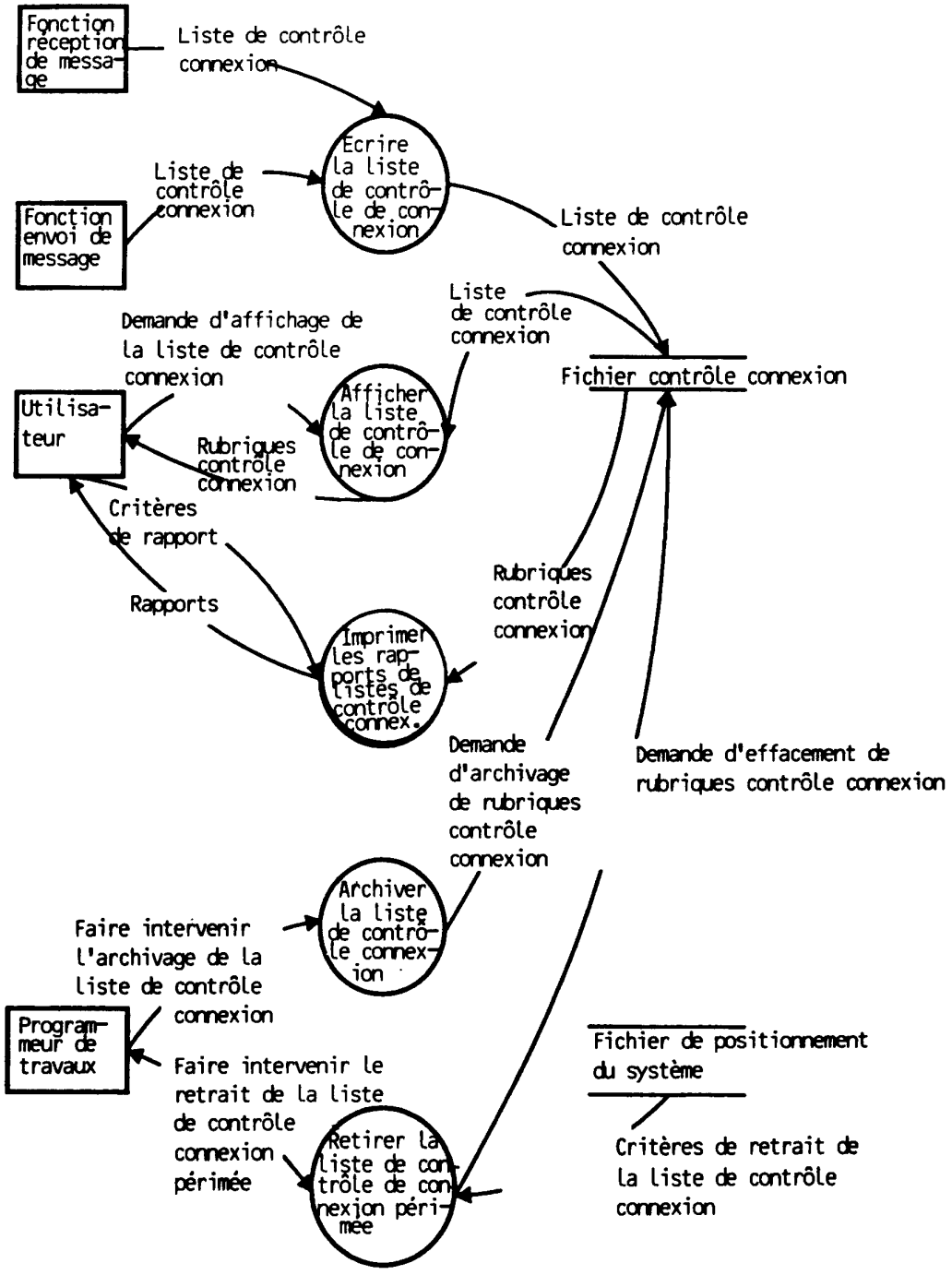

Fonction réception de message
Liste de contrôle connexion
Ecrire la liste de contrôle de connexion
Liste de contrôle connexion
Fonction envoi de message
Liste de contrôle connexion
Liste de contrôle connexion
Fichier contrôle connexion
Demande d'affichage de la liste de contrôle connexion
Utilisateur
Afficher la liste de contrôle de connexion
Rubriques contrôle connexion
Critères de rapport
Rapports
Imprimer les rapports de listes de contrôle connex.
Rubriques contrôle connexion
Demande d'archivage de rubriques contrôle connexion
Demande d'effacement de rubriques contrôle connexion
Archiver la liste de contrôle connexion
Faire intervenir l'archivage de la liste de contrôle connexion
Programmeur de travaux
Faire intervenir le retrait de la liste de contrôle connexion périmée
Retirer la liste de contrôle de connexion périmée
Fichier de positionnement du système
Critères de retrait de la liste de contrôle connexion

FIG.7

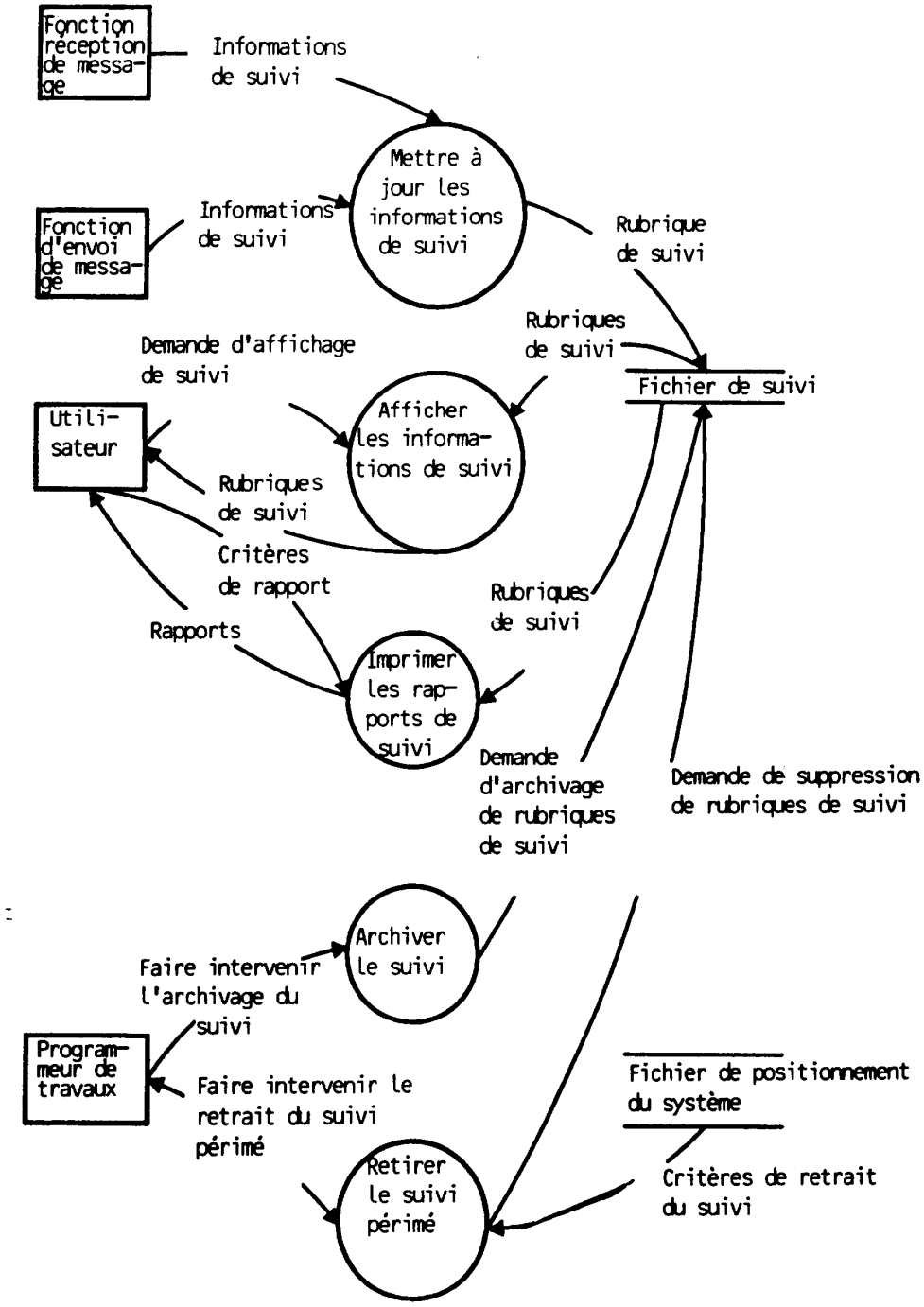

Fonction réception de message
Informations de suivi
Mettre à jour les informations de suivi
Fonction d'envoi de message
Informations de suivi
Rubrique de suivi
Rubriques de suivi
Fichier de suivi
Demande d'affichage de suivi
Afficher les informations de suivi
Utilisateur
Rubriques de suivi
Critères de rapport
Rapports
Rubriques de suivi
Imprimer les rapports de suivi
Demande d'archivage de rubriques de suivi
Demande de suppression de rubriques de suivi
Archiver le suivi
Faire intervenir l'archivage du suivi
Programmeur de travaux
Faire intervenir le retrait du suivi périmé
Fichier de positionnement du système
Retirer le suivi périmé
Critères de retrait du suivi

FIG.8

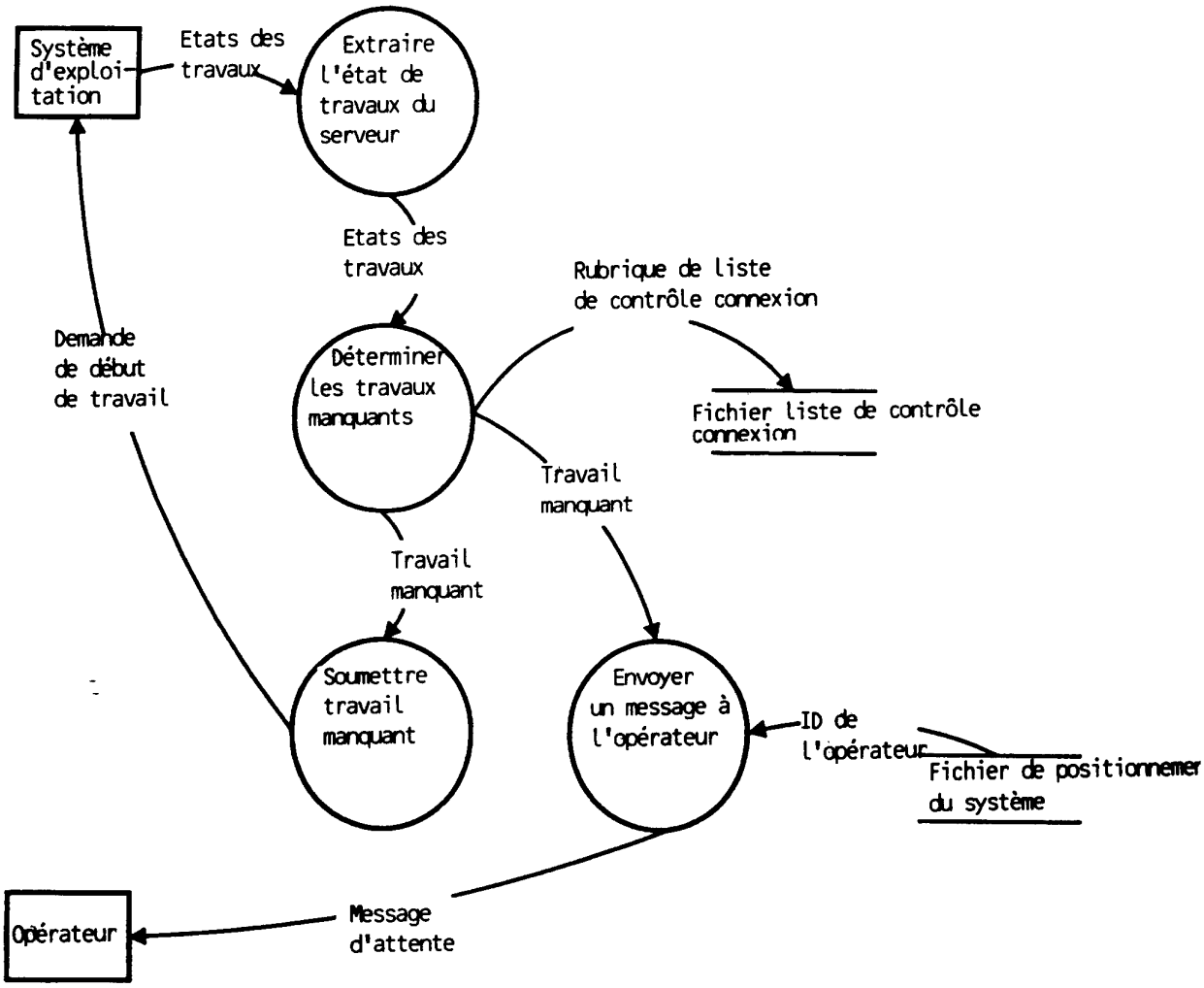

Système d'exploitation
Etats des travaux
Extraire l'état de travaux du serveur
Etats des travaux
Rubrique de liste de contrôle connexion
Demande de début de travail
Déterminer les travaux manquants
Fichier liste de contrôle connexion
Travail manquant
Travail manquant
Soumettre travail manquant
Envoyer un message à l'opérateur
ID de l'opérateur
Fichier de positionnement du système
Opérateur
Message d'attente

FIG.9

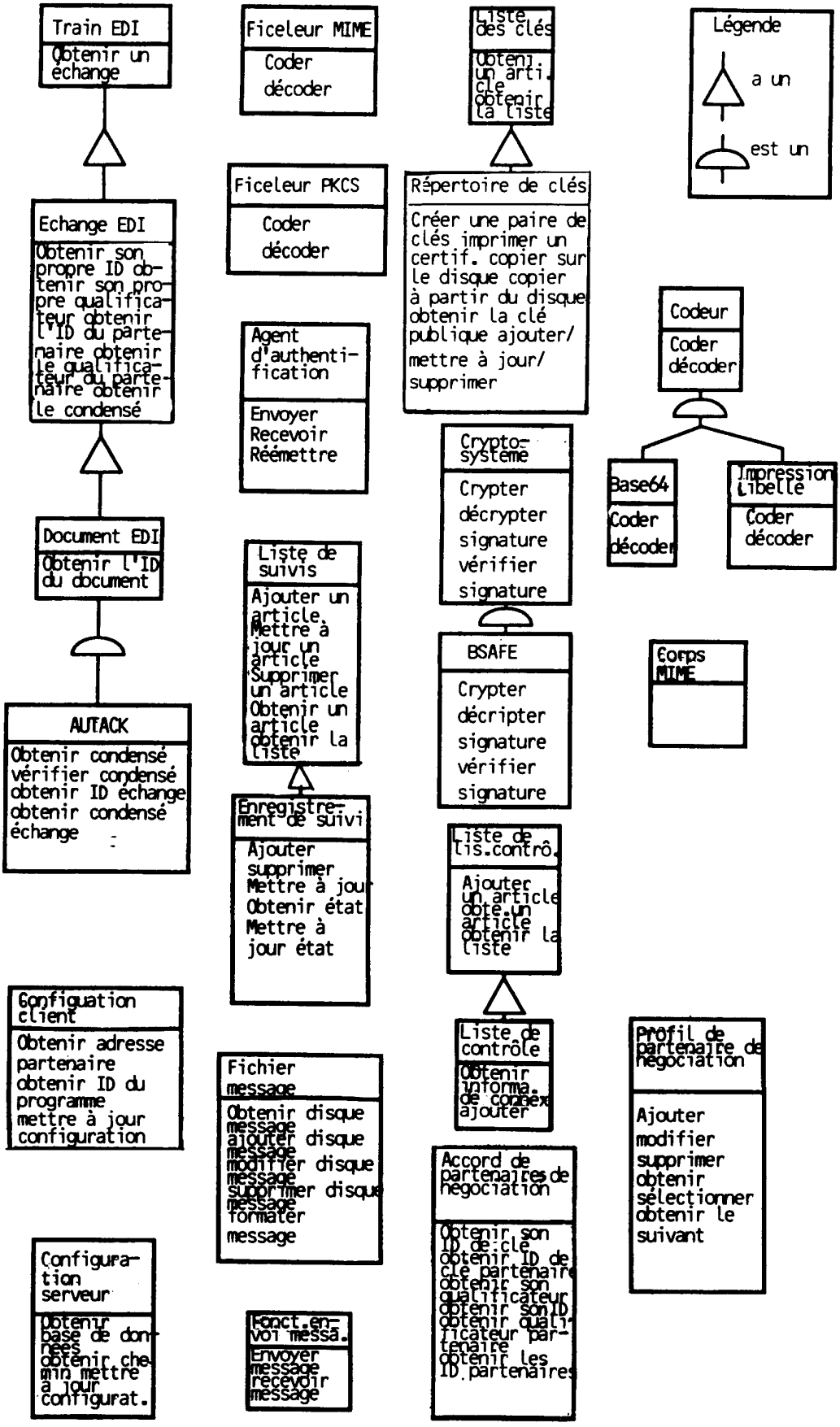

Train EDI
Obtenir un échange
Echange EDI
Obtenir son propre ID obtenir son propre qualificateur obtenir l'ID du partenaire obtenir le qualificateur du partenaire obtenir le condensé
Document EDI
Obtenir l'ID du document
AUTACK
Obtenir condensé vérifier condensé obtenir ID échange obtenir condensé échange
Configuation client
Obtenir adresse partenaire obtenir ID du programme mettre à jour configuration
Configuration serveur
Obtenir base de données obtenir chemin mettre à jour configurat.
Ficeleur MIME
Coder décoder
Ficeleur PKCS
Coder décoder
Agent d'authentification
Envoyer Recevoir Réémettre
Liste de suivis
Ajouter un article Mettre à jour un article Supprimer un article Obtenir un article obtenir la liste
Enregistrement de suivi
Ajouter supprimer Mettre à jou Obtenir état Mettre à jour état
Fichier message
Obtenir disque message ajouter disque message modifier disque message supprimer disque message formater message
Fonct.envoi messa.
Envoyer message recevoir message
Liste des clés
Obten. un arti. cle obtenir la liste
Répertoire de clés
Créer une paire de clés imprimer un certif. copier sur le disque copier à partir du disque obtenir la clé publique ajouter/ mettre à jour/ supprimer
Crypto-système
Crypter décrypter signature vérifier signature
BSAFE
Crypter décripter signature vérifier signature
Liste de lis.contrô.
Ajouter un article obté.un article obtenir la liste
Liste de contrôle
Obtenir informa. de connex ajouter
Accord de partenaires de négociation
Obtenir son ID de clé obtenir ID de clé partenaire obtenir son qualificateur obtenir son ID obtenir qualificateur partenaire obtenir les ID partenaires
Légende
a un
est un
Codeur
Coder décoder
Base64
Coder décoder
Impression libelle
Coder décoder
Corps MIME
Profil de partenaire de négociation
Ajouter modifier supprimer obtenir sélectionner obtenir le suivant

FIG.10

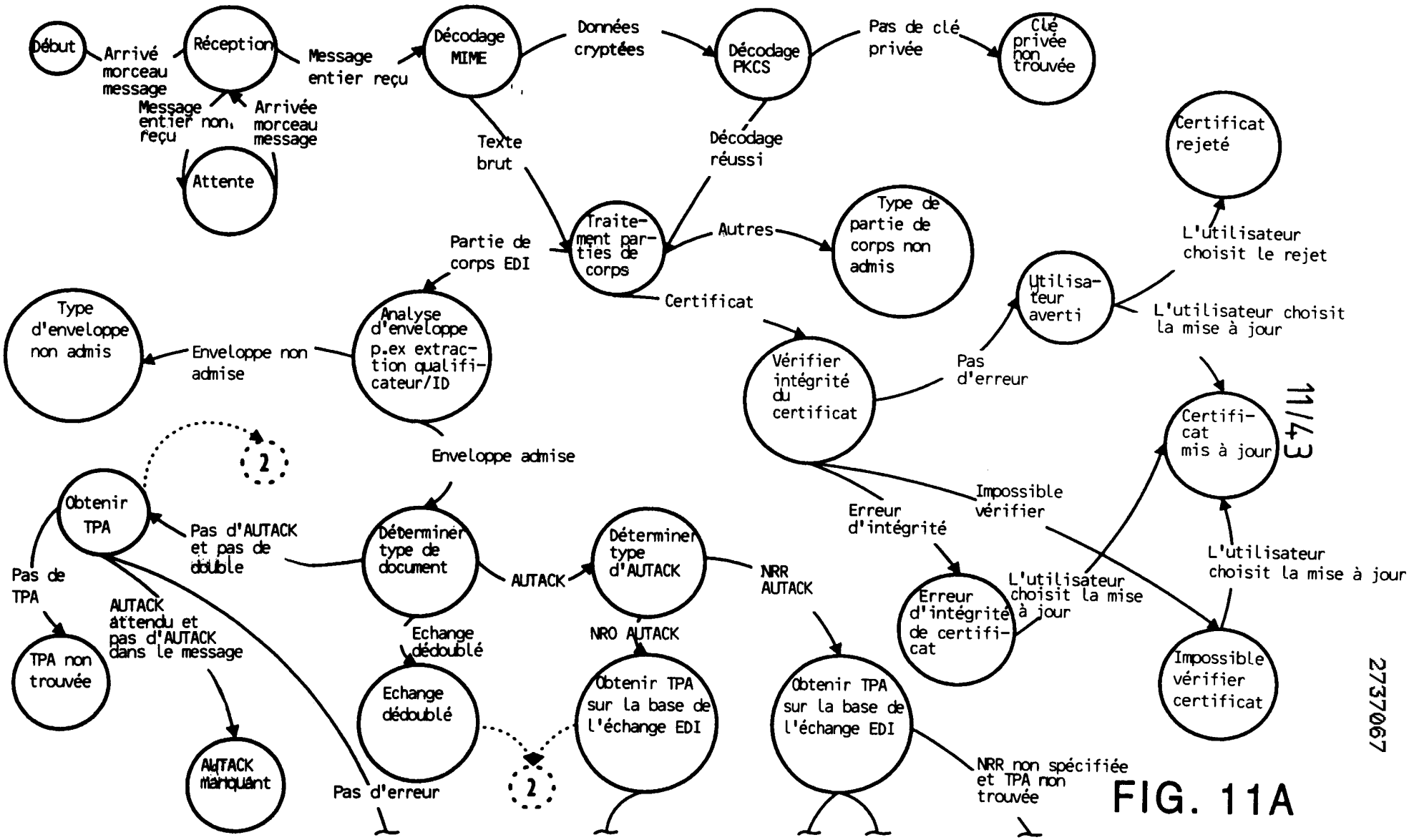

Début
Arrivé morceau message
Réception
Message entier reçu
Décodage MIME
Données cryptées
Décodage PKCS
Pas de clé privée
Clé privée non trouvée
Message entier non reçu
Arrivée morceau message
Attente
Texte brut
Décodage réussi
Traitement parties de corps
Autres
Type de partie de corps non admis
Partie de corps EDI
Certificat
Certificat rejeté
L'utilisateur choisit le rejet
Utilisateur averti
L'utilisateur choisit la mise à jour
Type d'enveloppe non admis
Enveloppe non admise
Analyse d'enveloppe p.ex extraction qualificateur/ID
Vérifier intégrité du certificat
Pas d'erreur
Certificat mis à jour
Enveloppe admise
Impossible vérifier
Erreur d'intégrité
Obtenir TPA
Pas d'AUTACK et pas de double
Déterminer type de document
AUTACK
Déterminer type d'AUTACK
NRR AUTACK
Erreur d'intégrité de certificat
L'utilisateur choisit la mise à jour
L'utilisateur choisit la mise à jour
Pas de TPA
TPA non trouvée
AUTACK attendu et pas d'AUTACK dans le message
Echange dédoublé
NRO AUTACK
Impossible vérifier certificat
AUTACK manquant
Echange dédoublé
Obtenir TPA sur la base de l'échange EDI
Obtenir TPA sur la base de l'échange EDI
Pas d'erreur
NRR non spécifiée et TPA non trouvée
2
2
11/43
2737067

FIG. 11A

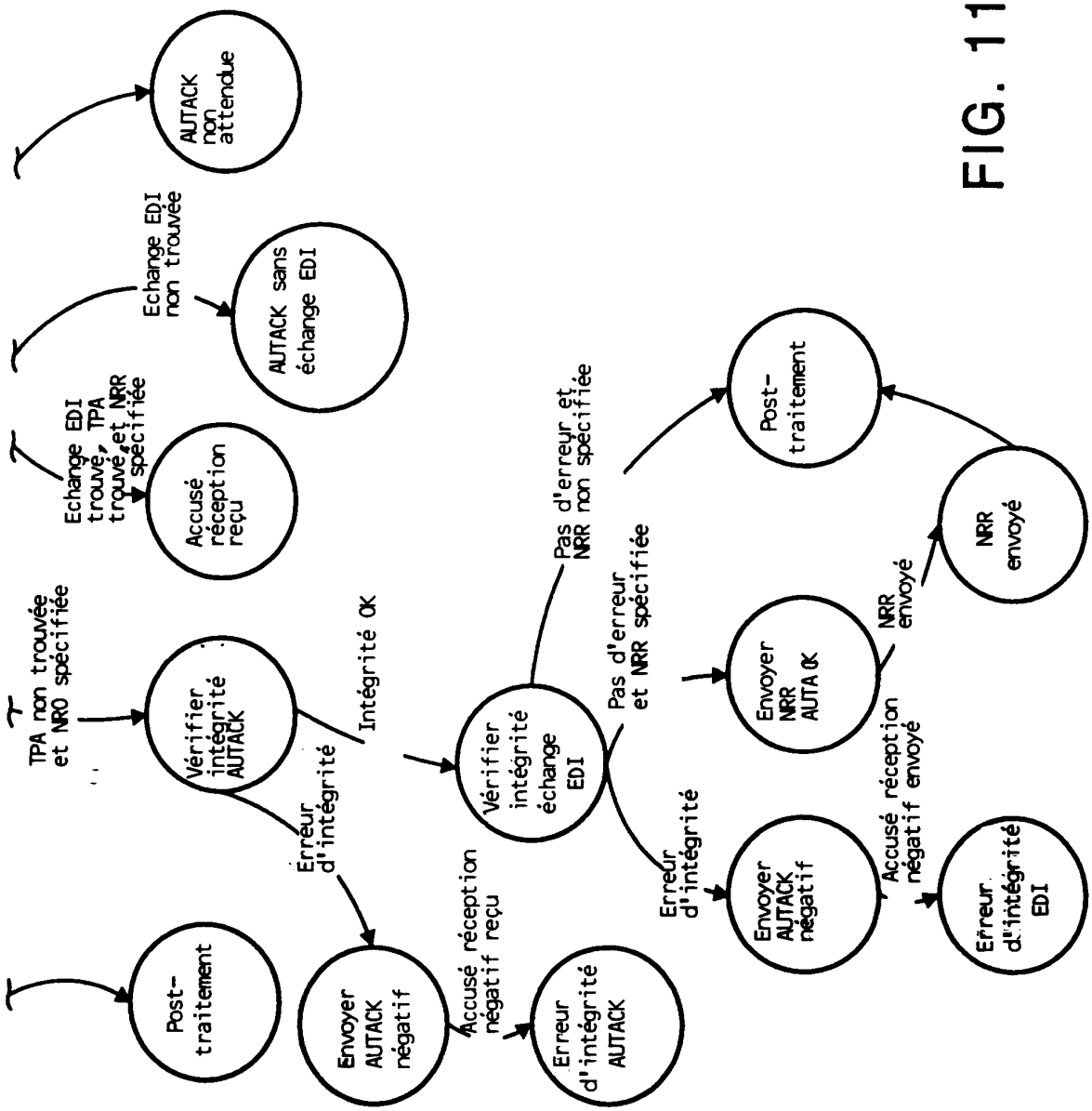

AUTACK non attendue
Echange EDI non trouvée
AUTACK sans échange EDI
Echange EDI trouvé, TPA trouvé, et NRR spécifiée
Accusé réception reçu
TPA non trouvée et NRO spécifiée
Vérifier intégrité AUTACK
Intégrité OK
Erreur d'intégrité
Post-traitement
Envoyer AUTACK négatif
Accusé réception négatif reçu
Erreur d'intégrité AUTACK
Vérifier intégrité échange EDI
Pas d'erreur et NRR non spécifiée
Pas d'erreur et NRR spécifiée
Erreur d'intégrité
Post-traitement
Envoyer NRR AUTACK
NRR envoyé
NRR envoyé
Envoyer AUTACK négatif
Accusé réception négatif envoyé
Erreur d'intégrité EDI

FIG. 11B

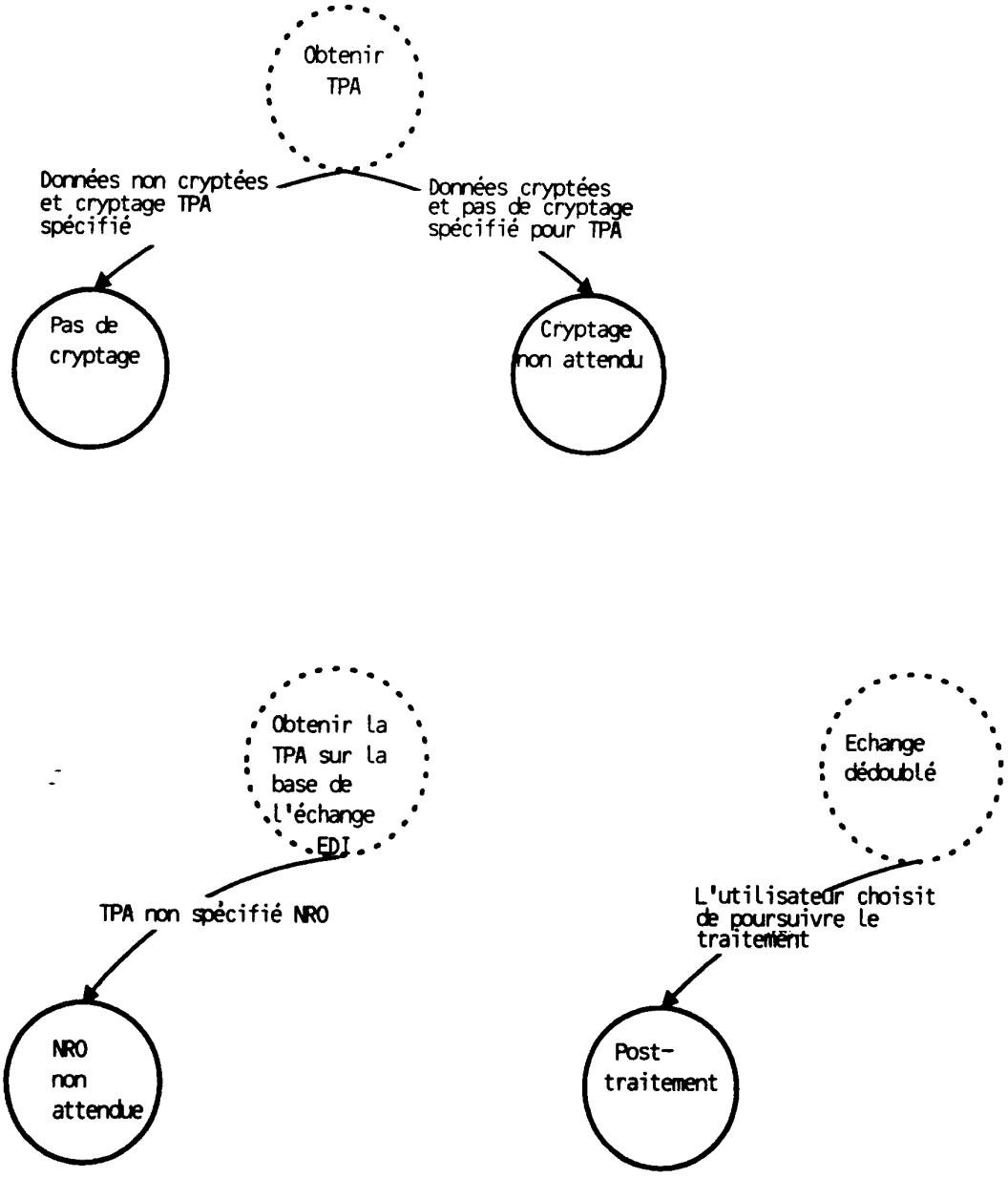

Obtenir TPA
Données non cryptées et cryptage TPA spécifié
Données cryptées et pas de cryptage spécifié pour TPA
Pas de cryptage
Cryptage non attendu
Obtenir la TPA sur la base de l'échange EDI
TPA non spécifié NRO
NRO non attendue
Echange dédoublé
L'utilisateur choisit de poursuivre le traitement
Post-traitement

FIG. 12

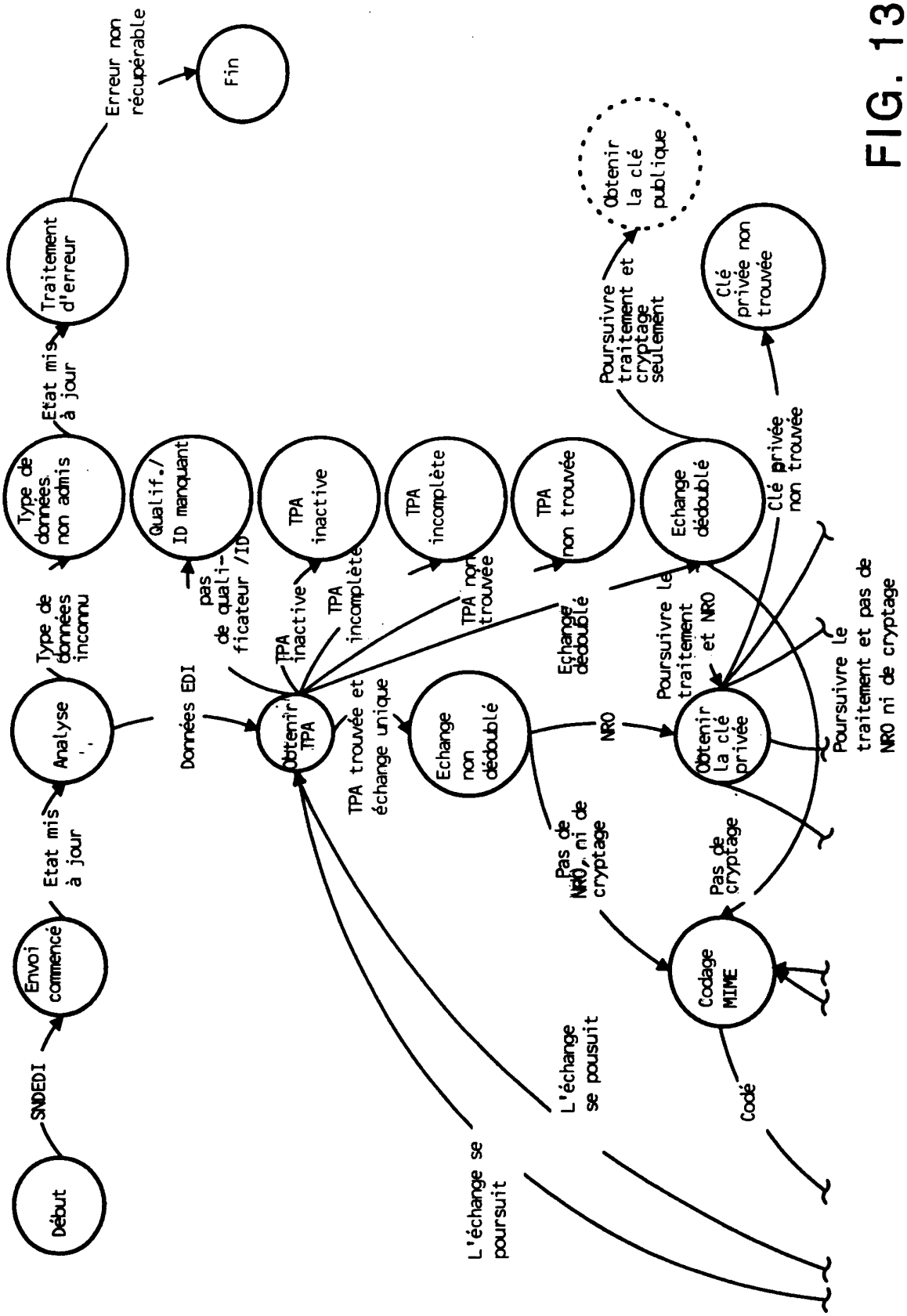

Début
SNDEDI
Envoi commencé
Etat mis à jour
Analyse
Type de données inconnu
Etat mis à jour
Type de données non admis
Traitement d'erreur
Erreur non récupérable
Fin
Données EDI
Obtenir TPA
Qualif./ ID manquant
pas de qualificateur /ID
TPA inactive
TPA incomplète
TPA non trouvée
TPA trouvée et échange unique
Echange non dédoublé
Echange dédoublé
TPA inactive
TPA incomplète
TPA non trouvée
Echange dédoublé
Poursuivre le traitement et NRO
Poursuivre traitement et cryptage seulement
Obtenir la clé publique
Clé privée non trouvée
Clé privée non trouvée
NRO
Obtenir la clé privée
Poursuivre le traitement et pas de NRO ni de cryptage
Pas de NRO, ni de cryptage
Pas de cryptage
Codage MIME
Codé
L'échange se pousuit
L'échange se poursuit

FIG. 13A

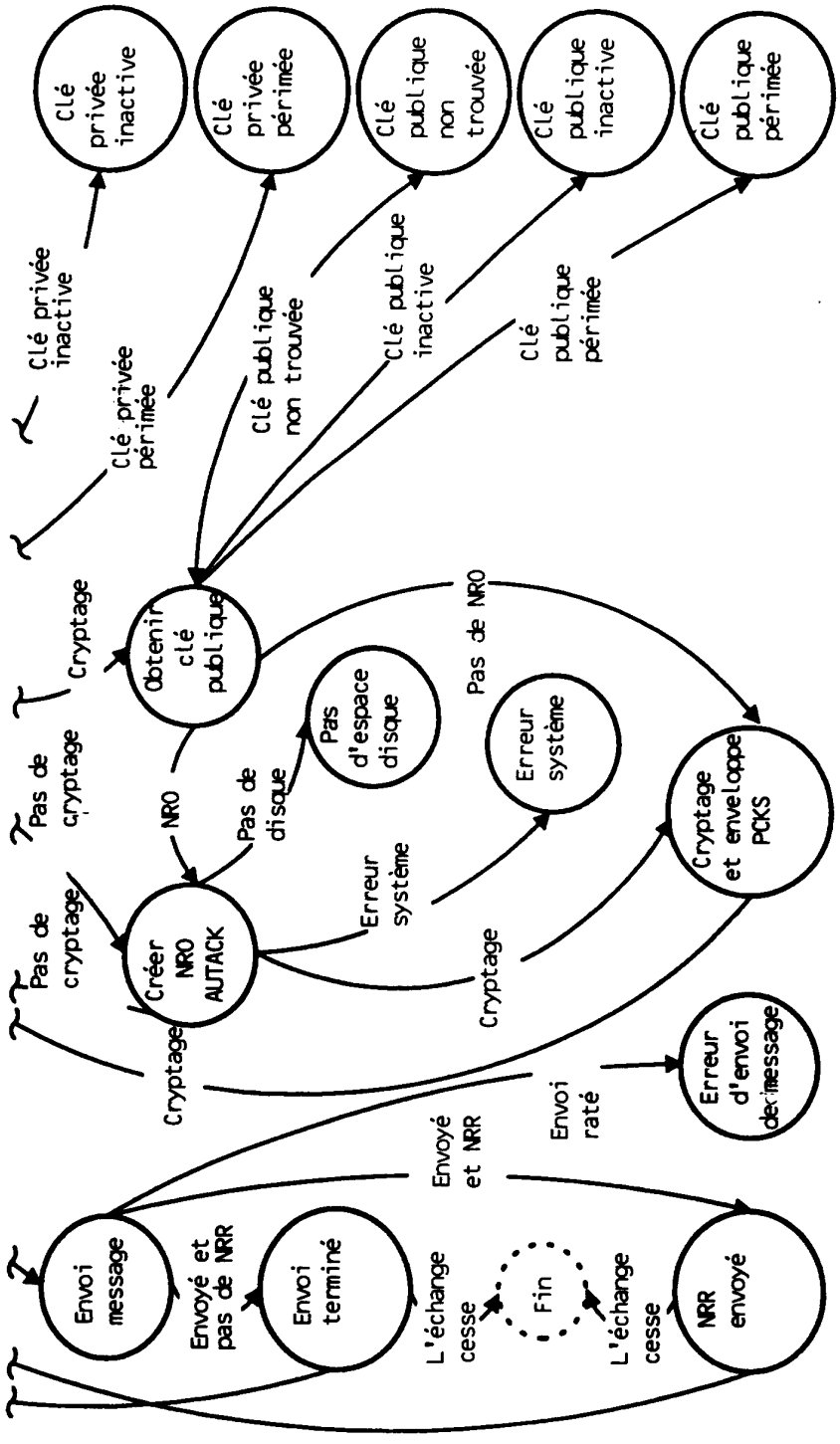

Clé privée inactive
Clé privée périmée
Clé publique non trouvée
Clé publique inactive
Clé publique périmée
Cryptage
Obtenir clé publique
Pas de cryptage
Pas de disque
Pas d'espace disque
Erreur système
Pas de NRO
Créer NRO AUTACK
Cryptage et enveloppe PCKS
Envoi message
Envoyé et pas de NRR
Envoi terminé
L'échange cesse
Fin
Envoyé et NRR
Envoi raté
Erreur d'envoi de message
NRR envoyé

FIG. 13B

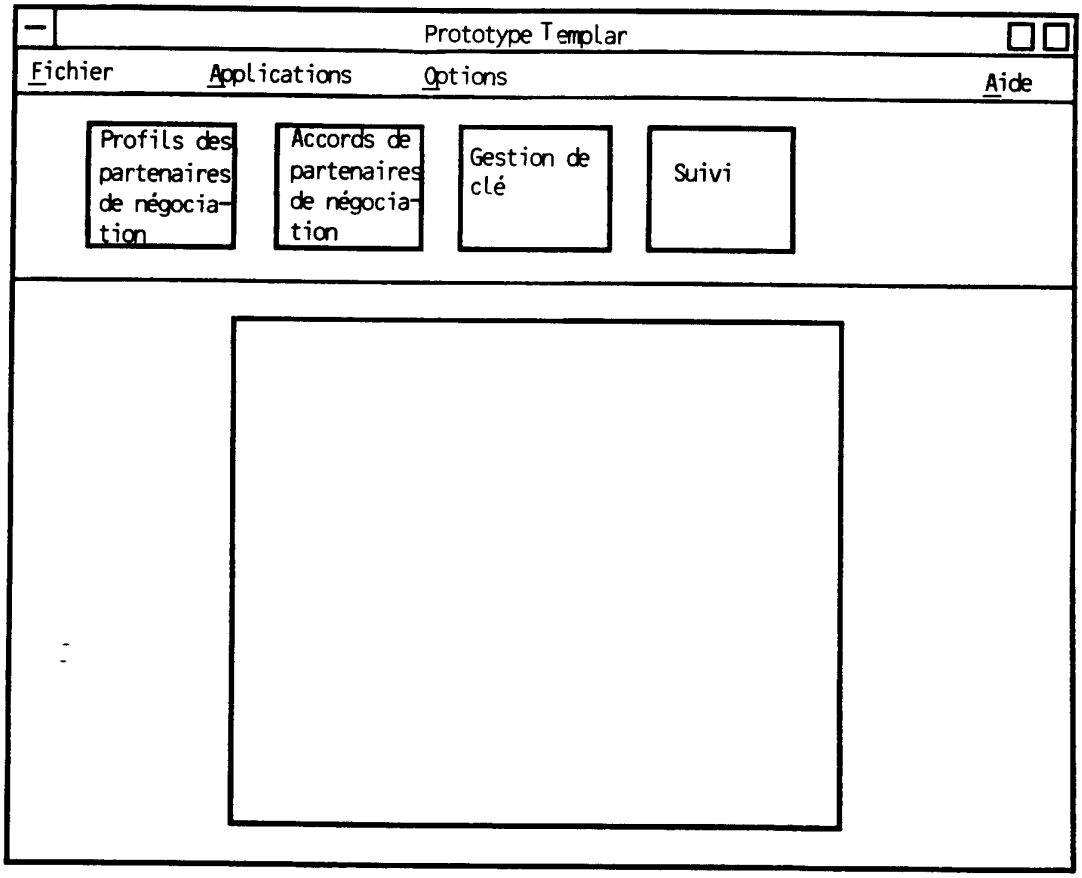

Prototype Templar
Fichier
Applications
Options
Aide
Profils des partenaires de négociation
Accords de partenaires de négociation
Gestion de clé
Suivi

FIG. 14

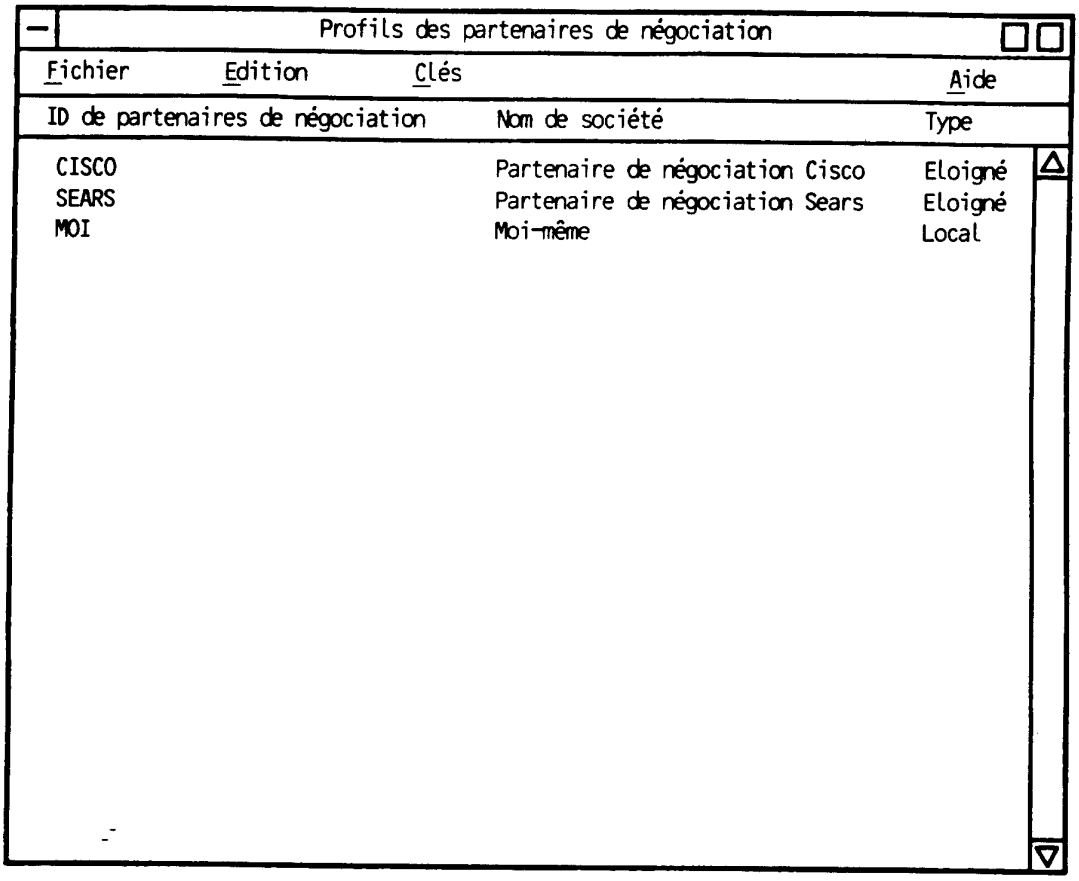

Profils des partenaires de négociation
Fichier
Edition
Clés
Aide
ID de partenaires de négociation
Nom de société
Type
CISCO
Partenaire de négociation Cisco
Eloigné
SEARS
Partenaire de négociation Sears
Eloigné
MOI
Moi-même
Local

FIG. 15

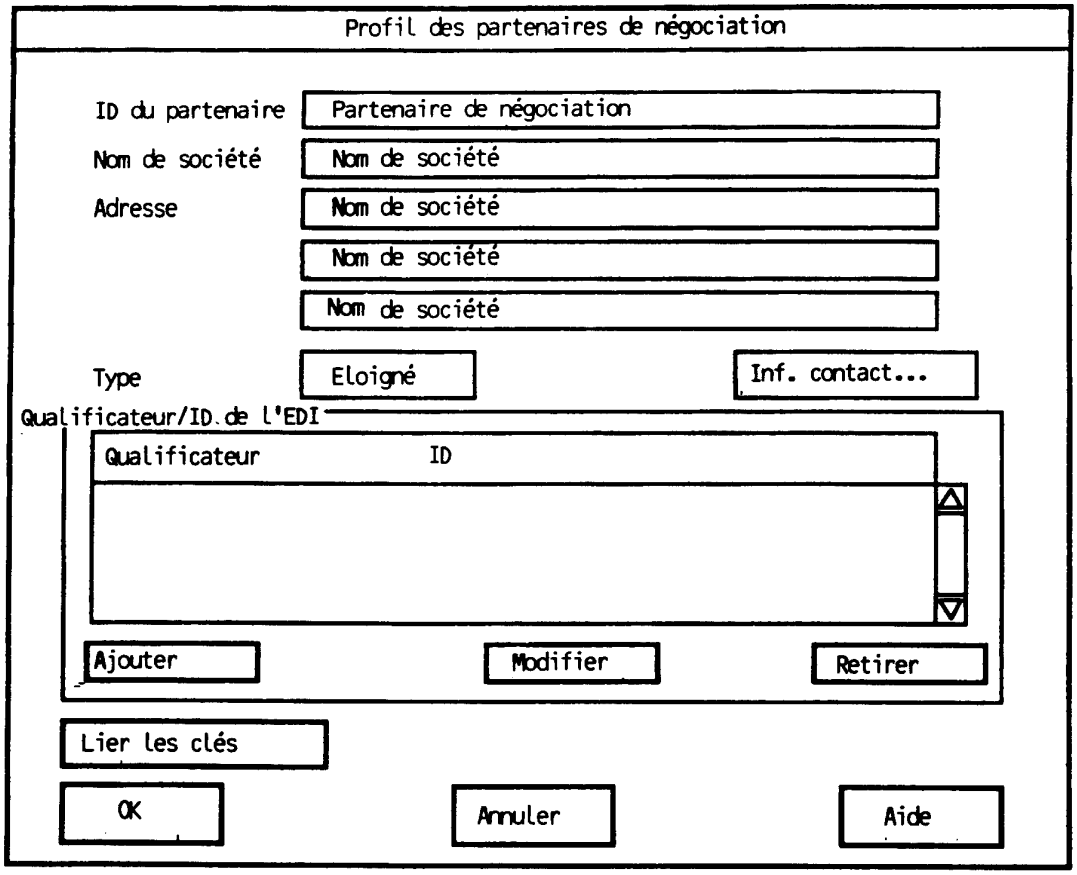

Profil des partenaires de négociation
ID du partenaire
Partenaire de négociation
Nom de société
Nom de société
Adresse
Nom de société
Nom de société
Nom de société
Type
Eloigné
Inf. contact...
Qualificateur/ID de l'EDI
Qualificateur
ID
Ajouter
Modifier
Retirer
Lier les clés
OK
Annuler
Aide

FIG. 16

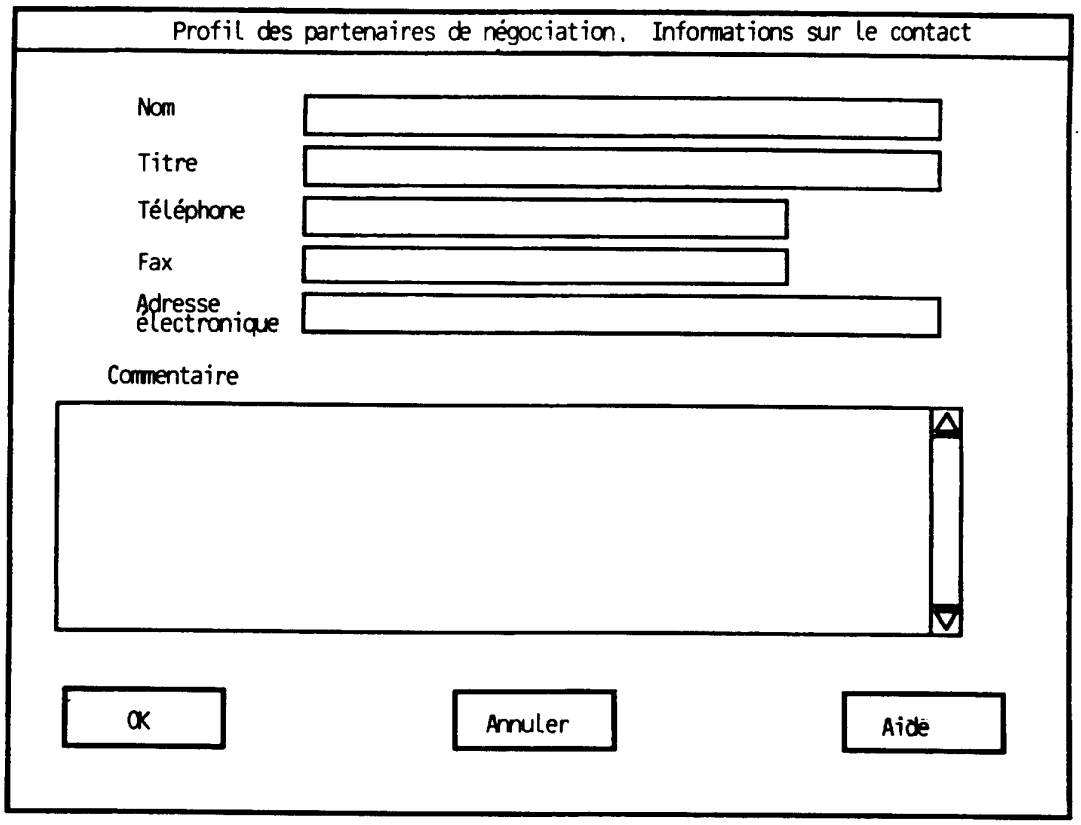

Profil des partenaires de négociation. Informations sur le contact
Nom
Titre
Téléphone
Fax
Adresse électronique
Commentaire
OK
Annuler
Aide

FIG. 17

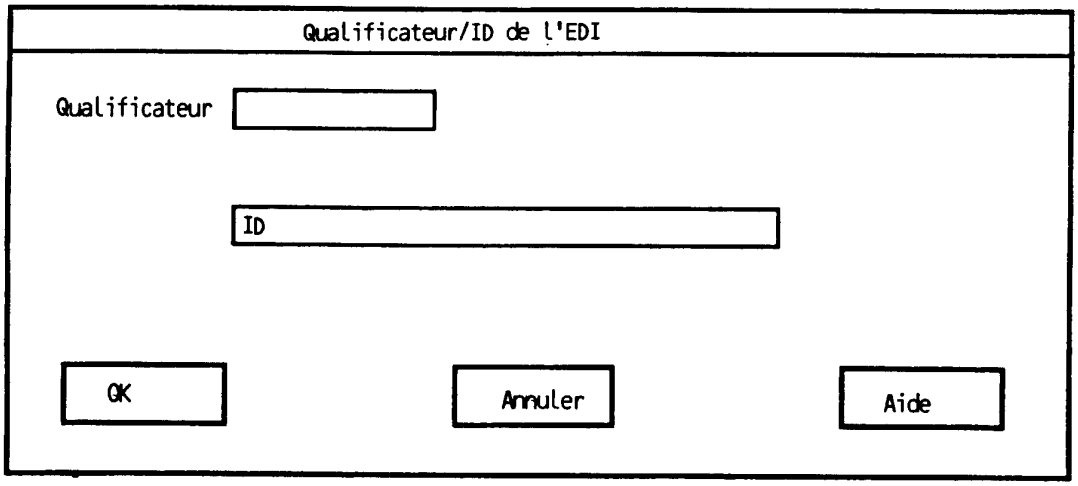


FIG. 18

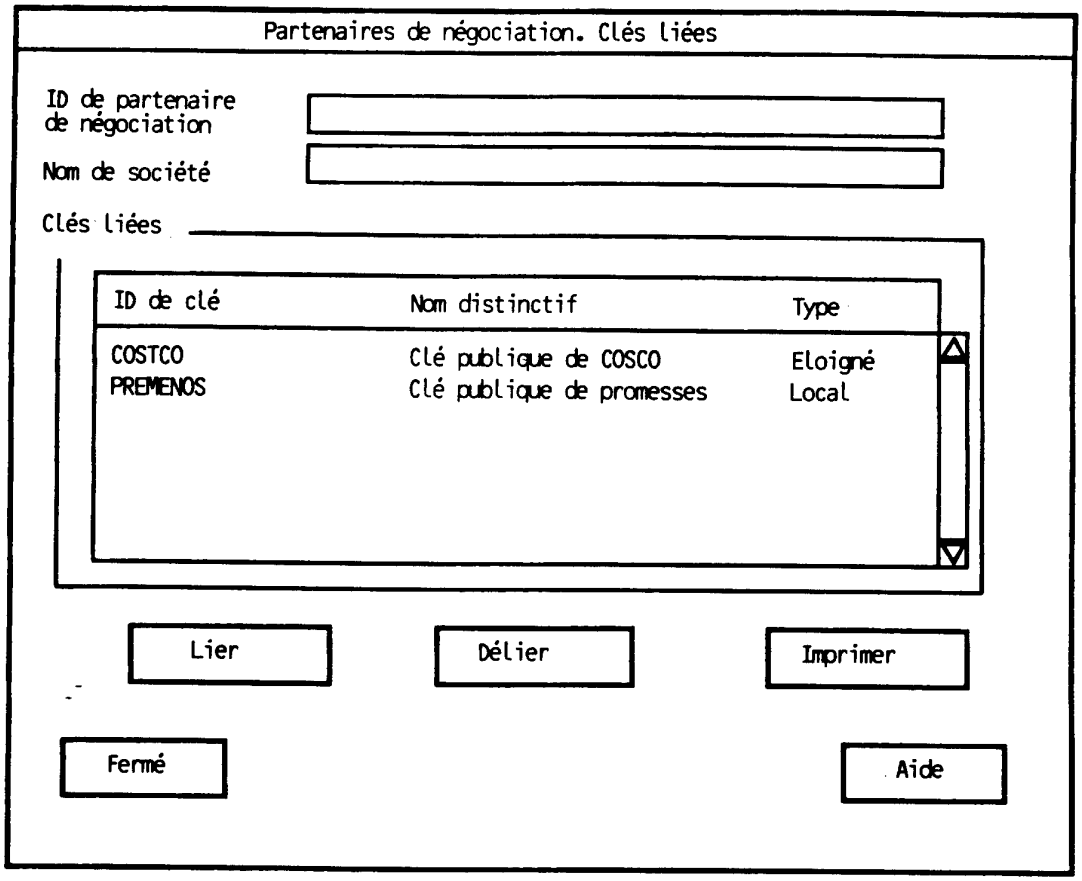

Partenaires de négociation. Clés liées
ID de partenaire de négociation
Nom de société
Clés liées
ID de clé
Nom distinctif
Type
COSTCO
Clé publique de COSCO
Eloigné
PREMENOS
Clé publique de promesses
Local
Lier
Délier
Imprimer
Fermé
Aide

FIG. 19

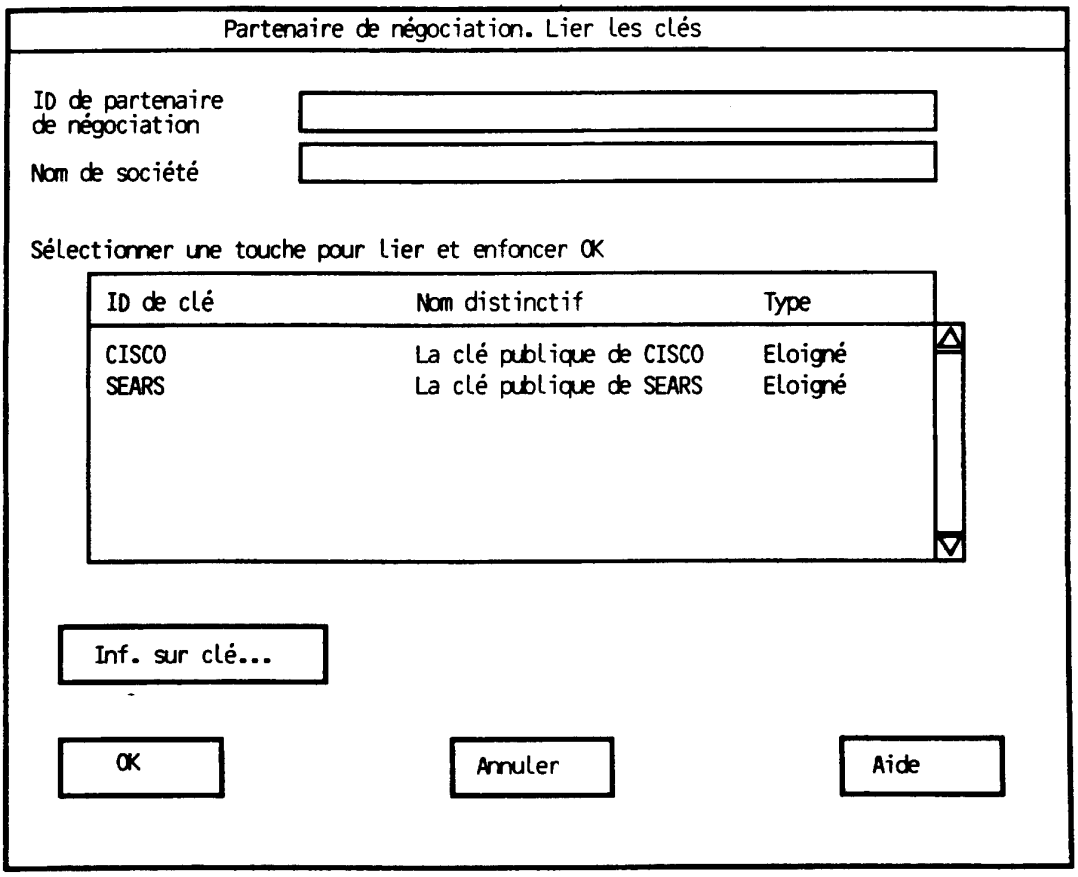

Partenaire de négociation. Lier les clés
ID de partenaire de négociation
Nom de société
Sélectionner une touche pour lier et enfoncer OK
ID de clé
Nom distinctif
Type
CISCO
La clé publique de CISCO
Eloigné
SEARS
La clé publique de SEARS
Eloigné
Inf. sur clé...
OK
Annuler
Aide

FIG. 20

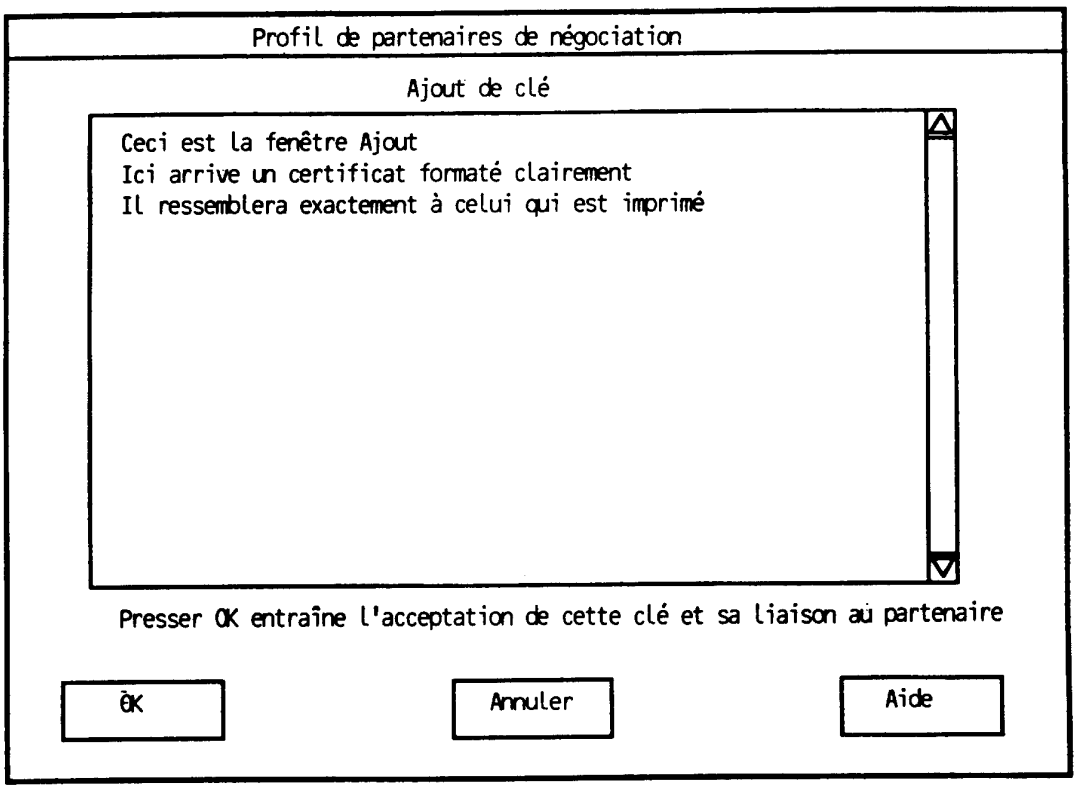

Profil de partenaires de négociation
Ajout de clé
Ceci est la fenêtre Ajout
Ici arrive un certificat formaté clairement
Il ressemblera exactement à celui qui est imprimé
Presser OK entraîne l'acceptation de cette clé et sa liaison au partenaire
OK
Annuler
Aide

FIG. 21

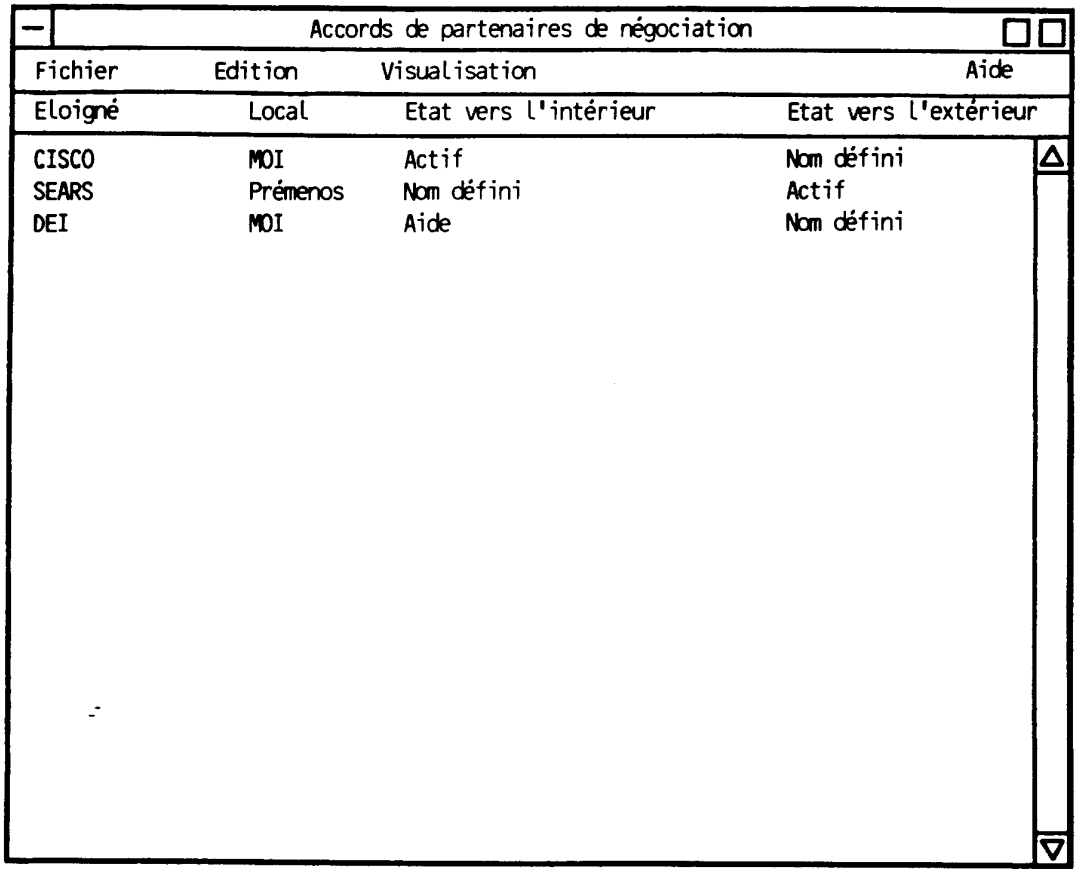

Accords de partenaires de négociation
Fichier
Edition
Visualisation
Aide
Eloigné
Local
Etat vers l'intérieur
Etat vers l'extérieur
CISCO
MOI
Actif
Nom défini
SEARS
Prémenos
Nom défini
Actif
DEI
MOI
Aide
Nom défini

FIG. 22

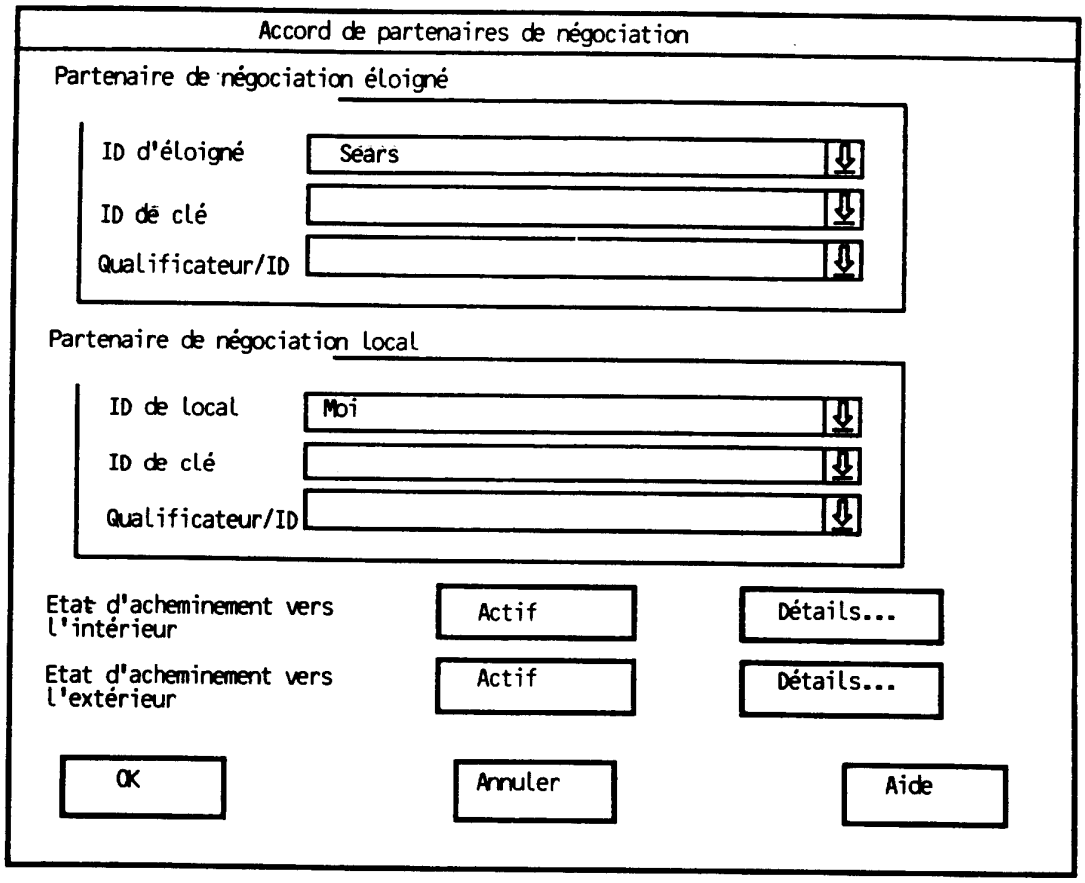

Accord de partenaires de négociation
Partenaire de négociation éloigné
ID d'éloigné
Sears
ID de clé
Qualificateur/ID
Partenaire de négociation local
ID de local
Moi
ID de clé
Qualificateur/ID
Etat d'acheminement vers l'intérieur
Actif
Détails...
Etat d'acheminement vers l'extérieur
Actif
Détails...
OK
Annuler
Aide

FIG. 23

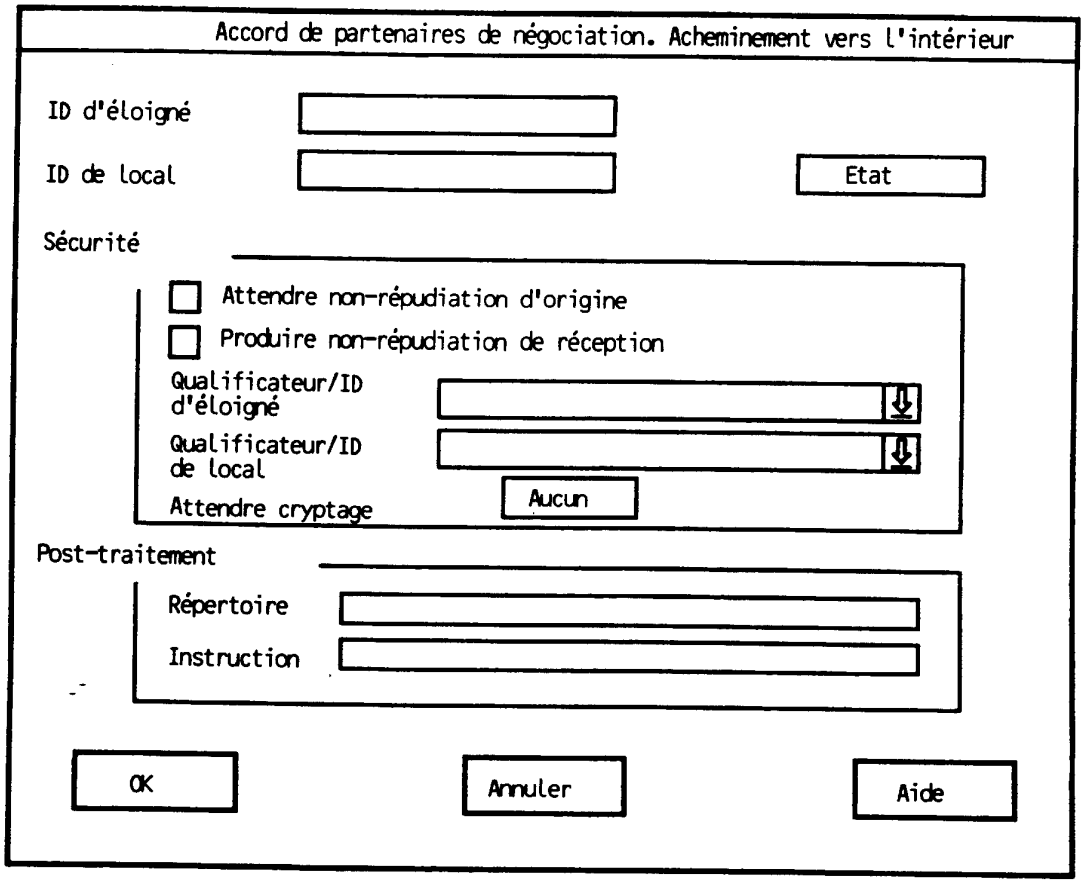

Accord de partenaires de négociation. Acheminement vers l'intérieur
ID d'éloigné
ID de local
Etat
Sécurité
Attendre non-répudiation d'origine
Produire non-répudiation de réception
Qualificateur/ID d'éloigné
Qualificateur/ID de local
Attendre cryptage
Aucun
Post-traitement
Répertoire
Instruction
OK
Annuler
Aide

FIG. 24

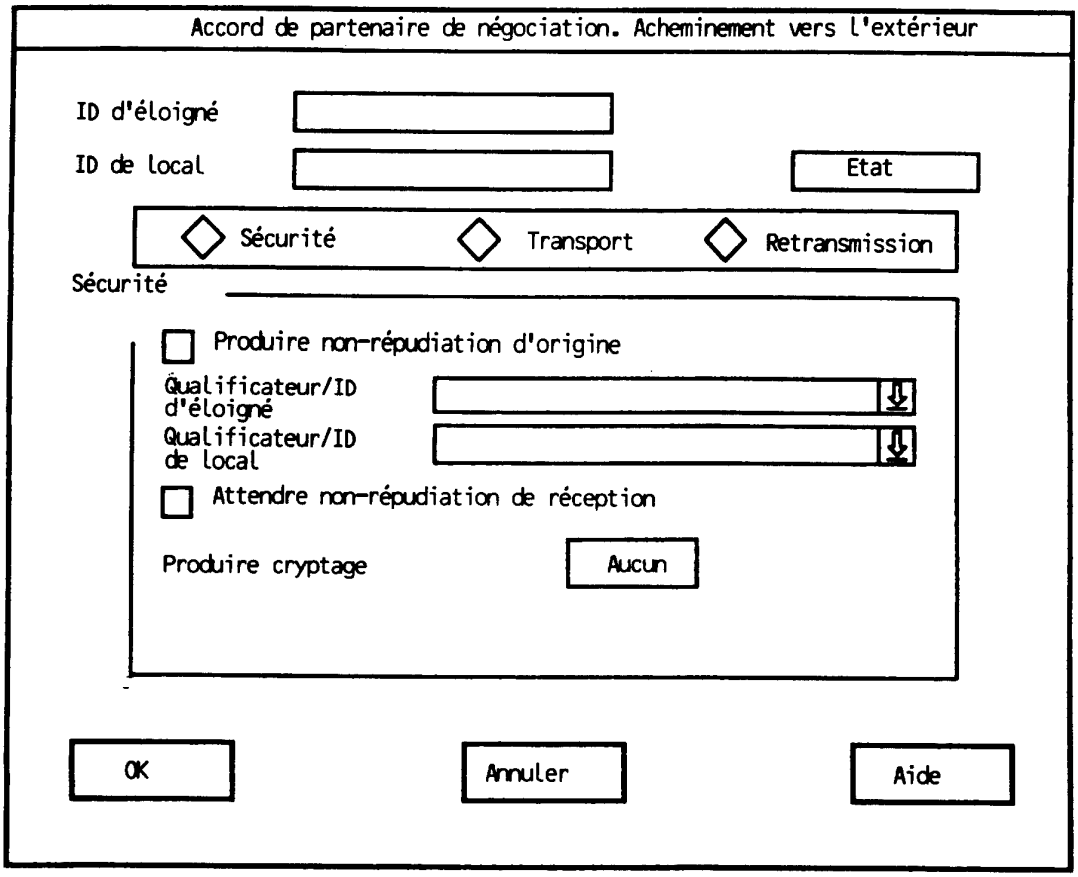

Accord de partenaire de négociation. Acheminement vers l'extérieur
ID d'éloigné
ID de local
Etat
Sécurité
Transport
Retransmission
Sécurité
Produire non-répudiation d'origine
Qualificateur/ID d'éloigné
Qualificateur/ID de local
Attendre non-répudiation de réception
Produire cryptage
Aucun
OK
Annuler
Aide

FIG. 25

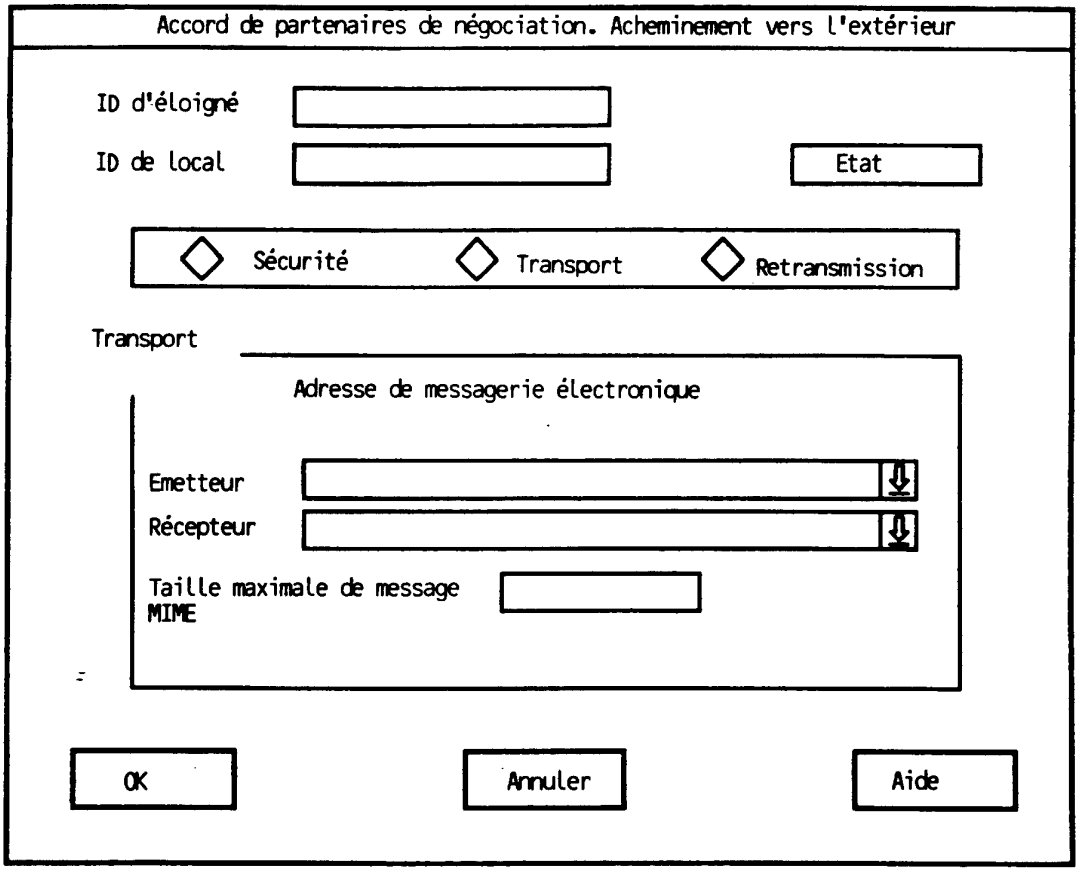

Accord de partenaires de négociation. Acheminement vers l'extérieur
ID d'éloigné
ID de local
Etat
Sécurité
Transport
Retransmission
Transport
Adresse de messagerie électronique
Emetteur
Récepteur
Taille maximale de message MIME
OK
Annuler
Aide

FIG. 26

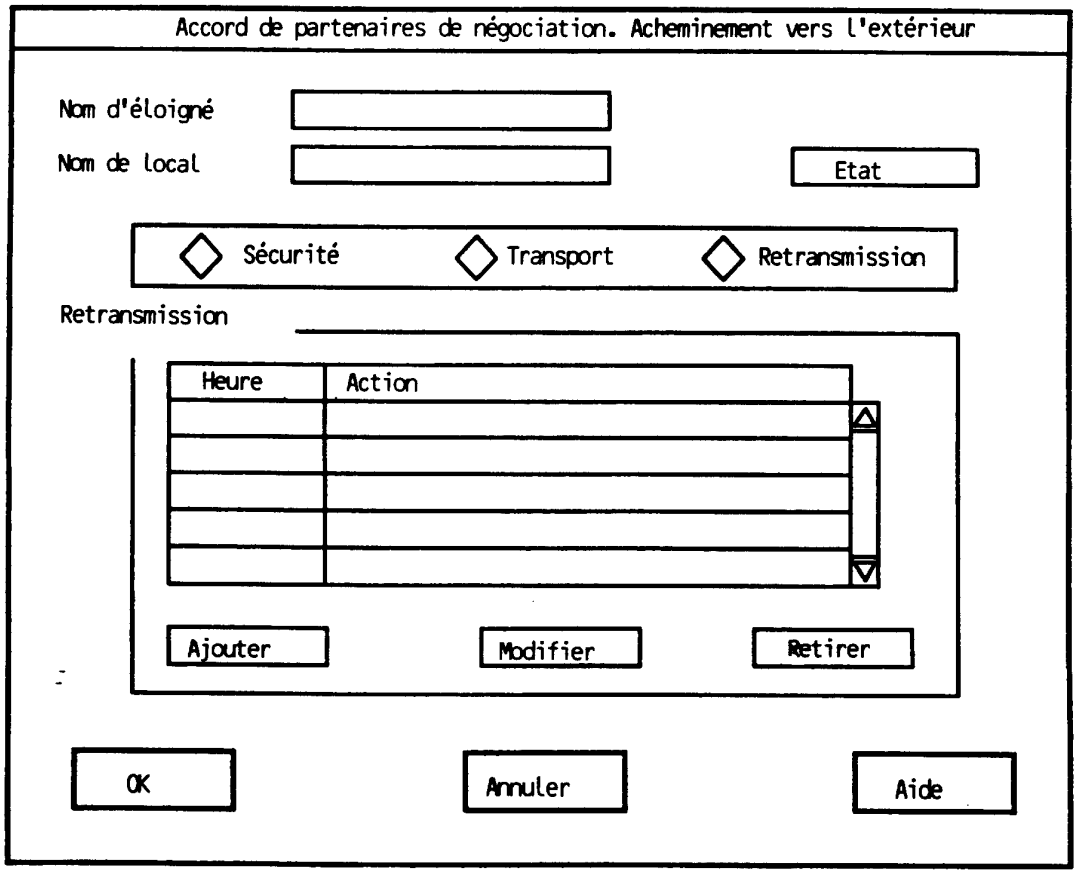

Accord de partenaires de négociation. Acheminement vers l'extérieur
Nom d'éloigné
Nom de local
Etat
Sécurité
Transport
Retransmission
Retransmission
Heure
Action
Ajouter
Modifier
Retirer
OK
Annuler
Aide

FIG. 27

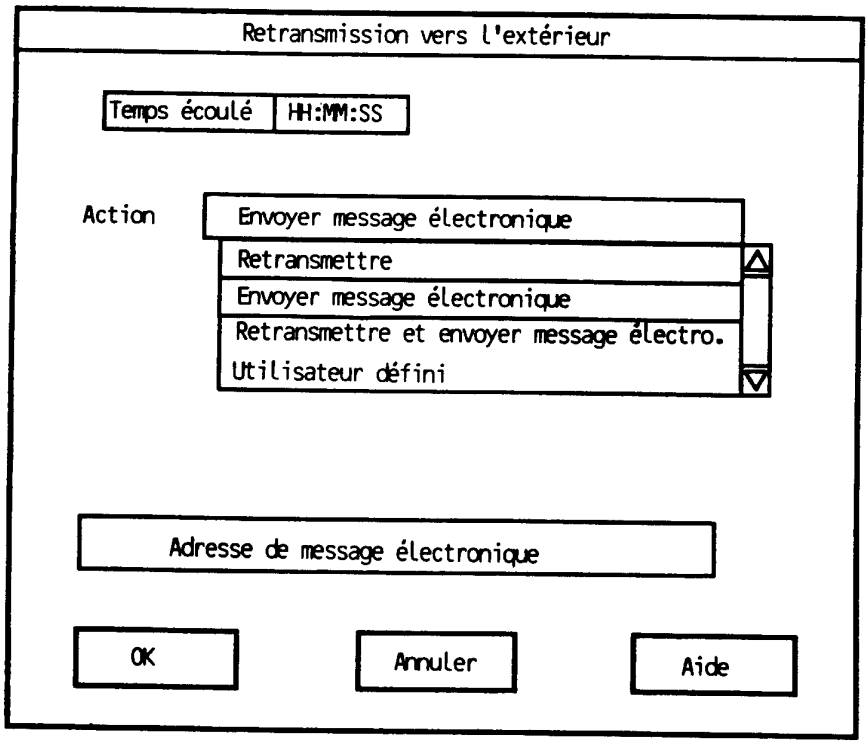

Retransmission vers l'extérieur
Temps écoulé
HH:MM:SS
Action
Envoyer message électronique
Retransmettre
Envoyer message électronique
Retransmettre et envoyer message électro.
Utilisateur défini
Adresse de message électronique
OK
Annuler
Aide

FIG. 28

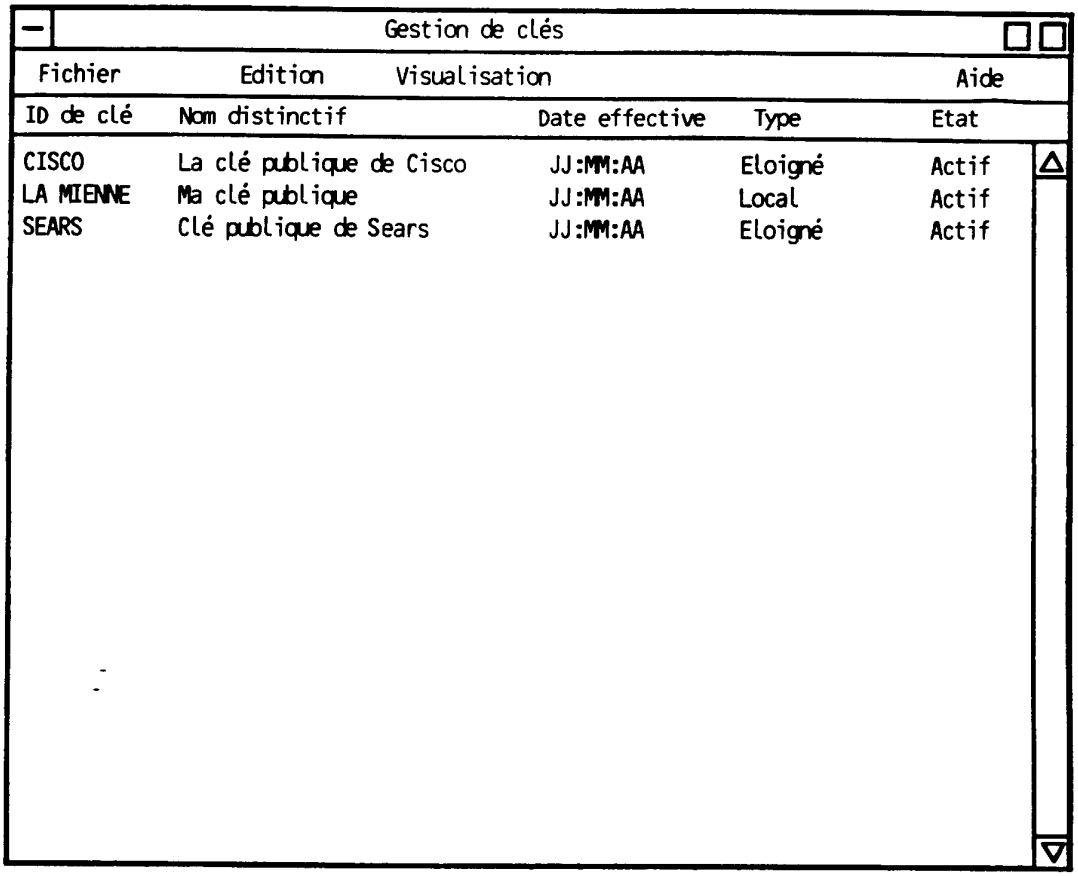

Gestion de clés
Fichier
Edition
Visualisation
Aide
ID de clé
Nom distinctif
Date effective
Type
Etat
CISCO
La clé publique de Cisco
JJ:MM:AA
Eloigné
Actif
LA MIENNE
Ma clé publique
JJ:MM:AA
Local
Actif
SEARS
Clé publique de Sears
JJ:MM:AA
Eloigné
Actif

FIG. 29

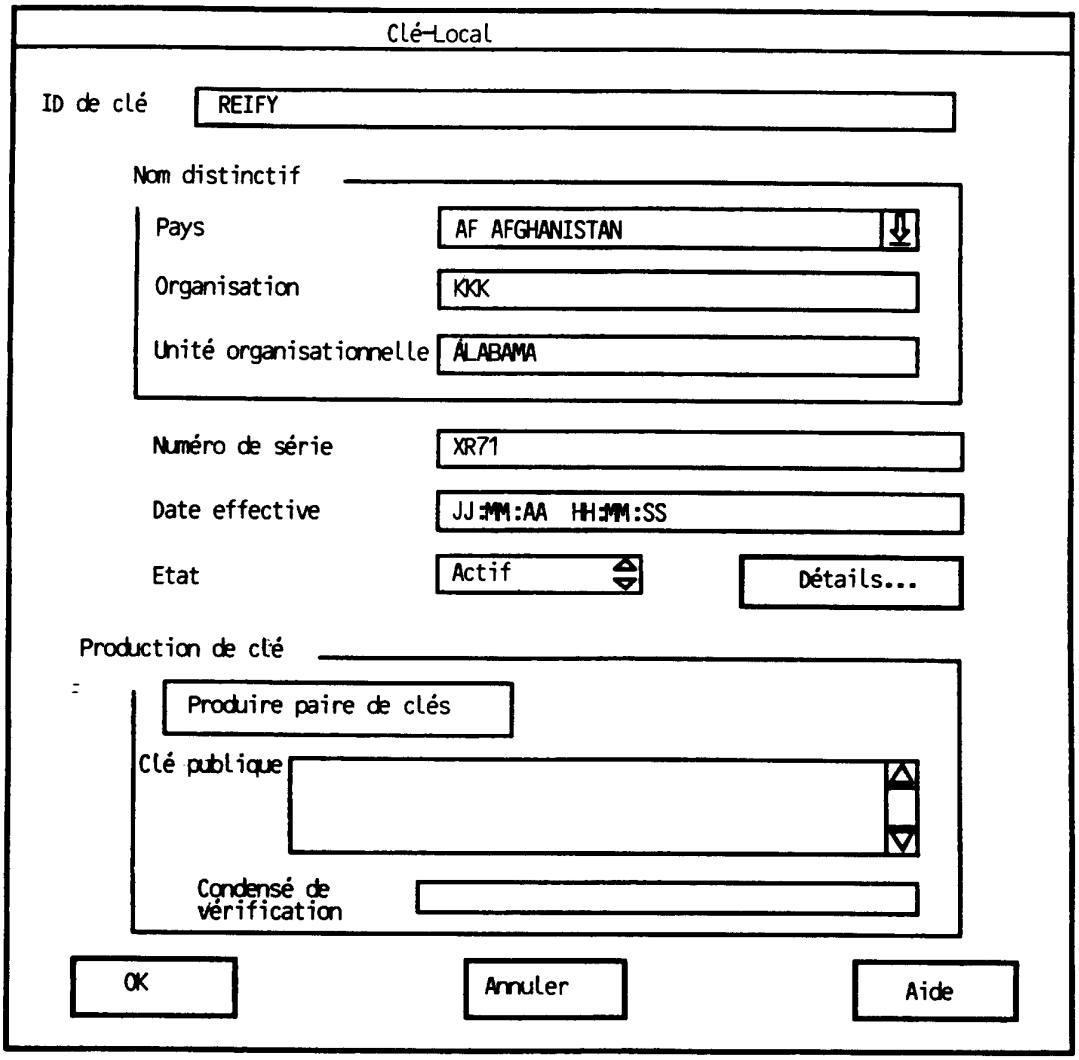

Clé-Local
ID de clé
REIFY
Nom distinctif
Pays
AF AFGHANISTAN
Organisation
KKK
Unité organisationnelle
ALABAMA
Numéro de série
XR71
Date effective
JJ:MM:AA HH:MM:SS
Etat
Actif
Détails...
Production de clé
Produire paire de clés
Clé publique
Condensé de vérification
OK
Annuler
Aide

FIG. 30

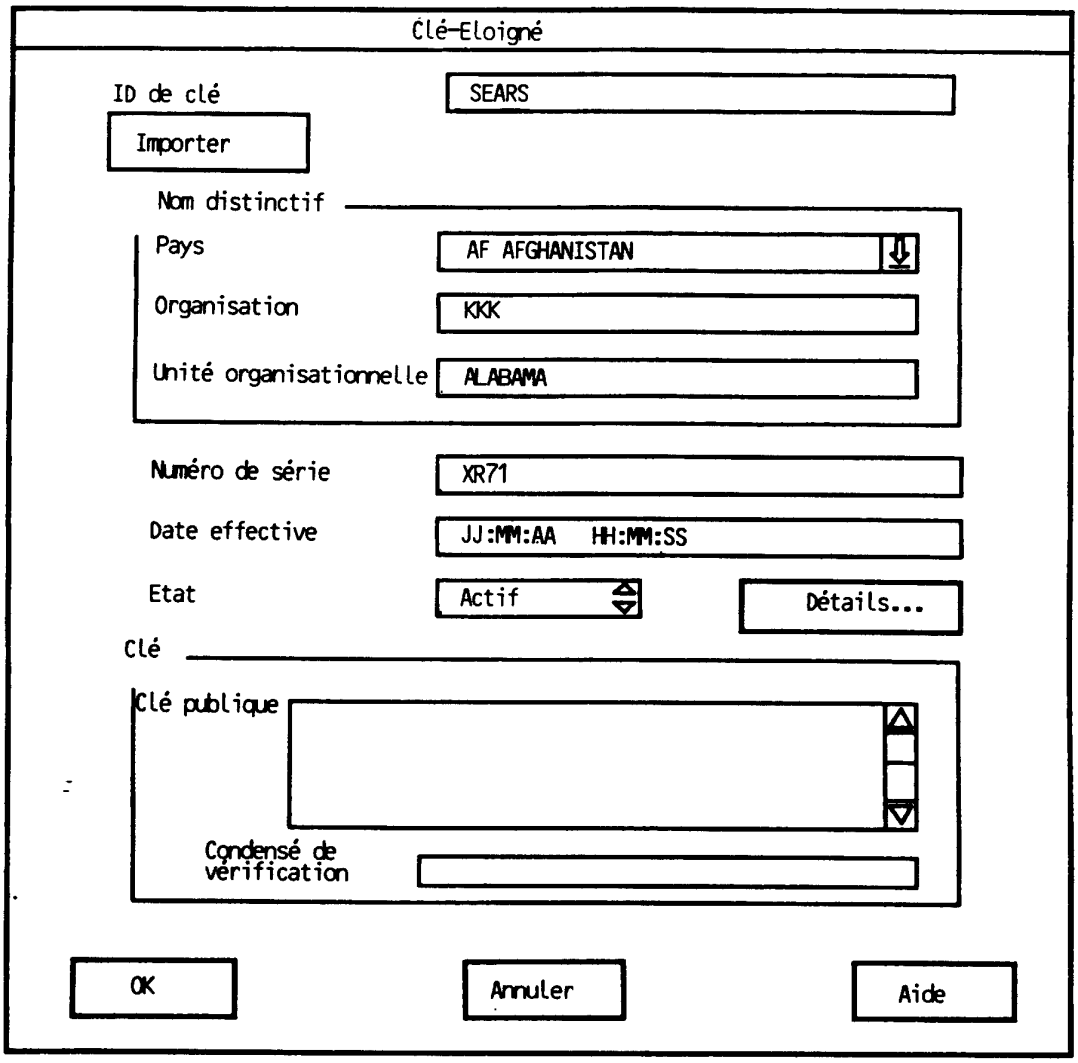

Clé-Eloigné
ID de clé
SEARS
Importer
Nom distinctif
Pays
AF AFGHANISTAN
Organisation
KKK
Unité organisationnelle
ALABAMA
Numéro de série
XR71
Date effective
JJ:MM:AA HH:MM:SS
Etat
Actif
Détails...
Clé
Clé publique
Condensé de vérification
OK
Annuler
Aide

FIG. 31

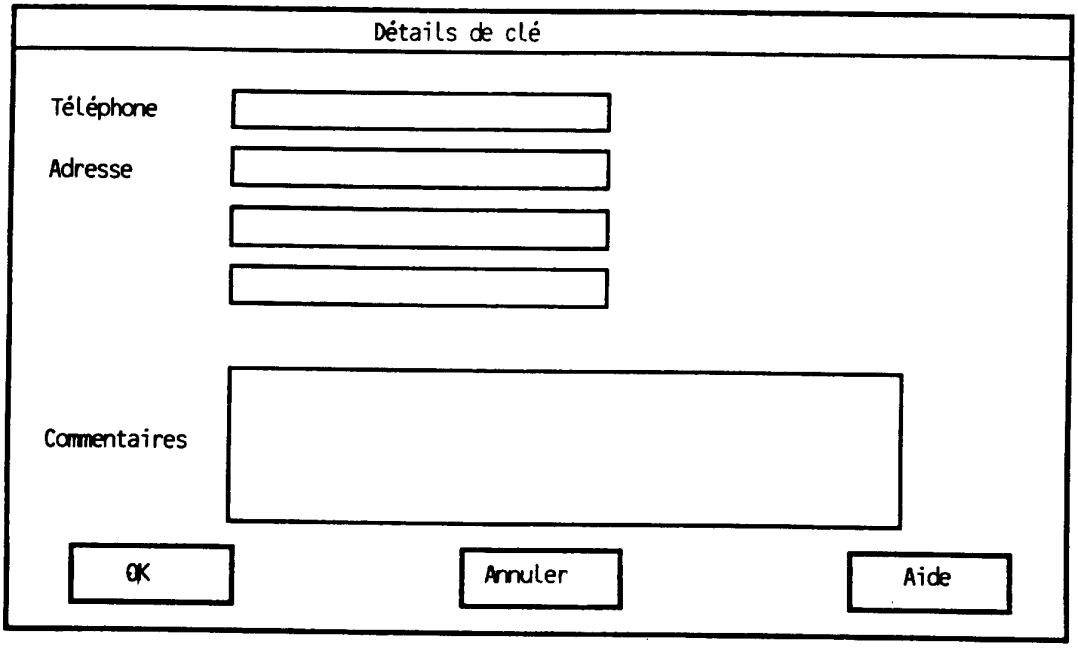

Détails de clé
Téléphone
Adresse
Commentaires
OK
Annuler
Aide

FIG. 32

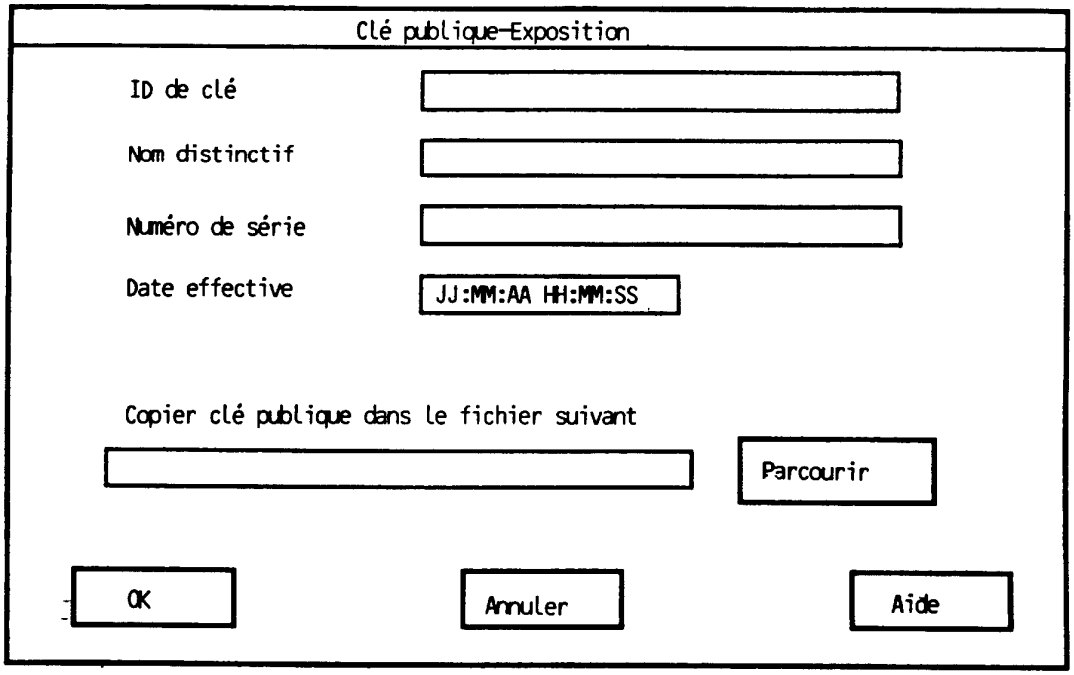

Clé publique-Exposition
ID de clé
Nom distinctif
Numéro de série
Date effective
JJ:MM:AA HH:MM:SS
Copier clé publique dans le fichier suivant
Parcourir
OK
Annuler
Aide

FIG. 33

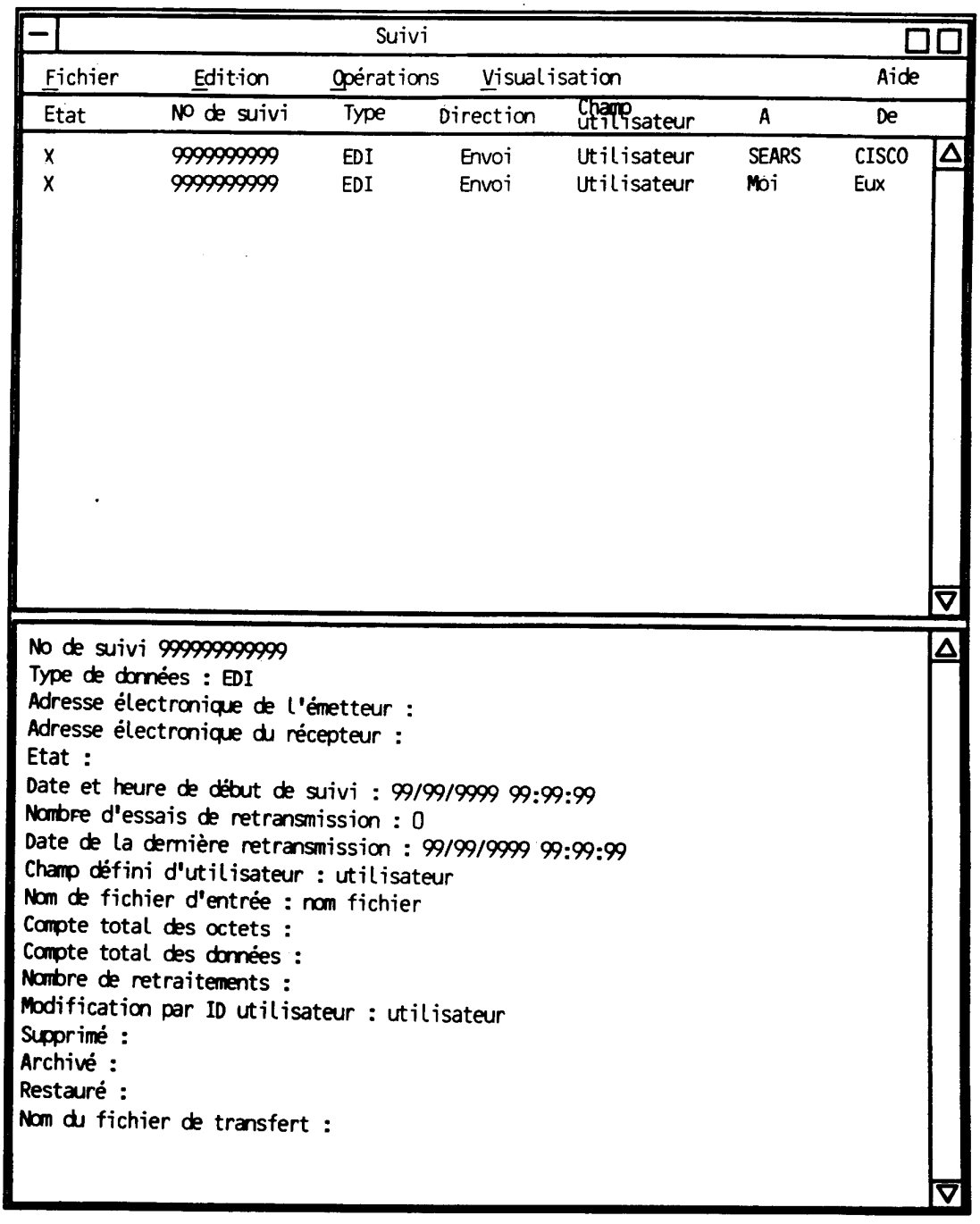

Suivi
Fichier
Edition
Opérations
Visualisation
Aide
Etat
NO de suivi
Type
Direction
Champ utilisateur
A
De
X 9999999999 EDI Envoi Utilisateur SEARS CISCO
X 9999999999 EDI Envoi Utilisateur Moi Eux
No de suivi 999999999999
Type de données : EDI
Adresse électronique de l'émetteur :
Adresse électronique du récepteur :
Etat :
Date et heure de début de suivi : 99/99/9999 99:99:99
Nombre d'essais de retransmission : 0
Date de la dernière retransmission : 99/99/9999 99:99:99
Champ défini d'utilisateur : utilisateur
Nom de fichier d'entrée : nom fichier
Compte total des octets :
Compte total des données :
Nombre de retraitements :
Modification par ID utilisateur : utilisateur
Supprimé :
Archivé :
Restauré :
Nom du fichier de transfert :

FIG. 34

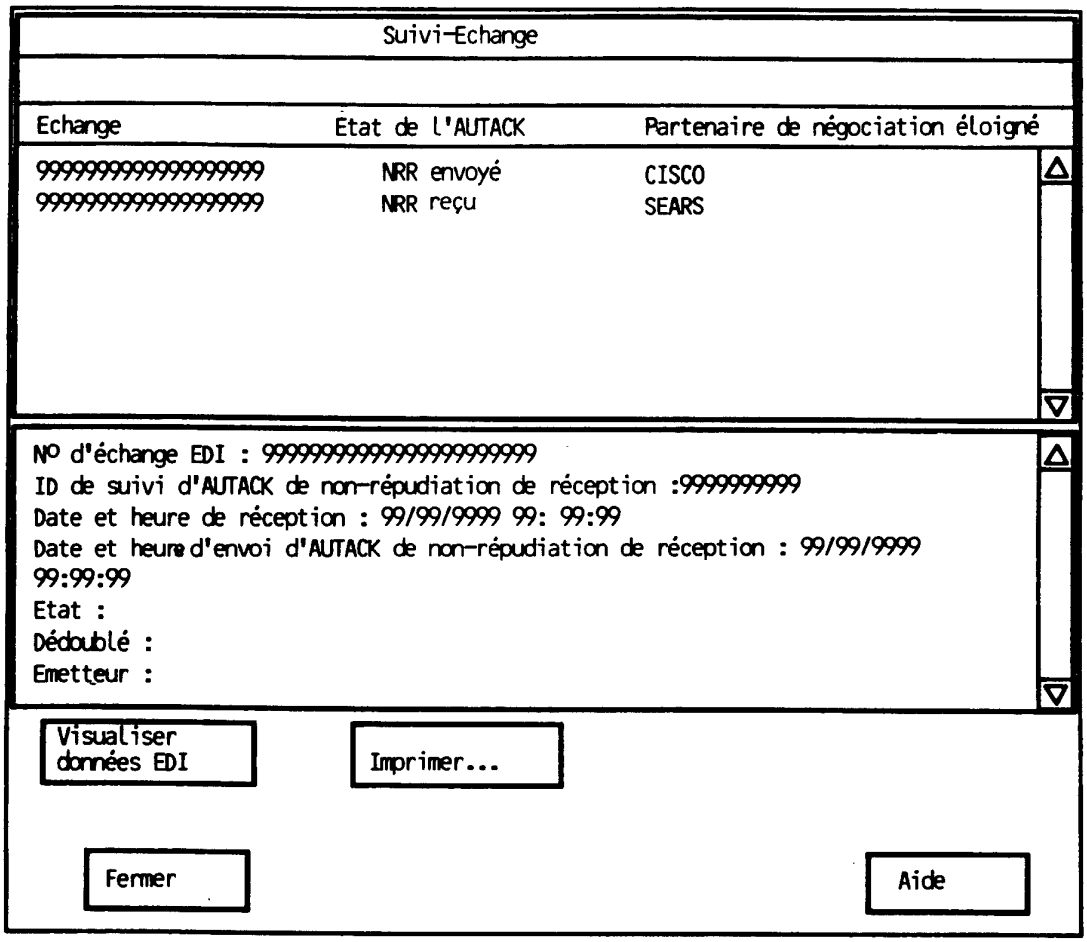

Suivi-Echange
Echange
Etat de l'AUTACK
Partenaire de négociation éloigné
99999999999999999999
NRR envoyé
CISCO
99999999999999999999
NRR reçu
SEARS
N° d'échange EDI : 99999999999999999999
ID de suivi d'AUTACK de non-répudiation de réception :9999999999
Date et heure de réception : 99/99/9999 99: 99:99
Date et heure d'envoi d'AUTACK de non-répudiation de réception : 99/99/9999
99:99:99
Etat :
Dédoublé :
Emetteur :
Visualiser données EDI
Imprimer...
Fermer
Aide

FIG. 35

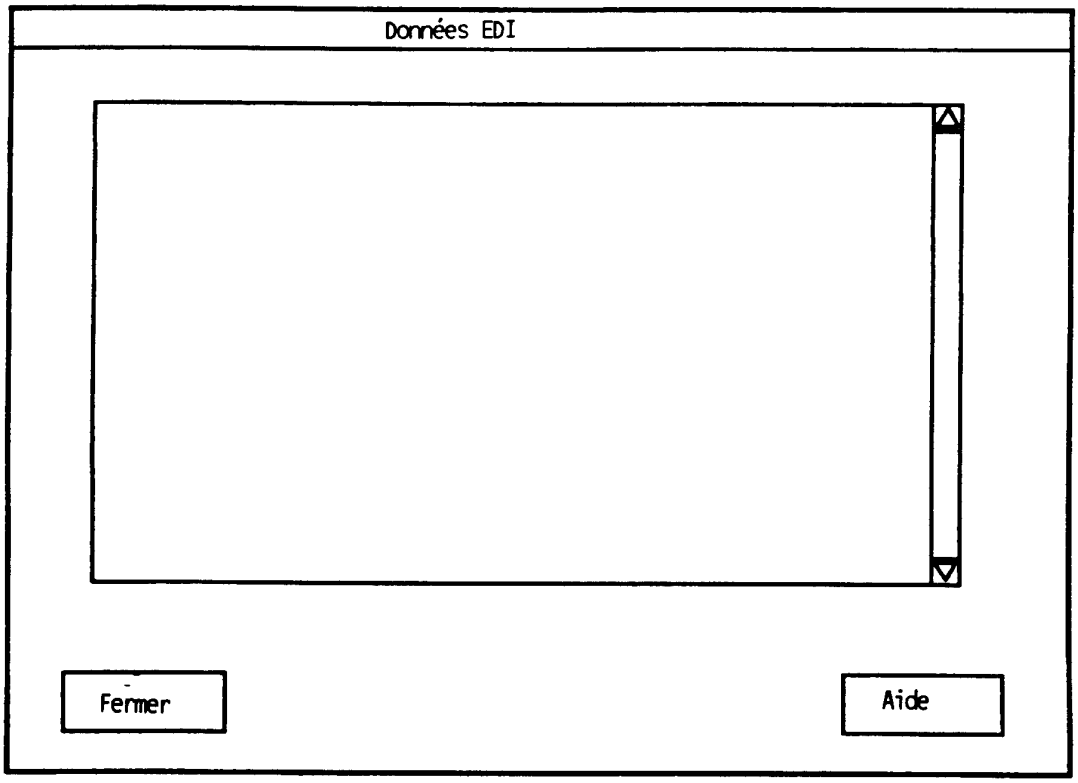


FIG. 36

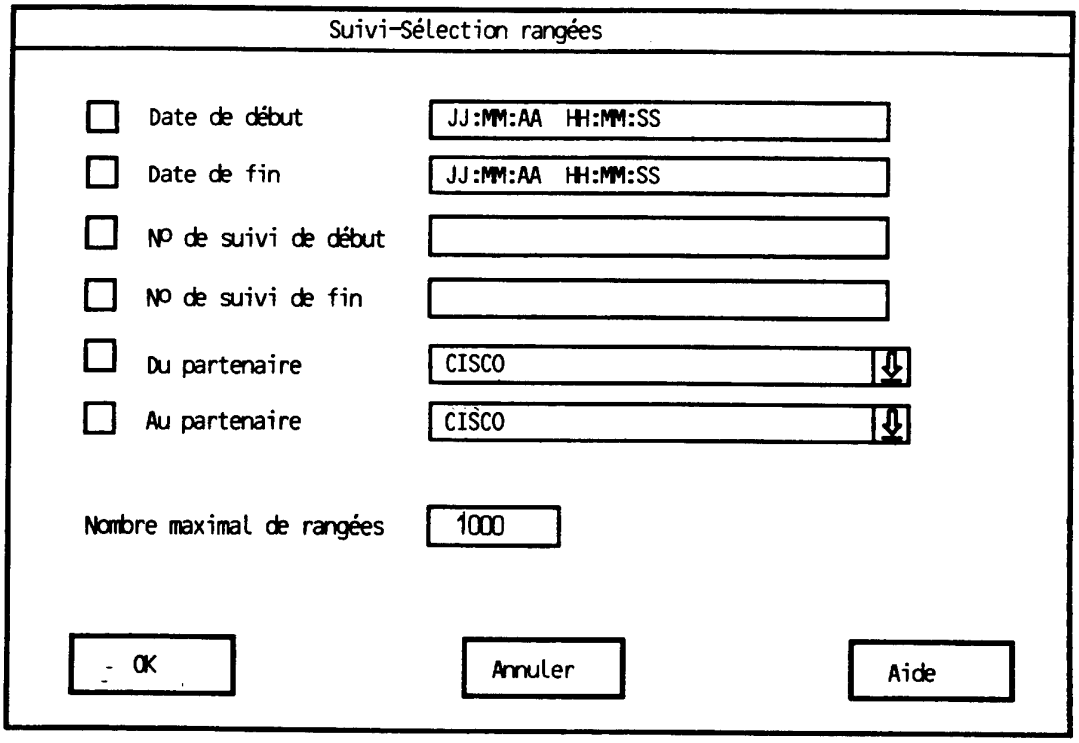

Suivi-Sélection rangées
Date de début
JJ:MM:AA HH:MM:SS
Date de fin
JJ:MM:AA HH:MM:SS
Nº de suivi de début
Nº de suivi de fin
Du partenaire
CISCO
Au partenaire
CISCO
Nombre maximal de rangées
1000
OK
Annuler
Aide

FIG. 37

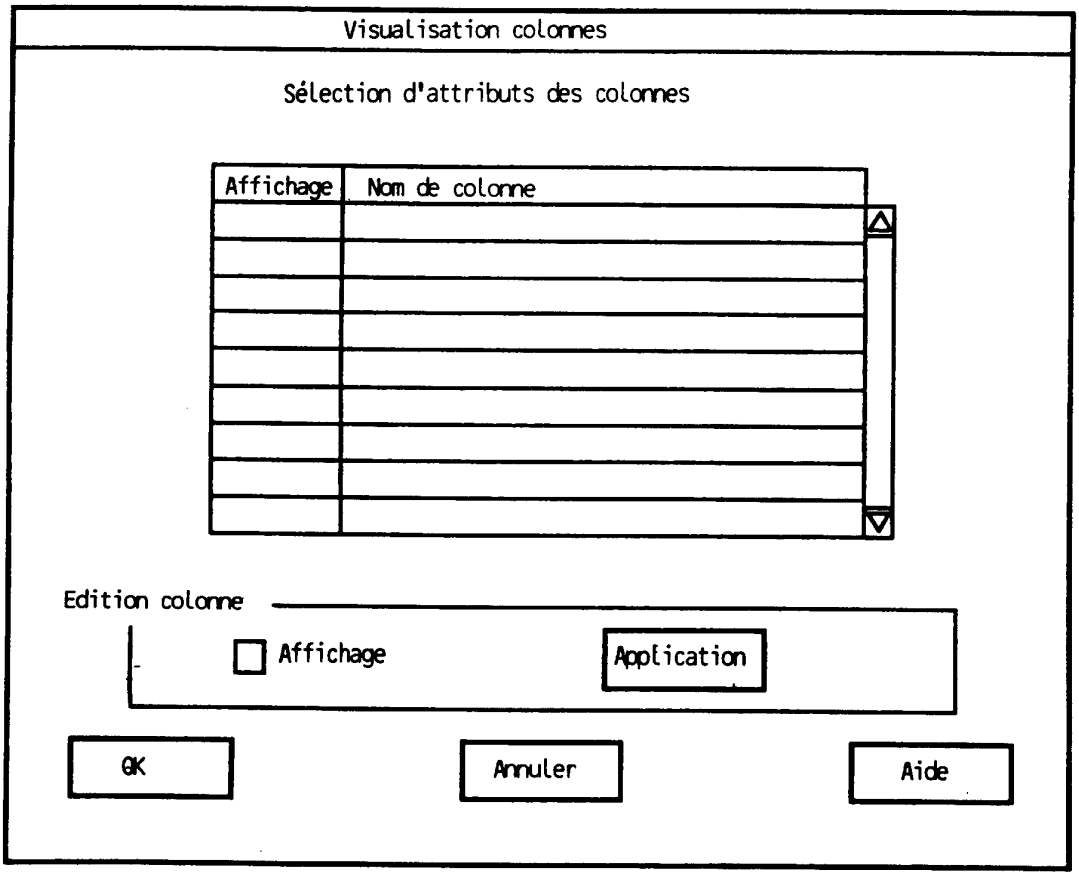

Visualisation colonnes
Sélection d'attributs des colonnes
Affichage
Nom de colonne
Edition colonne
Affichage
Application
OK
Annuler
Aide

FIG. 38

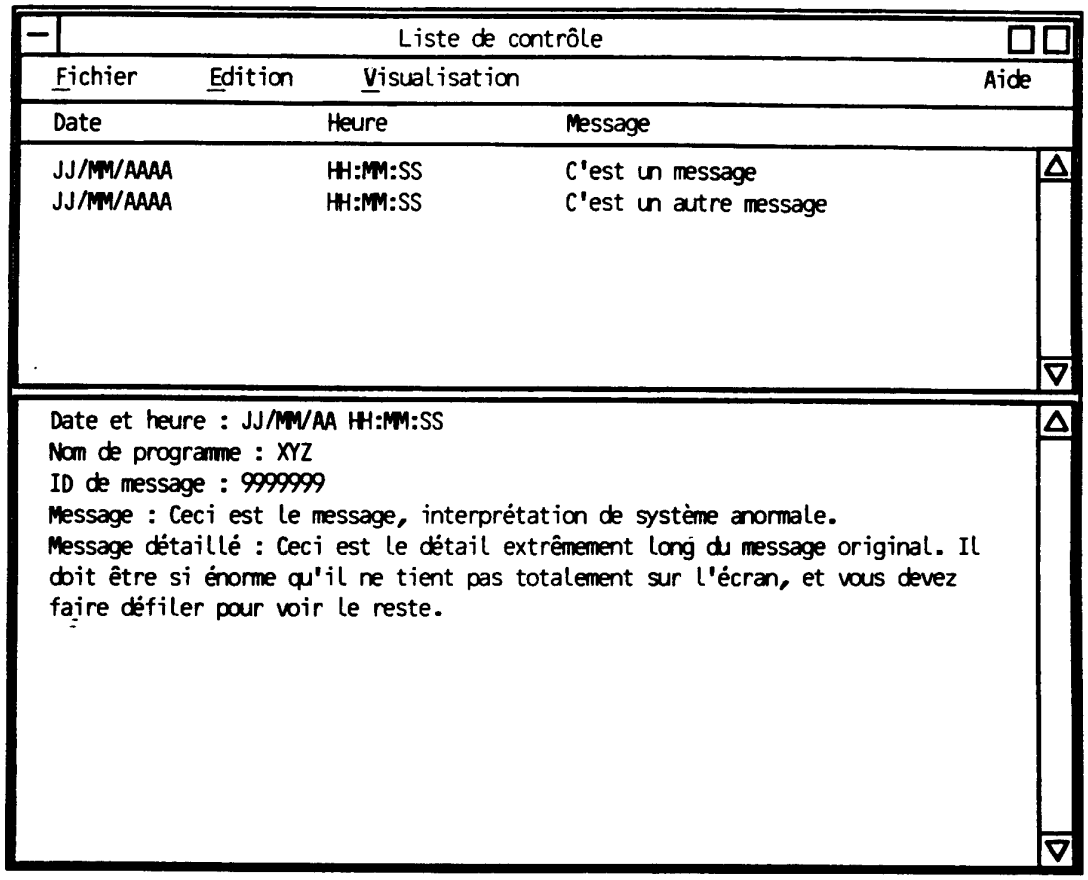

Liste de contrôle
Fichier
Edition
Visualisation
Aide
Date
Heure
Message
JJ/MM/AAAA
HH:MM:SS
C'est un message
JJ/MM/AAAA
HH:MM:SS
C'est un autre message
Date et heure : JJ/MM/AA HH:MM:SS
Nom de programme : XYZ
ID de message : 9999999
Message : Ceci est le message, interprétation de système anormale.
Message détaillé : Ceci est le détail extrêmement long du message original. Il doit être si énorme qu'il ne tient pas totalement sur l'écran, et vous devez faire défiler pour voir le reste.

FIG. 39

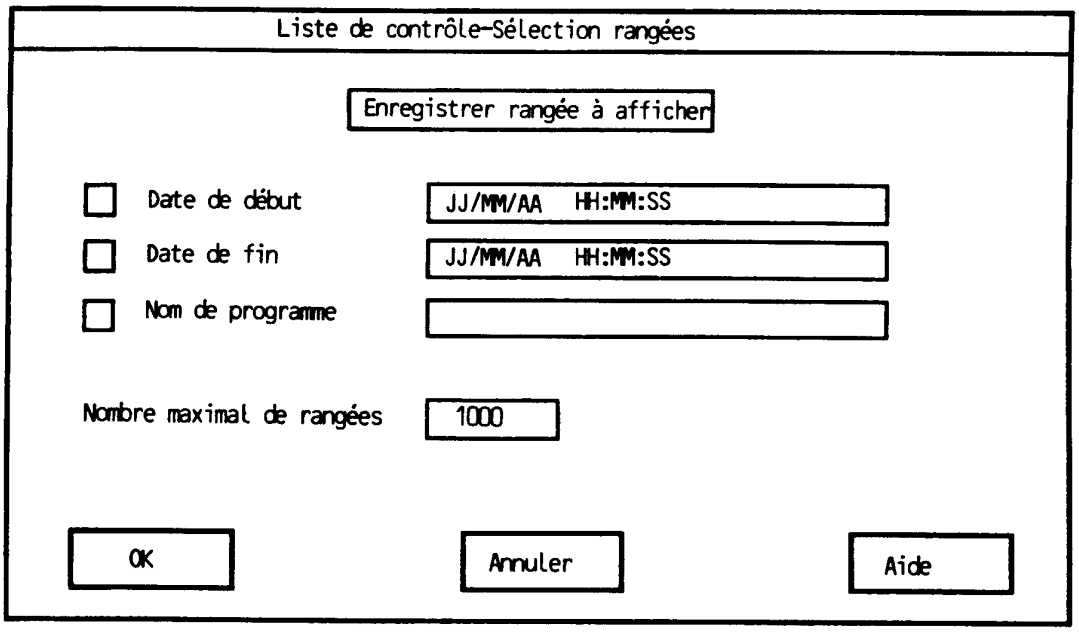

Liste de contrôle-Sélection rangées
Enregistrer rangée à afficher
Date de début
JJ/MM/AA HH:MM:SS
Date de fin
JJ/MM/AA HH:MM:SS
Nom de programme
Nombre maximal de rangées
1000
OK
Annuler
Aide

FIG. 40

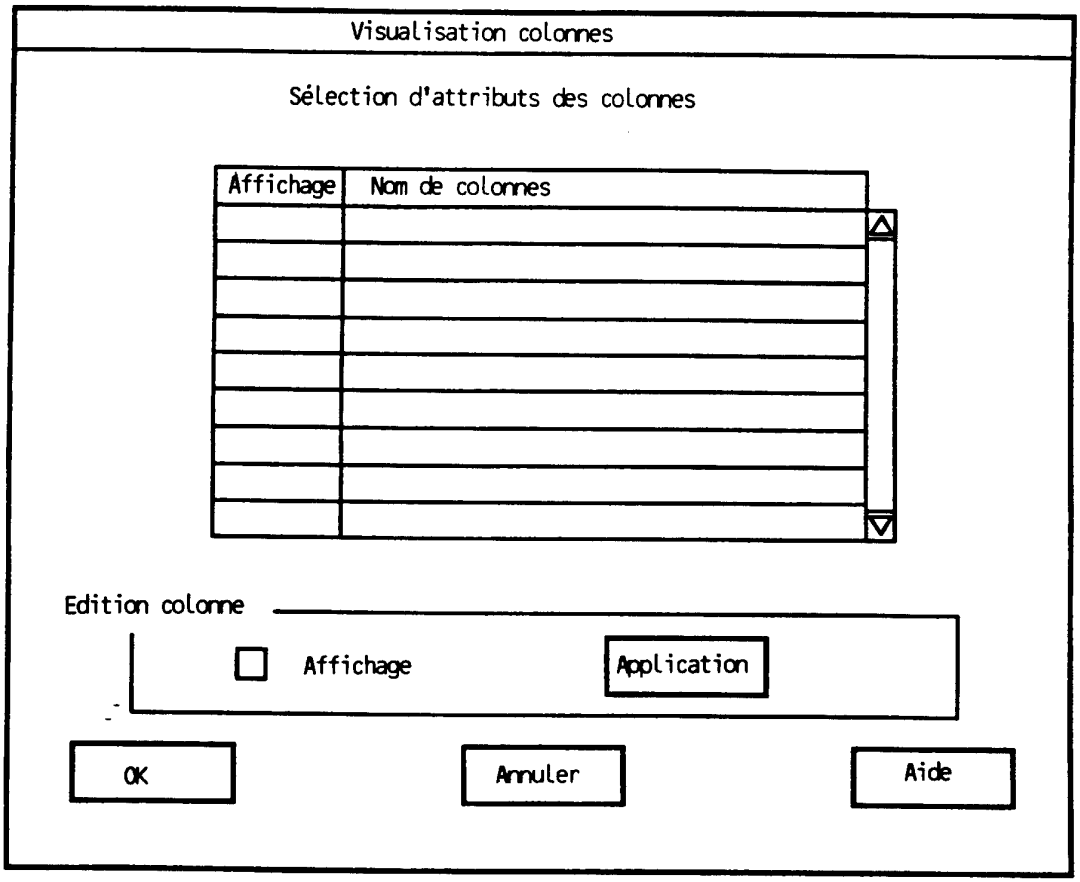

Visualisation colonnes
Sélection d'attributs des colonnes
Affichage
Nom de colonnes
Edition colonne
Affichage
Application
OK
Annuler
Aide

FIG. 41