F

OMPI

PCT/AI/ANF/6
ORIGINAL : anglais
DATE : 26 octobre 2021

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
GENÈVE

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

INSTRUCTIONS ADMINISTRATIVES DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT) :

ANNEXE F
NORME CONCERNANT LE DÉPÔT ET LE TRAITEMENT SOUS FORME ÉLECTRONIQUE DES DEMANDES INTERNATIONALES

en vigueur à compter du 1er janvier 2022

1. Le présent document contient le texte consolidé de l'annexe F des Instructions administratives du Traité de coopération en matière de brevets (PCT), tel qu'il est en vigueur à compter du 1er janvier 2022. Il a été établi conformément à l'article 58.4) et à la règle 89.2.a) et modifié conformément à la règle 89.2.b) et selon la procédure de modification prévue à la section 2.5 de l'annexe F.

2. Le texte des instructions administratives en vigueur à compter du 1er janvier 2022 se trouve, mis à part ses annexes A et F (disponibles séparément), dans le document PCT/AI/22 daté du 26 octobre 2021. Le texte de l'appendice I de l'annexe F des instructions administratives en vigueur à compter du 1er juillet 2021 se trouve dans le document PCT/AI/DTD/15 daté du 21 avril 2021. Le présent document doit être lu avec ces textes, sous réserve de tout ajout ou modification dont ils pourraient faire l'objet.

3. Le présent document est publié sur le site Internet de l'OMPI à l'adresse suivante : *www.wipo.int/pct/fr/texts/index.htm*; des exemplaires imprimés peuvent être obtenus auprès du Bureau international de l'OMPI sur simple demande.

ANNEXE F
NORME CONCERNANT LE DÉPÔT ET LE TRAITEMENT SOUS FORME ÉLECTRONIQUE DES DEMANDES INTERNATIONALES
(texte en vigueur à partir du 1er janvier 2022)

TABLE DES MATIÈRES

1. INTRODUCTION

La présente annexe a été élaborée afin de permettre la normalisation du dépôt, du traitement et de l'archivage électroniques des demandes internationales en vertu du Traité de coopération en matière de brevets (PCT)[1], en particulier en vertu de la règle 89*bis* du Règlement d'exécution du PCT et de la septième partie des instructions administratives du PCT. La norme doit permettre au déposant de déposer une demande internationale sous forme électronique qui soit acceptable pour l'ensemble des offices récepteurs, des administrations chargées de la recherche internationale et des administrations chargées de l'examen préliminaire international aux fins de la phase internationale, ainsi qu'aux fins de la phase nationale pour tous les offices désignés qui acceptent le dépôt ou le traitement des demandes sous forme électronique. Elle comprend une série d'exigences ainsi que des options pour les déposants et les offices récepteurs en ce qui concerne le dépôt des demandes internationales (et des documents connexes) sous forme électronique, sur la base des modalités de mise en œuvre énoncées dans la présente annexe et ses appendices.

L'application de la norme est subordonnée à certains choix des offices récepteurs concernant par exemple le type de signatures électroniques et le niveau de complexité des certificats numériques qu'ils acceptent. En vertu de l'instruction 710, les offices récepteurs sont tenus d'informer le Bureau international des choix qu'ils effectuent et ce dernier les publiera à l'intention des déposants. Les offices désignés sont aussi tenus de notifier au Bureau international les types de signatures électroniques et de certificats numériques qu'ils acceptent parmi ceux autorisés en vertu de la norme. Tous les offices récepteurs et offices désignés acceptant le dépôt électronique sont néanmoins tenus d'accepter les demandes internationales qui sont conformes à la "norme commune de base" visée dans l'instruction 703 et développée dans l'appendice III.

La norme s'applique aux demandes internationales déposées selon le PCT aux fins de la phase internationale mais également, en vertu de l'article 27.1) du PCT, aux fins de l'instruction de la demande durant la phase nationale. Il est également prévu que cette norme s'applique aux demandes déposées en dehors du PCT par les offices nationaux et régionaux qui le souhaitent. Elle peut également faire l'objet d'une application plus large si elle est adoptée, *mutatis mutandis*, en tant que norme générale de l'OMPI pour les demandes de brevets déposées sous forme électronique. À l'entrée en vigueur du Traité sur le droit des brevets (PLT), et sous réserve de son adoption par l'Assemblée du PLT, la norme deviendra applicable aux offices nationaux et régionaux qui seront liés par les dispositions de cet instrument.

Les principes techniques du dépôt électronique figurent dans la partie principale de l'annexe. On trouvera des précisions supplémentaires, concernant notamment certaines modalités de mise en œuvre, dans les appendices.

---

[1] Dans le présent document, les termes "articles", "règles" et "instructions" désignent respectivement les articles du Traité de coopération en matière de brevets (PCT), les règles du règlement d'exécution du PCT (ci-après dénommé "règlement d'exécution") et les instructions administratives du PCT (ci-après dénommées "instructions administratives") ou les dispositions correspondantes qu'il est proposé de modifier ou d'ajouter, selon le cas. Les textes actuels sont disponibles sur le site Internet de l'OMPI, à l'adresse suivante : http://www.wipo.int/pct/fr/texts/index.htm. Voir également les abréviations, les interprétations et le glossaire qui figurent dans la partie 9 de la présente annexe.

2. PRINCIPES GÉNÉRAUX DE LA NORME E-PCT

La présente annexe et ses appendices contiennent la norme technique définissant notamment les prescriptions, formats et procédures applicables au dépôt et au traitement, y compris aux fins des communications entre offices et administrations PCT,[2] des demandes internationales et des documents et données qui s'y rapportent ("norme E-PCT"). La partie ci-après donne un aperçu des besoins opérationnels et stratégiques qui sous-tendent cette norme.

2.1 Champ d'application

La présente norme s'applique à la création et à l'échange de documents PCT électroniques tout au long de la procédure PCT. Elle couvre les aspects techniques suivants :

a) prescriptions portant sur les documents électroniques relatifs à la demande internationale, à leur format et à leur structure;

b) empaquetage et transmission électroniques de la demande internationale; et

c) règles et principes d'application de la présente norme tout au long de la procédure PCT.

On trouvera dans les différents appendices des informations techniques supplémentaires précisant le contenu de la présente annexe. Sauf exception expressément indiquée dans la présente annexe, tous les systèmes établis aux fins du dépôt et du traitement électroniques des documents et des données PCT doivent être conformes aux prescriptions de la présente norme.

Questions qui ne sont pas examinées dans le cadre du présent document :

d) prescriptions relatives aux logiciels à utiliser dans le cadre de l'application de la présente norme; et

e) systèmes électroniques utilisés par les offices du PCT lors de la phase nationale, sauf lorsque l'article 27.1) du PCT est applicable (et compte tenu des considérations générales exposées dans la section 1).

2.2 Justification et objectifs

Le dépôt et le traitement électroniques des documents PCT sont depuis longtemps considérés comme des mesures qui s'imposent pour améliorer le fonctionnement du système du PCT. Le dépôt et le traitement électroniques des demandes internationales apporteront de nombreux avantages, et notamment :

---

[2] Le terme "office" est souvent utilisé ici dans un sens général qui inclut les offices récepteurs, les administrations chargées de la recherche internationale, les administrations chargées de l'examen préliminaire international, les offices désignés, les offices élus, le Bureau international et les offices de propriété industrielle nationaux ou régionaux, selon le contexte.

a) la réduction des vices de forme dans les demandes internationales établies au moyen d'un logiciel officiel;

b) la suppression de la saisie manuelle des données dans les systèmes informatiques;

c) un format de documents et de données agréé pour l'échange avec d'autres offices de propriété intellectuelle;

d) un traitement des demandes plus rapide et moins onéreux;

e) la possibilité pour les utilisateurs du PCT de tirer parti des techniques modernes telles que l'Internet; et

f) la possibilité de publication et de partage des documents et des données par des moyens entièrement électroniques.

2.2.1 Conditions à remplir

Les détails des conditions d'application des systèmes et des normes E-PCT sont trop nombreux pour être examinés ici. Toutefois, un résumé de l'essentiel de ces conditions figure dans la description des buts de la présente norme, ci-après :

2.2.1.1 Sécurité

Les solutions mises en œuvre dans le cadre de l'application de la présente norme doivent satisfaire aux quatre critères fondamentaux suivants en matière de sécurité des échanges de données électroniques :

a) l'authentification, qui est la procédure de validation de l'identité revendiquée par ou pour une entité;

b) l'intégrité des données, qui consiste à veiller à ce que les données ne subissent pas de modification à partir du moment de leur envoi, et à éviter leur modification, altération ou destruction par accident ou par suite d'un acte malveillant;

c) la non-répudiation, qui permet à l'expéditeur des données de disposer de preuves solides et fondées du fait que les données ont bien été transmises (avec la collaboration du destinataire), et au destinataire de disposer de preuves solides et fondées concernant l'identité de l'expéditeur, ces preuves devant être suffisantes pour que l'un ou l'autre ne puisse de manière crédible nier avoir été en possession de ces données; comprend la possibilité de vérification de l'intégrité et de l'origine des données par un tiers;

d) la confidentialité, qui consiste à veiller à ce que l'information ne puisse être lue que par les entités autorisées.

La norme admet en particulier une solution fondée sur une infrastructure à clé publique (ICP) pour l'authentification et la sécurisation des données dans

l'environnement Internet. Cela étant, elle laisse la porte ouverte à d'autres solutions susceptibles de satisfaire à l'avenir aux quatre critères susmentionnés.

Tout office disposant d'une solution opérationnelle satisfaisant aux quatre critères ci-dessus peut soumettre sa spécification en vue de son inclusion dans la présente norme. La modification proposée ferait alors l'objet d'une consultation en vertu de la règle 89.2.b) du règlement d'exécution du PCT.

2.2.1.2 Efficacité

La norme devrait promouvoir les techniques à haut rendement qui favorisent le partage d'informations instantané ou à la demande. Les systèmes PCT électroniques doivent en fin de compte diminuer les coûts pour les déposants et les offices grâce à une réduction de l'utilisation du papier et à des gains de temps.

2.2.1.3 Interopérabilité

Les systèmes compatibles avec la présente norme doivent recevoir et produire les documents et données électroniques dans un format uniformisé permettant un échange d'informations sans perte de données entre les déposants et les offices et entre les offices eux-mêmes. L'échange de données entre les systèmes devrait s'effectuer par l'intermédiaire d'un protocole commun assurant la fiabilité de la transmission sans qu'il soit nécessaire d'établir des procédures particulières et coûteuses pour chaque type de liaison.

2.3 Aperçu des secteurs de communication PCT

Dans la figure 1, les différents échanges intervenant au cours de la procédure PCT ont été classés en quatre secteurs nécessitant des variations dans l'application des critères opérationnels complexes dont il est question ci-dessus, concernant par exemple le degré de confidentialité ou d'authentification. Les "secteurs de communication PCT" sont décrits ci-dessous.

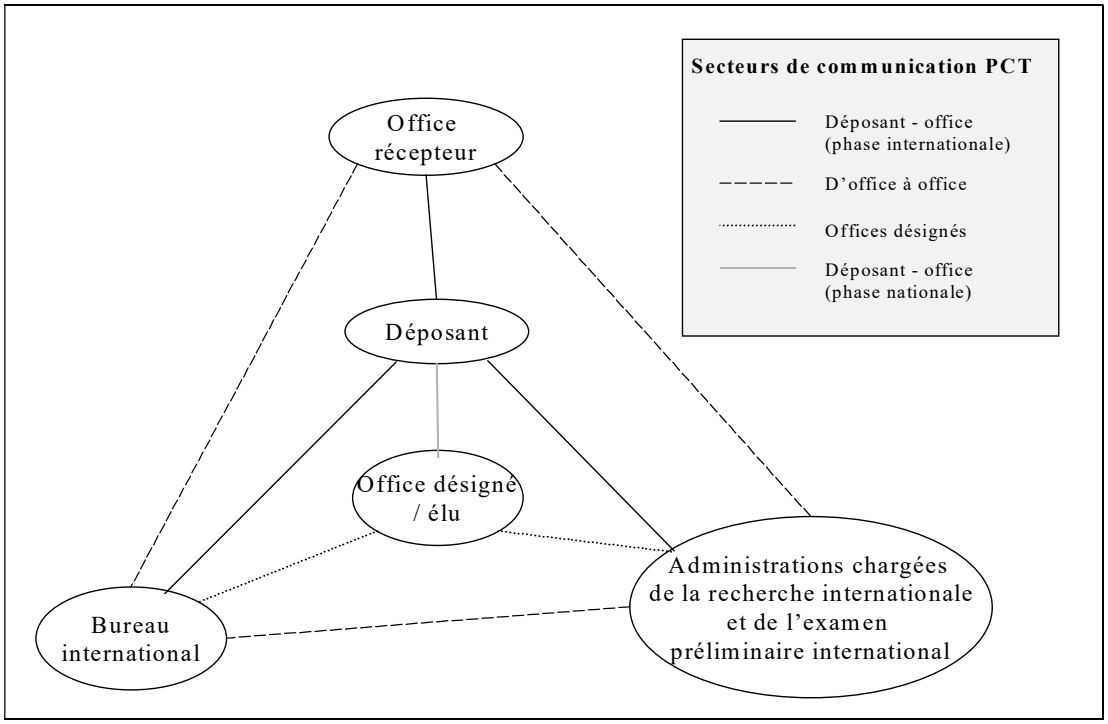


Figure 1- Secteurs de communication PCT

2.3.1 Secteur de communication entre le déposant et l'office (phase internationale)

Le secteur de communication entre le déposant et l'office (phase internationale) comprend toutes les communications entre les déposants et les offices aux fins de la phase internationale. Il englobe le dépôt initial, ainsi que tous les échanges ultérieurs entre le déposant et l'office récepteur, le Bureau international, l'administration chargée de la recherche internationale et l'administration chargée de l'examen préliminaire international.

Les opérations PCT suivantes notamment relèvent de ce secteur :

– le déposant dépose une demande internationale auprès de l'office récepteur

– le déposant envoie des modifications au Bureau international ou à l'administration chargée de l'examen préliminaire international

– le déposant envoie une requête en changements au Bureau international (règle 92*bis* du règlement d'exécution du PCT)

– le déposant envoie une demande d'examen préliminaire international à l'administration chargée de l'examen préliminaire international

– le déposant envoie un pouvoir

– le déposant retire la demande internationale

– le Bureau international envoie au déposant une copie de la brochure

– le Bureau international envoie des formulaires au déposant

– le Bureau international envoie au déposant une traduction du rapport d'examen préliminaire international

– l'administration chargée de la recherche internationale envoie au déposant le rapport de recherche international accompagné des documents cités

En plus de remplir les critères opérationnels complexes indiqués ci-dessus dans la section 2.2, les systèmes compris dans ce secteur de communication doivent pouvoir être utilisés efficacement par un très grand nombre de déposants et, dans le cas des systèmes utilisés par les déposants, par plusieurs offices différents. Les législations nationales peuvent prévoir des restrictions concernant l'utilisation de certaines techniques[3] ou les systèmes accessibles au grand public. Par conséquent, les systèmes doivent être conçus de manière à tenir compte de ces restrictions ou prescriptions particulières.

2.3.2 Secteur de communication entre offices (d'office à office)

[3] En particulier, les techniques cryptographiques font l'objet de diverses restrictions au niveau national.

Ce secteur englobe l'échange de documents et les transactions intervenant généralement entre un office PCT envoyant des documents et/ou des données et un autre office au cours de la phase internationale, y compris les opérations PCT suivantes :

– l'office récepteur envoie une copie de recherche à l'administration chargée de la recherche internationale

– l'office récepteur envoie l'exemplaire original au Bureau international

– l'office récepteur envoie le document de priorité au Bureau international

– l'administration chargée de la recherche internationale envoie le rapport de recherche internationale au Bureau international

– l'administration chargée de l'examen préliminaire international transmet la demande au Bureau international

– l'administration chargée de l'examen préliminaire international envoie le rapport d'examen préliminaire international au Bureau international

L'exigence de sécurité dont il est question dans la section 2.2, notamment en matière d'authentification et de confidentialité, est particulièrement importante pour les communications relevant de ce secteur.

2.3.3 Secteur de communication des offices désignés

Le secteur de communication des offices désignés englobe les communications entre les offices désignés/élus[4] et le Bureau international. Les échanges et les communications portent notamment sur les documents de priorité et les données de publication et comprennent les opérations PCT suivantes :

– le Bureau international envoie une brochure à l'office désigné/élu

– le Bureau international envoie des documents de priorité à l'office désigné/élu

– le Bureau international envoie un rapport d'examen préliminaire international à l'office désigné/élu

– le Bureau international envoie des formulaires à l'office désigné/élu

Les niveaux d'interopérabilité et de sécurité de l'information exigés dans ce secteur varient considérablement en fonction du type de données échangées et peuvent différer des exigences applicables dans le secteur de communication entre offices. Par exemple, la communication aux offices désignés des demandes après leur publication n'exige qu'un faible degré de confidentialité, voire aucun.

---

[4] Les termes "offices désignés" désignent aussi les offices agissant en qualité d'offices élus, sauf indication contraire du contexte. Dans certains cas, le fait que les deux qualités sont visées est souligné par la mention "offices désignés/élus".

2.3.4 Secteur de communication entre le déposant et l'office (phase nationale)

Les communications entre le déposant et les offices intervenant au cours de la phase nationale doivent, dans la mesure où l'article 27.1) du PCT est applicable, se conformer à la présente norme.

2.4 Cadre stratégique de la norme de dépôt électronique des demandes internationales (norme E-PCT)

Les objectifs énoncés dans la présente partie appellent l'établissement d'un ensemble de systèmes PCT automatisés sûrs et interopérables permettant le partage rapide et efficace de documents et de données électroniques entre déposants et offices PCT, au bénéfice de toutes les parties. Le Bureau international envisage la création d'un environnement dans lequel tout déposant peut, à l'aide d'un logiciel gratuit et normalisé, déposer une demande internationale auprès de tout office dans le monde qui accepte le dépôt électronique. L'environnement PCT du futur offrira à tous les offices PCT et à leurs clients un accès à l'information plus rapide et plus fiable.

Un tel degré d'intégration des systèmes est toujours difficile à atteindre. Cela suppose une coopération étroite de toutes les parties concernées et des investissements considérables en temps et en efforts. Les moyens techniques à mettre en œuvre pour assurer notamment la sécurité des données sont en constante évolution, tout comme l'Internet lui-même. Les systèmes devront donc être réévalués à maintes reprises.

Cet objectif n'est toutefois pas irréalisable, compte tenu en particulier de l'extrême rapidité du progrès technique et de l'évolution constante des normes internationales en matière d'échange de données. La présente norme est conçue de manière à tirer parti des normes existantes lorsque c'est possible, en misant sur les points forts des technologies facilement disponibles et largement utilisées.

2.5 Procédure de modification

2.5.1 Champ d'application

Il est nécessaire de modifier la norme de temps à autre en fonction de l'expérience pratique et du progrès technique. La procédure de modification définie dans la présente section constitue le moyen habituel par lequel le Directeur général ouvre des consultations en vertu de la règle 89.2.b) en ce qui concerne les propositions de modification du contenu de l'annexe F (y compris ses appendices) (ci-après dénommées "propositions de modification"), avant de décider de l'opportunité de promulguer ces modifications. Les procédures décrites dans la présente section doivent aussi être utilisées comme un moyen d'information supplémentaire lorsqu'il est proposé d'apporter à d'autres parties des instructions administratives des modifications qui peuvent avoir des conséquences du point de vue des exigences techniques figurant dans la présente annexe.

2.5.2 Site Internet; liste de diffusion; groupe consultatif

Le Bureau international tient à jour un site Internet destiné au traitement des propositions de modification. Le site Internet permet aux personnes intéressées d'inscrire leur adresse électronique sur une liste de diffusion relative au dépôt électronique, en vue d'être tenues informées de la publication sur le site de nouvelles propositions de modification (ou d'autres documents relatifs au dépôt électronique selon le PCT).

Tout office national, administration PCT, organisation intergouvernementale (y compris les offices régionaux) ou organisation non gouvernementale invité à prendre part aux réunions de l'Assemblée de l'Union du PCT peut s'inscrire sur le site Internet en vue de participer aux travaux d'un groupe consultatif chargé d'examiner les propositions de modification. Les participants sont vivement encouragés à désigner comme représentants au sein du groupe consultatif des techniciens et des juristes afin de faire en sorte que les propositions de modifications soient examinées de façon exhaustive. Les participants doivent, de préférence, s'inscrire au début du cycle annuel de gestion des modifications défini dans la section 2.5.4 ci-après.

Les offices nationaux des États contractants du PCT et les administrations internationales instituées en vertu du PCT participant au groupe consultatif le font en qualité de membres et les autres participants, à titre d'observateurs. Tous les membres et observateurs du groupe consultatif sont automatiquement inscrits sur la liste de diffusion relative au dépôt électronique. Le Bureau international, qui assure le secrétariat, coordonne les activités du groupe. L'examen des questions se fait de manière informelle sur le site Internet et par courrier électronique et, si nécessaire, par d'autres moyens de communication; des réunions entre membres du groupe eux-mêmes ne sont pas envisagées.

Les membres et les observateurs du groupe consultatif sont invités à examiner la manière dont il convient de mettre en œuvre les propositions de modification et, en particulier, de déterminer si des modifications doivent être promulguées et la date à laquelle elles doivent prendre effet, et de faire des recommandations dans ce sens. Le groupe est censé exercer ses activités sur la base du consensus.

Le Bureau international doit informer les membres et les observateurs du groupe consultatif de toutes les propositions de modification présentées dans le cadre de la procédure de consultation ordinaire en vertu de la règle 89.2.b) du PCT qui contiennent des modifications de l'annexe F ou qui risquent, selon le Bureau international, de nécessiter qu'il soit apporté des modifications à l'annexe F si elles sont adoptées.

2.5.3 Propositions de modification

Les propositions de modification peuvent être soumises au Bureau international par tout office ou administration qui a le droit de s'inscrire comme membre du groupe consultatif. Elles peuvent également être présentées par le Bureau international. Un office, une administration ou le Bureau international lui-même peut, s'il le désire, soumettre une proposition de modification qui lui a été présentée par un tiers. Les propositions de modification peuvent être soumises à tout moment de l'année, de préférence sur le site Internet.

Une proposition de modification peut être modifiée ou retirée par l'office ou l'administration qui l'a soumise. Chaque proposition de modification est publiée par le Bureau international sur le site Internet, sous la forme d'un dossier relatif à la proposition de modification, auquel sont jointes en annexe les observations formulées, les modifications proposées, etc. S'ils ne sont pas joints en annexe au dossier concerné, les échanges de vues sur cette proposition sont consignés dans des archives accessibles sur le site Internet.

Chaque proposition de modification doit indiquer les changements demandés en ce qui concerne le texte ou les dessins, une liste des éléments sur lesquels ces changements pourraient avoir des incidences, le motif du changement proposé, y compris les questions de traitement ou de politique générale en jeu, ainsi que la date proposée pour sa mise en œuvre, et doit comporter, si possible, un projet de plan d'exécution (par exemple, une nouvelle DTD en format XML). Elle doit aussi indiquer de préférence si, du point de vue de l'auteur de la proposition, celle-ci a un caractère purement technique ou un caractère juridique et technique.

L'examen des propositions de modification devrait normalement s'effectuer dans le cadre du cycle annuel (ordinaire) de gestion des modifications visé à la section 2.5.4. Si nécessaire, en général à la demande de l'auteur de la proposition, le Bureau international peut décider, après avoir consulté le groupe consultatif, d'accélérer l'examen d'une proposition de modification selon la procédure définie à la section 2.5.5. Il est entendu que l'examen de toute proposition de modification découlant d'un changement apporté à la législation nationale d'un État contractant du PCT en rapport avec les normes contenues dans la présente annexe s'effectuera dans le cadre de la procédure accélérée.

2.5.4 Cycle annuel de gestion des modifications

1. Chaque proposition de modification reçue par le Bureau international est publiée, dès sa réception, sur le site Internet, dans un dossier créé à cet effet, avec une mention indiquant que des observations sur cette proposition peuvent être envoyées au Bureau international. Cette publication est notifiée à bref délai par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

2. Les observations des parties intéressées reçues après la publication et la notification d'une proposition de modification visée à la section 2.5.3 sont publiées à bref délai sur le site Internet, dans le dossier relatif à la proposition de modification, et notifiées aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

3. L'examen de la proposition est ensuite suspendu jusqu'au mois de février suivant, à moins que la proposition ne fasse l'objet de la procédure accélérée visée à la section 2.5.5.

4. Le 15 février ou à bref délai après cette date, le Bureau international publie sur le site Internet une liste de toutes les propositions de modification en suspens et les renvois aux dossiers de propositions de modification correspondants, en indiquant que des observations peuvent être envoyées au Bureau international jusqu'au 31 mars au plus tard, et le notifie par courrier électronique à toutes les personnes inscrites sur la liste de diffusion relative au dépôt électronique. Le Bureau international envoie également à tous les offices et administrations PCT, aux organisations intergouvernementales intéressées et à certaines organisations non gouvernementales représentant les utilisateurs, une circulaire imprimée relative au site Internet, en les invitant à formuler des observations avant le 31 mars et en indiquant qu'il tient à leur disposition des exemplaires sur papier de ces propositions de modification.

5. Toutes les autres observations reçues par le Bureau international sont publiées, dès leur réception, dans le dossier relatif à la proposition de modification sur le site Internet et notifiées par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

6. À bref délai après le 31 mars, le Bureau international invite le groupe consultatif à examiner les propositions de modification et les observations y relatives, puis le groupe consultatif fait des recommandations au Bureau international jusqu'au 15 mai au plus tard. Ces recommandations sont immédiatement publiées dans le dossier relatif à la proposition de modification sur le site Internet et notifiées par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

7. En tenant compte des observations formulées et des recommandations du groupe consultatif, après les avoir révisées si nécessaire, le Bureau international publie sur le site Internet, le 30 juin au plus tard, les modifications destinées à entrer en vigueur le 1er janvier de l'année suivante ou, exceptionnellement, avant cette date, et le notifie par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

8. Les procédures habituelles en matière de promulgation des modifications des instructions administratives sont applicables (envoi d'une circulaire imprimée et publication dans la Gazette du PCT).

9. Le cas échéant, les exigences nouvelles ou révisées des offices sont notifiées au Bureau international, comme le prévoit l'instruction 710, aux fins de la publication dans la Gazette du PCT.

2.5.5 Examen accéléré des propositions de modification

1. À tout moment, sur demande ou de sa propre initiative, le Bureau international peut décider d'accélérer l'examen d'une proposition de modification, même si cette dernière a jusque-là fait l'objet d'un traitement ordinaire.

2. Chaque proposition de modification dont l'examen a été accéléré fait l'objet d'une publication sur le site Internet aux fins de la formulation d'observations et d'une notification par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique, comme il est indiqué aux paragraphes 1 et 2 de la section 2.5.4, à ceci près que les observations doivent être formulées dans un délai de six semaines. Parallèlement à cette publication, le Bureau international envoie la circulaire imprimée visée au paragraphe 4 de la section 2.5.4 en invitant à la formulation d'observations dans un délai de six semaines. Toutes les observations reçues sont publiées, dès leur réception, dans le dossier relatif à la proposition de modification sur le site Internet, et notifiées par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

3. Parallèlement aux actions visées au paragraphe 2, le Bureau international invite les membres et les observateurs du groupe consultatif à examiner les propositions de modification et toutes les observations ultérieures formulées dans le délai de six semaines visé au paragraphe 2, et à faire des recommandations avant la fin de ce délai de six semaines, y compris, le cas échéant, sur la date appropriée d'entrée en vigueur des modifications proposées. Ces recommandations sont immédiatement publiées dans le dossier relatif à la proposition de modification sur le site Internet, et notifiées par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

4. En tenant compte des observations formulées et des recommandations des membres et des observateurs du groupe consultatif, après les avoir révisées si nécessaire, le Bureau international publie les modifications, et la date à laquelle elles entrent en vigueur, sur le site Internet, puis les notifie par courrier électronique aux personnes inscrites sur la liste de diffusion relative au dépôt électronique.

5. Les modifications sont promulguées et toute nouvelle exigence des offices est notifiée et publiée, comme indiqué aux paragraphes 8 et 9 de la section 2.5.4.

2.5.6 Gestion des différentes versions

Lorsque la pratique et les systèmes techniques de l'office destinataire le permettent, des versions antérieures de certains éléments de la norme (en particulier les DTDs et le protocole sur l'interopérabilité en matière de dépôt électronique) peuvent fonctionner de manière simultanée pour une durée limitée. Chaque version doit être clairement identifiée par un numéro approprié.

3. STRUCTURE ET FORMAT DE LA DEMANDE INTERNATIONALE PRÉSENTÉE SOUS FORME ÉLECTRONIQUE (NORME E-PCT)

Les demandes internationales présentées sous forme électronique contiennent de nombreux types de documents et d'informations différents. Du texte, les images et les listages des séquences peuvent tous être imprimés sur papier mais chacun de ces éléments requiert une représentation électronique distincte. Par exemple, du texte peut être archivé sous forme de "codes de caractères" alors que les images peuvent être conservées sous forme de quadrillages d'éléments d'image appelés bitmaps. Le concept se complique davantage du fait que les informations peuvent être conservées sous de multiples formats électroniques. Les listages des séquences peuvent être archivés comme du texte en clair. Le texte imprimé peut faire l'objet d'une numérisation optique et être conservé comme s'il s'agissait d'une image.

Outre le format, la structure (ou l'absence de structure) de l'information peut avoir des conséquences importantes quant à la capacité des systèmes automatisés à faciliter le traitement de l'information. Les images des pages de texte ne présentent pas une structure de texte électronique et doivent donc faire l'objet d'une reconnaissance électronique ou être saisies afin que l'on puisse y effectuer des recherches.

D'autre part, le texte et d'autres informations peuvent être structurés de façon à mettre en œuvre les règles applicables en l'espèce et associer l'information avec des identifiants significatifs. Le format spécifié par cette norme pour un tel texte structuré est appelé XML (eXtensible Markup Language).

Le format XML permet aux systèmes d'ordinateur d'identifier certains éléments d'information particuliers, ce qui en accroît les capacités. Par exemple, si un document constitutif d'une demande internationale a été structuré en format XML conformément à la norme E-PCT, un système d'ordinateur pourra automatiquement afficher la première revendication; il pourra lier les références des figures aux véritables figures (dans les dessins); il pourra établir des hyperliens entre les citations de brevets et d'autres documents, et lesdits brevets et documents. Les documents structurés accroissent aussi considérablement les capacités des systèmes de recherche d'information et de publication.

Outre l'information structurée dans un format électronique donné, les demandes internationales peuvent inclure des documents contenant différents types d'informations dans divers formats électroniques. Cette collection de documents doit être structurée dans son ensemble afin de permettre aux systèmes d'ordinateur d'identifier le type de document et chacun de ses composants.

Le choix du format et de la structure électroniques est essentiel au moment de mettre en place les systèmes d'information automatisés pour le traitement des documents car le résultat peut soit faciliter soit au contraire ralentir ledit traitement. La présente section décrit le format et la structure nécessaires pour que les documents constitutifs des demandes internationales présentées sous forme électronique soient conformes à la norme E-PCT. La présente section décrit les divers formats de document électronique acceptables et la manière dont ils doivent être structurés.

3.1 Formats électroniques de document acceptables

La présente annexe est fondée sur le principe de la mise en place d'un environnement basé sur des normes existantes pour l'échange électronique des documents constitutifs de demandes internationales. Ceci a une conséquence notable la norme applicable à l'envoi de documents électroniques favorise l'utilisation de programmes ouverts et ne préconisera pas, autant que cela est possible, l'utilisation de formats commerciaux exclusifs (formats propriétaires) pour l'échange de documents électroniques. Cette ligne de conduite permet notamment d'éviter aux offices d'avoir à conserver des exemplaires multiples de dépôts électroniques dans des versions particulières de formats propriétaires sur lesquelles ils n'ont aucun contrôle.

En vertu de la présente norme, les documents constitutifs des demandes internationales doivent être exempts de virus ou autres éléments malveillants.

Il convient de noter que la présente norme s'applique également à d'autres documents ou à la correspondance ayant trait aux demandes internationales déposés ou traités sous forme électronique en vertu de la règle 89*bis*.2 et de l'instruction 713.b).

Tout document sous forme électronique qui est préparé ou transmis conformément à la présente norme doit être dans un des formats électroniques de document visés aux sections 3.1.1 à 3.1.3 qui sont acceptables en vertu de la section 3.4 dans le secteur de

communication concerné. On remarquera cependant que la section 3.4 permet, dans le secteur de communication entre offices (d'office à office), à l'office expéditeur et à l'office destinataire de se mettre d'accord pour utiliser d'autres types de formats électroniques de document pour des documents constitutifs des demandes internationales déposés sur papier et convertis en documents sous forme électronique, à l'exception de l'exemplaire original.

Les déposants peuvent présenter un listage des séquences de nucléotides et d'acides aminés dans tout format électronique de document visé aux sections 3.1.1 à 3.1.3 qui est acceptable en vertu de la section 3.4 dans le secteur de communication de déposant à office. Cependant, lorsque le listage des séquences n'est pas présenté dans le format électronique de document indiqué au paragraphe 40 de la Norme relative à la présentation du listage des séquences de nucléotides et d'acides aminés dans les demandes internationales de brevet déposées selon le PCT (voir l'annexe C des instructions administratives, ainsi que la norme ST.25 de l'OMPI et la section 3.1.1.2; on parlera ci-après de "fichier texte selon l'annexe C et la norme ST.25"), l'administration chargée de la recherche internationale et l'administration chargée de l'examen préliminaire international compétentes peuvent, aux fins de la recherche internationale et de l'examen préliminaire international, respectivement, inviter le déposant à leur remettre un listage des séquences dans ledit format électronique de document (voir la règle 13*ter*) (voir également le paragraphe 42.iv) de l'annexe C des instructions administratives en ce qui concerne le droit qu'ont les offices désignés ou élus d'inviter le déposant à leur fournir un listage des séquences dans le format électronique de document en question).

Lorsqu'un tableau figure dans une demande internationale, l'agencement (par exemple, colonnes et rangées) entre les éléments du tableau doit être maintenu, quel que soit le format électronique de document dans lequel le tableau est présenté.

3.1.1 Formats à codage de caractères

3.1.1.1 eXtensible Markup Language (XML)

Tous les documents en format XML doivent se conformer aux DTDs (Définitions des Types de Documents) spécifiées dans l'appendice I.

Le jeu de caractères codés utilisé pour tous les documents en format XML doit se limiter à celui spécifié par la norme ISO/IEC 10646:2000 (Unicode 3.0). La norme de codage de caractères utilisée pour les documents en format XML est la norme UTF-8.

En outre, chaque office récepteur peut indiquer une norme de codage de caractères telle que décrite dans les appels à commentaires RFC 2277 de l'IETF (*Internet Engineering Task Force Policy on Character Set and Languages*) et RFC 2130 de l'IETF (*Report of the IAB Character Set Workshop*) et doit informer le Bureau international de la spécification. Dans ce cas, il convient de définir ce qui suit :

a) un jeu de caractères codés;

b) une norme de codage de caractères;

c) des règles de conversion entre le jeu de caractères codés et la norme ISO/IEC 10646:2000.

Les normes de codage native-JIS et shift-JIS par exemple sont conformes aux règles indiquées ci-dessus.

Pour le secteur de communication entre le déposant et l'office (phase internationale), les offices récepteurs sont tenus d'accepter ce format conformément à la norme commune de base. En ce qui concerne le secteur de communication entre offices, les offices doivent être en mesure de transmettre et de recevoir ce format.

3.1.1.1.1 Numérotage des paragraphes dans les documents en XML (description)

Si la partie de la demande internationale correspondant à la description est codée en format XML, les paragraphes de cette partie sont numérotés par un numéro à quatre chiffres arabes commençant par des zéros si nécessaire, par exemple [0099], inscrit entre crochets et disposé à droite de la marge de gauche du document.

Si le nombre de paragraphes dépasse quatre chiffres, leur numérotage doit alors augmenter d'un chiffre, et ainsi de suite selon les besoins. Par exemple, le paragraphe [10000] suit le paragraphe [9999], et le paragraphe [100000] suit le paragraphe [99999].

3.1.1.2 Fichier texte selon l'annexe C et la norme ST.25

Tout listage des séquences présenté sous forme de fichier texte selon l'annexe C et la norme ST.25 (voir le paragraphe 40 de la Norme relative à la présentation du listage des séquences de nucléotides et d'acides aminés dans les demandes internationales de brevet déposées selon le PCT (annexe C des instructions administratives et norme ST.25 de l'OMPI)) doit être inclus par renvoi.

Pour le secteur de communication entre le déposant et l'office (phase internationale), les offices récepteurs sont tenus d'accepter ce format électronique de document conformément à la norme commune de base. En ce qui concerne le secteur de communication entre offices, ils doivent être en mesure de transmettre et de recevoir ce format.

3.1.1.3 ASCII

Tout fichier créé dans ce format doit être inclus par renvoi.

Pour le secteur de communication entre le déposant et l'office (phase internationale), les offices récepteurs sont tenus de notifier au Bureau international s'ils acceptent des documents dans ce format et, si tel est le cas, lesquels, et s'ils acceptent un format ASCII de sept ou de huit bits.

En ce qui concerne le secteur de communication entre offices, ce format peut ne pas être compris dans les paquets de documents, à moins qu'il soit inclus dans les documents constitutifs de la demande compactés (WAD, voir la section 4.1.1) d'origine déposés par le déposant, en tant que partie intégrante de l'exemplaire original (paquet du déposant, voir la section 5.2.2).

3.1.2 PDF

Tout fichier créé dans ce format doit être inclus par renvoi.

Tous les documents en format PDF doivent satisfaire aux conditions suivantes :

a) compatibilité avec la version 1.4 de Adobe Portable Document Format;

b) texte non comprimé pour faciliter la recherche;

c) texte non chiffré;

d) pas d'objets incorporés en OLE;

e) toutes les polices de caractères doivent être incorporées et utilisées par le biais d'une licence de distribution.

Pour le secteur de communication entre le déposant et l'office (phase internationale), les offices récepteurs sont tenus de notifier au Bureau international s'ils acceptent des documents dans ce format, en précisant le cas échéant la ou les versions qui sont acceptées. Afin de faciliter la tâche des offices qui n'acceptent pas de documents en format PDF, les offices qui décident d'accepter des documents dans ce format doivent aussi les convertir (partie texte et dessins) en images TIFF, puis les transmettre dans ces deux formats au Bureau international.

En ce qui concerne le secteur de communication entre offices, les offices sont tenus de notifier au Bureau international s'ils transmettent ou acceptent des documents dans ce format, en précisant la ou les versions utilisées. Pour ce qui est des documents présentés initialement en format PDF, les offices peuvent demander la transmission des documents en format PDF d'origine en sus des documents convertis en format TIFF.

3.1.3 Formats d'images

Des images peuvent être utilisées pour les dessins, les figures, les équations ou d'autres formes d'illustrations, ou des documents scannés. Un office récepteur peut choisir de permettre aux déposants de déposer tout ou partie de la description ou des revendications dans un format d'image.

3.1.3.1 Format de fichier d'images balisées (Tagged Image File Format – TIFF)

Tout fichier créé dans ce format doit être inclus par renvoi.

Les images en fac-similé en format TIFF (*Tagged Image File Format*) (en noir et blanc) à utiliser dans l'échange de documents constitutifs des demandes internationales doivent répondre aux prescriptions suivantes :

a) TIFF V6.0 avec compression de groupe 4, monobande, codage Intel

b) résolution de 300 ou 400 dpi, au choix

c) taille maximale : la taille des pages doit être A4[5] ou Lettre[6]. Cependant, la taille maximale recommandée est de 255 mm pour 170 mm.

Pour le secteur de communication entre le déposant et l'office (phase internationale), les offices récepteurs sont tenus d'accepter ce format. Des images peuvent être utilisées pour les dessins, les figures, les équations et d'autres formes d'illustrations, et pour les descriptions et les revendications. Ce format n'est pas fait pour être utilisé aux fins de remplacement des formats de document à caractères codés.

En ce qui concerne le secteur de communication entre offices, les offices doivent être capables de transmettre et de recevoir ce format. Les images peuvent être utilisées pour les dessins, les figures, les équations et d'autres formes d'illustrations, et pour les descriptions et les revendications. Ce format peut aussi être utilisé pour transmettre des documents scannés entre offices sous la forme d'images de pages.

3.1.3.2 Format d'échange de fichier JPEG (JFIF)

Tout fichier créé dans ce format doit être inclus par renvoi.

Les images en format JFIF à utiliser dans l'échange de documents relatifs aux demandes internationales doivent remplir les prescriptions suivantes :

a) résolution de 300 ou 400 dpi, au choix

b) taille maximale de 255 mm pour 170 mm.

Pour le secteur des communications entre le déposant et l'office (phase internationale), les offices sont tenus de notifier au Bureau international s'ils acceptent des images dans ce format ou pas. Des images peuvent être utilisées pour les dessins, les figures, les équations ou d'autres formes d'illustrations. Ce format n'est pas fait pour être utilisé aux fins de remplacement des formats de document à caractères codés.

En ce qui concerne le secteur des communications entre offices, les offices sont tenus de notifier au Bureau international s'ils transmettent ou acceptent des images dans ce format.

3.1.4 Formats de pré-conversion

Les documents en format de pré conversion présentés en vertu de l'instruction administrative 706.a) ou f) doivent être inclus comme des documents auxquels il est fait référence.

En ce qui concerne la communication entre le déposant et l'office (phase internationale), les offices récepteurs informent le Bureau international s'ils acceptent le dépôt, en vertu de l'instruction administrative 706.a) et f), de documents en format de pré conversion et, dans l'affirmative, l'informent des formats de pré conversion qu'ils acceptent (voir l'instruction administrative 710.a)iv)).

---

[5] Taille A4 = 210 x 297 mm, avec un maximum de 3307 x 4677 pixels à 400 dpi.

[6] Taille Lettre = 215,9 x 279,4 mm (8,5 x 11 pouces), avec un maximum de 3400 x 4400 pixels à 400 dpi.

Aux fins de la procédure prévue dans l'instruction administrative 706.b), tout office récepteur qui décide d'accepter les documents présentés en vertu de l'instruction administrative 706.a) ou f) dans un format de pré conversion que le Bureau international ne peut pas traiter doit transmettre le document en question au Bureau international à la fois dans un format électronique de document que le Bureau international peut traiter et dans le format de pré conversion original.

3.2 Structure des documents constitutifs d'une demande internationale déposée sous forme électronique (demande E-PCT)

Une demande internationale peut contenir de nombreux documents, chacun avec du texte, des dessins et des listages des séquences conservés dans des formats électroniques différents. Afin de répondre à la nécessité de maintenir une variété de formats électroniques de document tout en préservant une structure compréhensible par un ordinateur, une demande internationale déposée sous forme électronique, y compris ses documents constitutifs, doivent être conformes à la structure spécifiée dans la présente section.

Afin d'être conforme à la présente norme, chaque demande internationale déposée sous forme électronique doit contenir un fichier contenant un paquet de données en format XML qui fait explicitement référence aux documents soumis et doit être conforme à la DTD (définition de type de document) *"package-data"* décrite dans la section 3.1 de l'appendice I. Cependant, dans le secteur de communication entre offices (d'office à office), l'office expéditeur et l'office destinataire peuvent se mettre d'accord pour employer d'autres types de structures d'envoi pour des documents constitutifs des demandes internationales déposés sur papier et convertis en documents sous forme électronique. Dans ce cas, l'office destinataire en informe le Bureau international. Les documents référencés (tels que la requête et la nouvelle demande de brevet) font logiquement partie intégrante de la demande en tant que telle.

Comme cela est montré dans les figures 2 et 2*bis*, les documents référencés (entités externes) sont généralement la requête, la demande (description, revendications), les documents de priorité, etc., qui à leur tour peuvent contenir des images, des tableaux, des dessins qui sont des objets certes séparés mais également liés qui peuvent être codés en formats XML, PDF, ST.25, ASCII ou d'images (TIFF ou JFIF). Chaque document en format XML doit être conforme à l'une des DTDs décrites dans l'appendice I sauf les "autres documents" référencés, pour lesquels un office récepteur peut choisir d'accepter des documents en format XML conformes à des DTDs non spécifiées dans l'appendice I. Dans ce dernier cas, l'office doit notifier les DTDs au Bureau international. La version de la DTD doit être indiquée dans l'attribut "DTD-VERSION" du document en format XML (tel que spécifié par la DTD elle-même).

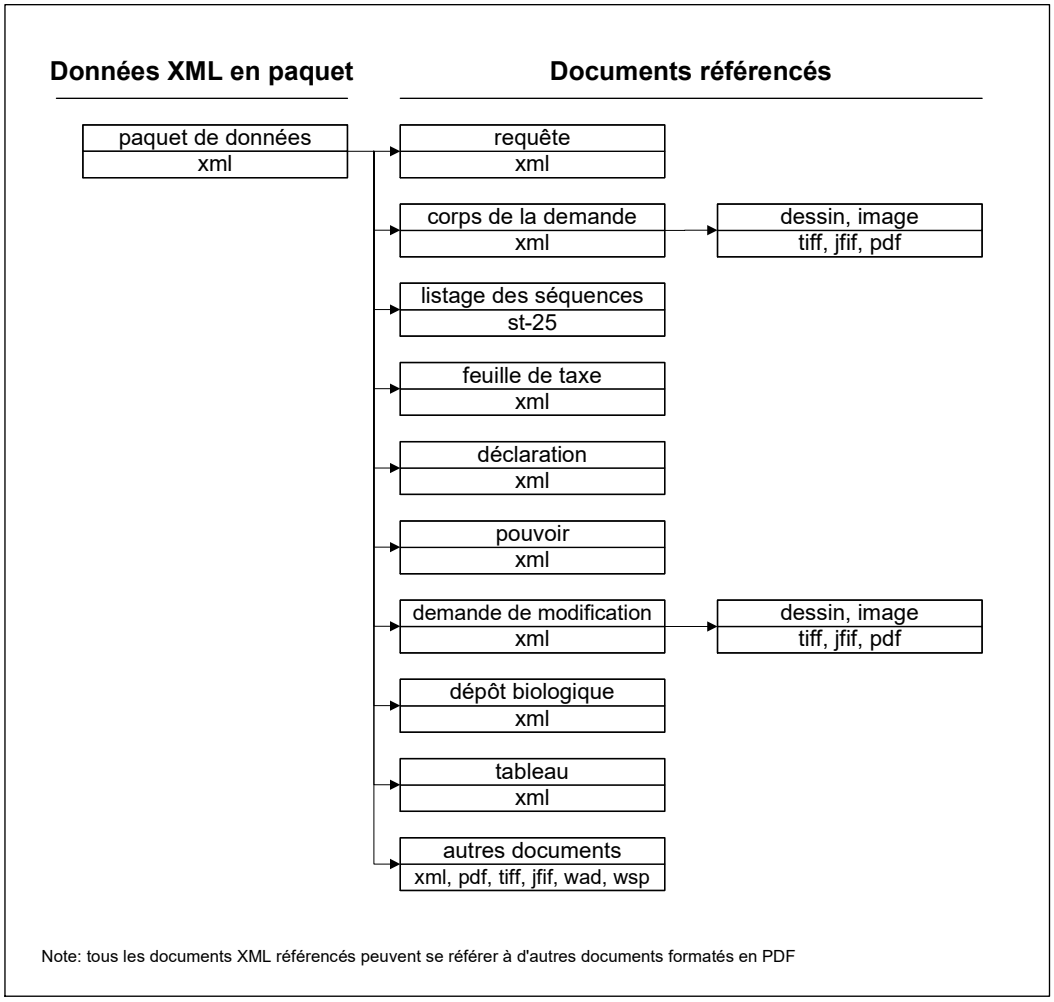


Figure 2 – Exemple de structure de documents constitutifs d'une demande internationale déposée sous forme électronique (demande E-PCT) lorsque le texte de la description, des revendications et de l'abrégé n'est pas en format à codage de caractère (en format XML)

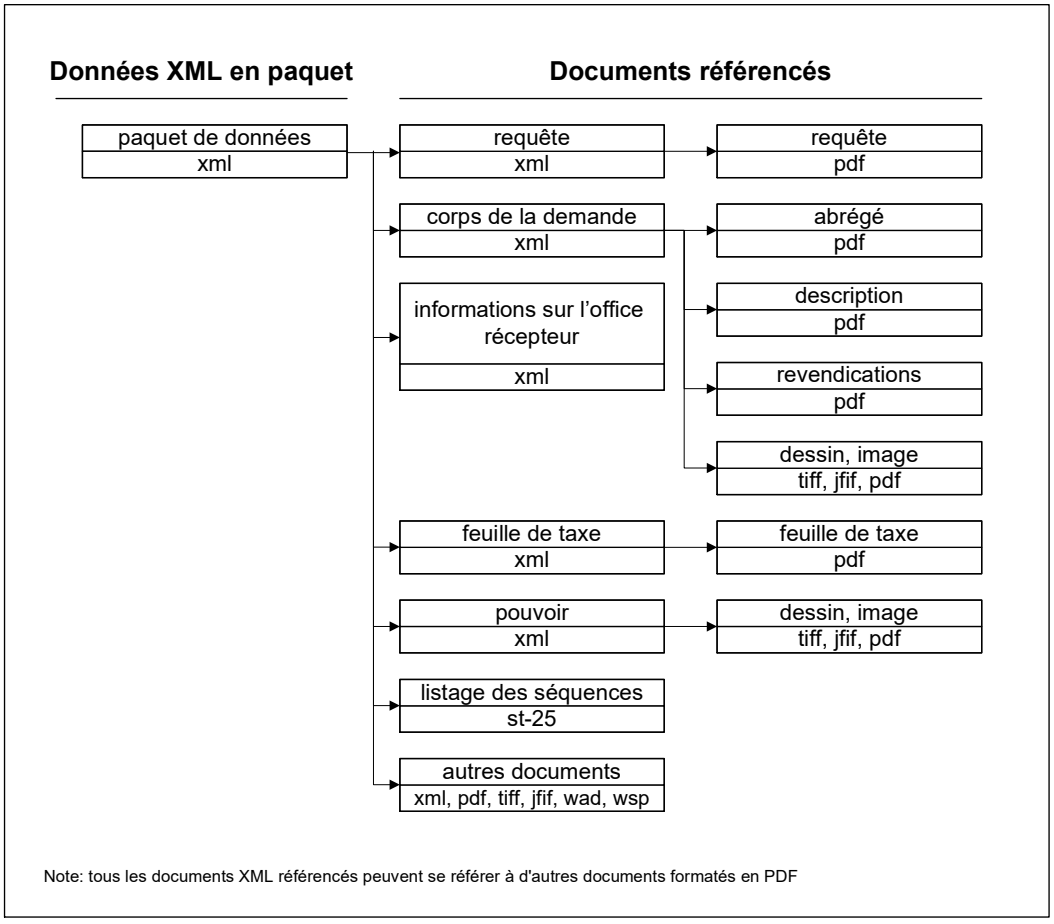


Figure 2*bis* – Exemple de structure de documents constitutifs d'une demande internationale déposée sous forme électronique (demande E-PCT) lorsque le texte de la description, des revendications et de l'abrégé n'est pas en format à codage de caractère (mais en format PDF)

3.3 Signature électronique

L'utilisation d'un certain nombre de types de signature est permise aux fins de l'échange de documents constitutifs de demandes internationales (voir l'instruction administrative 701) en vertu de la présente norme. Chaque office récepteur doit notifier les types de signature qu'il accepte au Bureau international.

Les sections ci-après décrivent ces types de signatures, qui peuvent être soit des signatures électroniques de base soit des signatures électroniques renforcées[7]. À ce stade, cette norme accepte l'utilisation de signatures de base multiples mais pas l'utilisation de signatures renforcées multiples.

3.3.1 Signature en fac-similé

Pour créer ce type de signature, un fichier en format XML (p. ex. la requête) doit comprendre l'élément <fax> et un renvoi à une entité externe inscrite dans l'attribut FILE désignant un fichier en format TIFF contenant une représentation en mode point (bitmap)

[7] Pour les définitions de la "signature électronique de base" et de la "signature électronique renforcée", voir la section 9.

de la signature. Le fichier en format TIFF doit être conforme aux prescriptions décrites dans la section 3.1.3.1.

3.3.2 Signature composée d'une chaîne de caractères

Pour créer ce type de signature, un fichier en format XML doit comprendre l'élément <text-string> contenant une chaîne de caractères qui est l'équivalent de la signature "manuscrite" de l'utilisateur, encadrée par le caractère 'barre oblique' "/" comme indiqué ci-après :

/janedoe/

La chaîne de caractères ne doit pas comprendre le caractère "/" et doit être choisie par le déposant comme signature électronique. Voici quelques exemples valables :

/John Smith/

/Tobeornottobe/

/1345728625235/

/Günter François/

3.3.3 Signature de type "click-wrap"

Pour créer ce type de signature, le déposant clique généralement sur un bouton dans l'interface utilisateur indiquant "J'accepte". Ceci est indiqué dans un fichier en format XML par la présence de l'élément vide <click-wrap/>.

3.3.4 Signature électronique renforcée

La signature électronique renforcée s'appuie sur l'utilisation d'une ICP et d'une signature numérique de type PKCS #7. Voir la section 4.2 et l'appendice II pour de plus amples informations sur la norme PKCS #7 et l'ICP.

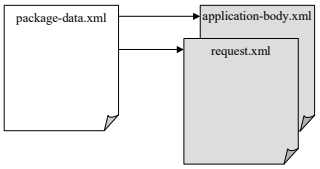
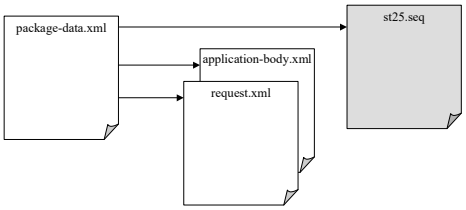
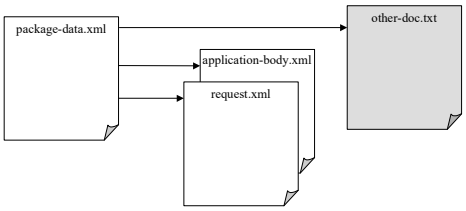
Le type "données signées" PKCS #7 est produit à partir du message électronique par l'action du signataire qui utilise sa clé de signature privée pour chiffrer l'empreinte du message. Le type "données signées" PKCS #7 comporte une copie du certificat numérique délivré au signataire.

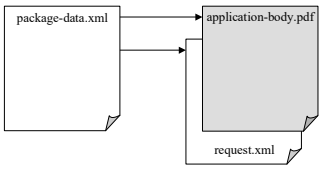
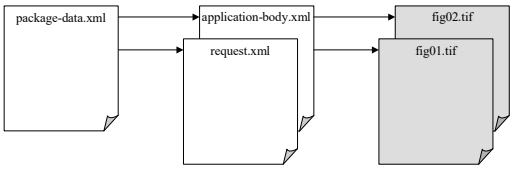
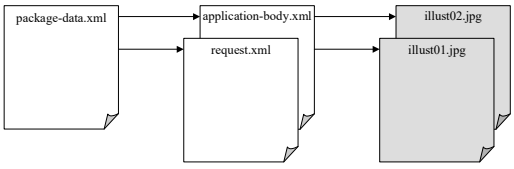
3.4 Formats de document acceptés, par secteur de communication PCT

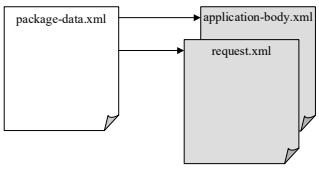
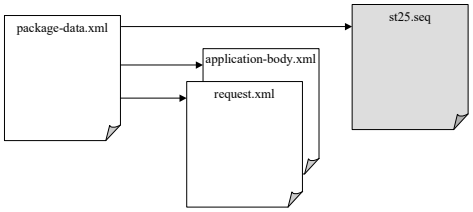
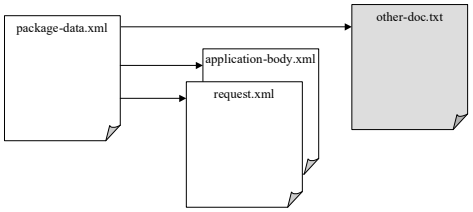
Les tableaux qui figurent ci-après listent tous les formats d'image et de document conformes à la présente norme par secteur de communication PCT. Pour chaque format, les tableaux présentent les options disponibles à l'usage des offices et un exemple correspondant du contenu d'un paquet conforme à la présente norme.

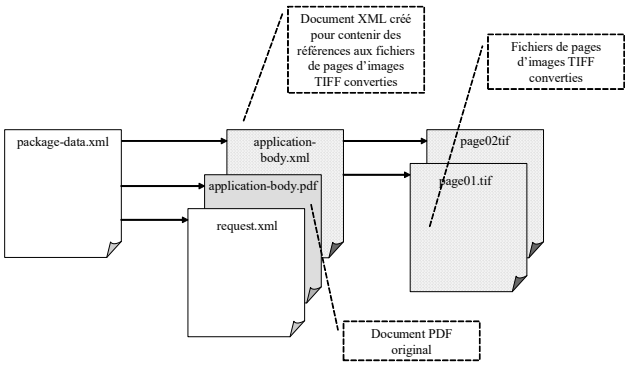
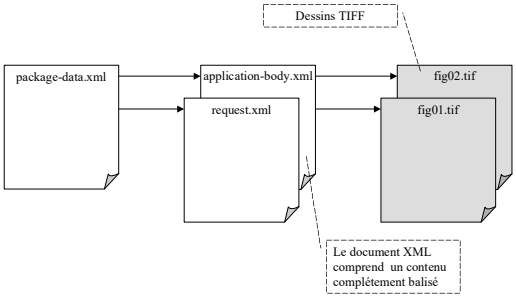
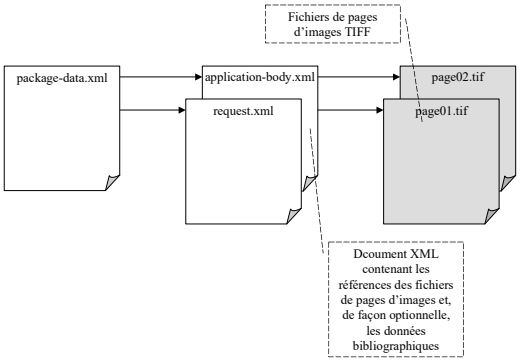
Tout document sous forme électronique qui est préparé ou transmis conformément à la présente norme doit être dans un des formats électroniques de document visés aux sections 3.1.1 à 3.1.3 qui sont acceptables dans le secteur de communication concerné conformément à la présente section. Cependant, dans le secteur de communication entre offices (d'office à office), l'office expéditeur et l'office destinataire peuvent se mettre d'accord pour employer d'autres types de formats électroniques de document pour des

documents constitutifs des demandes internationales déposés sur papier et convertis en documents sous forme électronique, à l'exception de l'exemplaire original. Dans ce cas, l'office destinataire en informe le Bureau international.

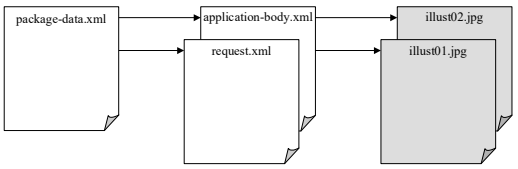
Secteur de communication entre le déposant et l'office (phase internationale)		
Format	*Options acceptées*	*Exemple de contenu de paquet*
XML Voir la section 3.1.1.1	Les offices récepteurs sont tenus d'accepter des documents dans ce format conformément à la norme commune de base. Ils doivent notifier au Bureau international du schéma d'encodage la norme de codage de caractères pour les documents en format XML (comme cela est décrit dans la section 3.1.1.1) lorsqu'elle est différente de la norme de codage UTF-8.	
Fichier texte selon l'annexe C et la norme ST.25 Voir la section 3.1.1.2	Les offices récepteurs sont tenus d'accepter des documents dans ce format conformément à la norme commune de base.	
ASCII Voir la section 3.1.1.3	Les offices récepteurs sont tenus de notifier au Bureau international s'ils acceptent ou non des documents dans ce format et, si tel est le cas, lesquels, et en quels caractères ASCII (sept et/ou huit bits)	

Secteur de communication entre le déposant et l'office (phase internationale)		
Format	*Options acceptées*	*Exemple de contenu de paquet*
PDF Voir la section 3.1.2	Les offices récepteurs sont tenus de notifier au Bureau international s'ils acceptent ou non des documents dans ce format. Afin de faciliter la tâche des offices qui n'acceptent pas de documents en format PDF, les offices qui décident d'accepter des documents dans ce format doivent aussi en convertir le texte et les dessins en images TIFF et transmettre ces documents au Bureau international dans les deux formats.	
TIFF Voir la section 3.1.3.1	Les offices récepteurs sont tenus d'accepter des documents dans ce format conformément à la norme commune de base. Les images peuvent être utilisées pour les dessins, les figures, les équations ou toute autre illustration. Ce format n'est pas destiné à être employé à titre de remplacement du codage des caractères.	
JFIF Voir la section 3.1.3.2	Les offices récepteurs sont tenus de notifier au Bureau international s'ils acceptent ou non des images dans ce format.	

Secteur de communication entre offices (d'office à office)		
Format	*Options acceptées*	*Exemple de contenu de paquet*
XML Voir la section 3.1.1.1	Les offices doivent pouvoir transmettre et recevoir ce format. Les offices récepteurs sont tenus de notifier au Bureau international la norme de codage de caractères pour les documents en format XML (comme cela est décrit dans la section 3.1.1.1) lorsqu'elle est différente de la norme de codage UTF-8.	
Annexe C Voir la section 3.1.1.2	Les offices doivent pouvoir transmettre et recevoir ce format.	
ASCII *Voir la section 3.1.1.3*	Les offices sont tenus de notifier au Bureau international s'ils transmettent et acceptent, ou non, les documents dans ce format.	

Secteur de communication entre offices (d'office à office)		
Format	*Options acceptées*	*Exemple de contenu de paquet*
PDF Voir la section 3.1.2	Les offices sont tenus de notifier au Bureau international s'ils transmettent et acceptent, ou non, des documents dans ce format. En ce qui concerne les documents initialement présentés en format PDF, les offices peuvent demander la transmission du document PDF original en sus du document converti en formats XML et TIFF.	
TIFF Voir la section 3.1.3.1	Les offices doivent pouvoir transmettre et recevoir ce format. Les images peuvent être utilisées pour des dessins, des figures, des équations ou d'autres formes d'illustrations, comme dans le premier exemple à droite.	
TIFF *(suite)*	Ce format peut également être utilisé pour transmettre des documents scannés ou basés sur des images entre offices, sous la forme de pages d'images, comme dans le second exemple à droite.[8]	

[8] Voir "TIFF" dans le tableau du secteur de communication entre le déposant et l'office pour un exemple d'images TIFF utilisées comme des dessins etc. Le contenu de paquet présenté ici à titre d'exemple n'est pas autorisé dans le secteur de communication entre le déposant et l'office.

Secteur de communication entre offices (d'office à office)		
Format	*Options acceptées*	*Exemple de contenu de paquet*
JFIF Voir la section 3.1.3.2	Les offices sont tenus de notifier au Bureau international s'ils acceptent de transmettre ou de recevoir des images dans ce format.	

4. EMPAQUETAGE DES DOCUMENTS CONSTITUTIFS DE DEMANDES INTERNATIONALES

Étant donné qu'une demande internationale est généralement constituée de plusieurs fichiers, il est utile d'assembler ceux-ci en un seul "paquet" électronique aux fins de la transmission. La présente norme prévoit deux types d'empaquetages de demandes internationales, à savoir les paquets non fondés sur une ICP et les paquets fondés sur une ICP. Les fichiers contenant des documents constitutifs de la demande compactés ("WADs") ne sont pas fondés sur une ICP alors que les paquets compactés et signés ("WASPs") le sont. On trouvera dans l'appendice II de plus amples précisions sur la mise en œuvre de solutions ICP aux fins de la présente norme.

Tout document sous forme électronique qui est préparé ou transmis conformément à la présente norme doit être empaqueté conformément aux sections 4.1 et 4.2. Cependant, dans le secteur de communication entre offices (d'office à office), l'office expéditeur et l'office destinataire peuvent se mettre d'accord pour ne pas empaqueter les documents constitutifs des demandes internationales déposés sur papier et convertis en documents sous forme électronique, ou pour les empaqueter autrement. Dans ce cas, l'office destinataire en informe le Bureau international.

Tous les fichiers d'échange de documents électroniques visés dans la présente norme doivent être préalablement présentés sous forme de WAD. On trouvera dans la section 5.2 des informations supplémentaires sur les combinaisons paquet/transmission autorisées en fonction des différents secteurs de communication PCT.

4.1 Paquets non fondés sur une ICP

La présente norme ne prévoit qu'un type de paquets non fondés sur une ICP : le paquet de documents constitutifs de la demande compactés (WAD).

4.1.1 Documents constitutifs de la demande compactés (WAD)

La demande internationale, ainsi que les documents auxquels elle renvoie expressément, le cas échéant, sont compactés en un seul bloc de données. Ce bloc de

données, dit “documents constitutifs de la demande compactés” (WAD) est créé par application du standard de compression ZIP.

Le logiciel employé pour créer le fichier ZIP doit être conforme aux spécifications du format de fichier ZIP, publiées dans le descriptif du logiciel PKZIP® de PKWARE® (révisé le 08/01/1998). Tous les fichiers ZIP doivent avoir une structure de répertoire plate.

Le standard ZIP donne au logiciel de compression le choix parmi un certain nombre d’algorithmes de compression. La méthode de compression sera la “déflation” avec l’option compression normale.

4.2 Types de paquets fondés sur une ICP

La présente norme ne prévoit que deux types de paquets fondés sur une ICP : le paquet compacté et signé (WASP) et le WASP combiné (C-WASP). Voir l’appendice II pour de plus amples informations sur l’ICP.

4.2.1 Paquet compacté et signé (WASP)

Lorsque la personne qui signe le WASP est le déposant (ou son représentant), la signature du WASP peut aussi être utilisée en tant que signature électronique renforcée de la demande (voir la section 3.3) si les systèmes techniques en place permettent que la demande soit ainsi signée de façon automatique.

Un certificat numérique simplifié ou qualifié (voir les définitions correspondantes dans la section 9) accompagne la signature numérique.

La figure 3 donne une représentation simplifiée du WASP. Le schéma a été délibérément simplifié pour exclure les détails techniques qui ne se rapportent pas directement aux éléments essentiels de la structure du paquet. Par exemple, l’emballage PKZIP n’a pas été représenté.

Dans le cas d’une notification envoyée au déposant par l’office, celui-ci prépare, signe et envoie le WASP qui contient ladite notification.

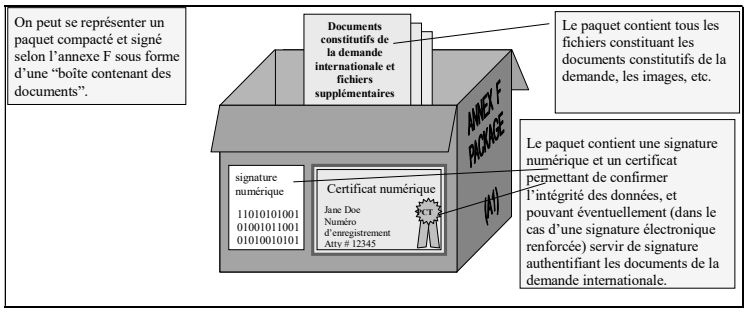


Figure 3 – Paquet compacté et signé (WASP)

Voir l’appendice II pour de plus amples précisions sur la spécification technique du WASP.

4.2.2 WASP combiné (C-WASP)

Le ou les WASPs envoyés au déposant par l'office sont compactés en utilisant le standard de compression ZIP tel que cela est décrit dans la section 4.1.1 et ils sont traités comme un seul bloc de données. Ce bloc de données est appelé le WASP combiné (C-WASP).

4.3 Convention de nommage des fichiers

La présente convention de nommage des fichiers est établie afin de renforcer l'automatisation des serveurs, de faciliter le travail produit au niveau du logiciel client et d'établir une bonne pratique de travail aux fins d'une meilleur compréhension par les utilisateurs du système. Elle s'applique au regard de tout document sous forme électronique qui est créé ou communiqué conformément à la présente norme. Cependant, dans le secteur de communication entre offices (d'office à office), l'office expéditeur et l'office destinataire peuvent se mettre d'accord pour appliquer d'autres règles de nommage des fichiers aux fins de leurs transactions. Dans ce cas, l'office destinataire en informe le Bureau international. La série de tableaux qui suit constitue la convention de nommage des fichiers et les logiciels clients devraient produire de manière automatique les suffixes et les extensions des fichiers en conséquence. Chacun de ces tableaux représente un niveau de la convention, suivie de tableaux présentant des exemples.

4.3.1 Tableaux

Tableau 1

Codes utilisés en fonction des descriptifs	
A	un seul caractère issu de la liste suivante : {ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz}
A…	toute combinaison d'au moins deux caractères issus de la liste suivante : {ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789}
AAA	toute combinaison de un, deux ou trois caractères issus de la liste suivante : {ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789}
NNNNNN	toute combinaison de six caractères issus de la liste suivante : {0123456789}

Tableau 2

Codes à utiliser à chaque fois		
A…	identifiant du déposant ou de l'office, ne peut pas dépasser 50 caractères	Obligatoire
-	séparateur (tiret)	
A…	nature du document *(voir le tableau 6)* ou du sous-document *(voir le tableau 7)*	
-	séparateur (tiret)	Optionnel
A	type de document *(voir le tableau 8)* dans le cas d'un fichier d'image	
NNNNNN	numéro de séquence du document, justifié à droite, avec des zéros à gauche pour remplir le vide	

.	séparateur (point)	Obligatoire
AAA	nature du fichier *(voir le tableau 5)*	

Tableau 3

Codes des fichiers externes référencés dans les documents		
A…	identifiant du déposant ou de l'office, ne peut pas dépasser 50 caractères	Obligatoire
-	séparateur (tiret)	
A…	nature du document *(voir le tableau 6)* ou du sous-document *(voir le tableau 7)*	
-	séparateur (tiret)	
A	type de document *(voir le tableau 8)*	
NNNNNN	numéro de séquence du type de document, justifié à droite, avec des zéros à gauche pour remplir le vide	
-	séparateur (tiret)	Optionnel
NNNNNN	numéro de la séquence de la page, justifié à droite, avec des zéros à gauche pour remplir le vide	
.	séparateur (point)	Obligatoire
AAA	nature du fichier *(voir le tableau 5)*	

Tableau 4

Fichiers non référencés dans les documents		
A…	identifiant du déposant ou de l'office, ne peut pas dépasser 50 caractères	Obligatoire
-	séparateur (tiret)	Optionnel
A…	nom du document tel que fourni par le déposant, ne peut pas dépasser 50 caractères	
.	séparateur (point)	Obligatoire
AAA	nature du fichier	

Tableau 5

Extensions de noms de fichiers acceptées	
txt	fichier en format texte, voir la section 3.1.1.3
xml	fichier en format XML, voir la section 3.1.1.1
tif	fichier en format TIFF, voir la section 3.1.3.1
jpg	fichier en format JFIF, voir la section 3.1.3.2
pdf	fichier en format PDF (Portable Document Format), voir la section 3.1.2
app	fichier en format ST.25, voir la section 3.1.1.2
zip	dossier contenant un ou plusieurs fichiers

Tableau 6

Types de documents et de paquets acceptés pour la phase initiale du dépôt électronique selon le PCT	
Type de document	*Code*
exemplaire original (paquet)	reco
copie pour l'office récepteur (paquet)	hoco
en-tête du paquet	pkgh
données du paquet	pkda
requête	requ
informations fournies par l'office récepteur	rrri
déclarations	decl
corps de la demande	appb

feuille de taxes	fees
pouvoir distinct original	poat
pouvoir général original	gpoa
copie du pouvoir général	cgpa
déclaration expliquant l'absence de signature	lacs
documents de priorité	pdoc
traduction de la demande	tapp
document en format de pré-conversion	dpcf
dépôt biologique	biod
listage des séquences	seql
listage des séquences ne faisant pas partie de la demande	seqn
tableau relatif au listage des séquences	seqt
autre tableau	tabx
accusé de réception	xmre
liste des demandes reçues	aprl
liste de diffusion	dspl
demande de modification	amnd
modification des données bibliographiques	bibc
correction d'office	exoc
correspondance	crsp
notification	noti
demande d'examen préliminaire international	dmnd
informations fournies par l'administration chargée de l'examen préliminaire international	idri
feuille de taxes selon le chapitre II	fee2
rapport de recherche internationale	isre
rapport d'examen préliminaire international	iper
opinion sur la recherche internationale	isop
traduction du rapport de recherche internationale	isrt
traduction du rapport d'examen préliminaire international	ipet
traduction de l'opinion sur la recherche internationale	isot
demande publiée	papp
types de documents propres à un office	[code de pays à 2 caractères]AA
tableau contenant plus de cinquante pages imprimées	mtbl

Tableau 7

Sous-documents acceptés pour la phase initiale du dépôt électronique du PCT	
Sous-documents	*Code*
description	desc
revendications	clms
abrégé	abst
dessins	draw

Tableau 8

Types de documents	
T	tableau
M	formule mathématique
C	structure ou formule chimique
S	listage des séquences
D	page de dessin (contient un ou plusieurs dessins par page d'image et une ou plusieurs pages d'image)
F	dessin (un seul dessin dans une seule page d'image)
I	image (contient une ou plusieurs pages d'image)
P	page du document

4.3.2 Identifiant du déposant

L'identifiant du déposant est choisi par le déposant avec ou sans l'aide du logiciel de dépôt. Le nom des fichiers contenus dans le paquet électronique de la demande internationale commence par le même identifiant. L'identifiant peut être un nom, un numéro d'enregistrement ou une autre chaîne de caractères signifiant quelque chose pour le déposant. L'identifiant peut être utilisé dans d'autres circonstances que pour le seul dépôt de la demande internationale comme par exemple pour nommer les fichiers électroniques présentés à l'office dans le cadre du traitement de la même demande internationale; il pourrait même être utilisé par le déposant dans le cadre de toutes ses demandes internationales. L'identifiant est placé en premier de telle sorte que tous les fichiers relatifs à un dépôt, à une demande internationale ou à un déposant apparaissent ensemble dans le répertoire.

Exemple de paquet du déposant contenant une demande internationale

Fichier	*Contenu*
dupont0340-pkda.xml	Paquet de données
dupont0340-requ.xml	Requête
dupont0340-fees.xml	Feuille de taxes
dupont0340-biod.xml	Dépôt biologique
dupont0340-decl-000001.xml	Première déclaration
dupont0340-decl-000002.xml	Deuxième déclaration
dupont0340-poat-000001.xml	Premier pouvoir
dupont0340-poat-I000001.tif	Première image du premier pouvoir
dupont0340-poat-I000002.tif	Deuxième image du premier pouvoir
dupont0340-poat-000002.xml	Deuxième pouvoir
dupont0340-poat-I000003.tif	Première image du deuxième pouvoir
dupont0340-lacs-I000001.tif	Premier manque de signature
dupont0340-lacs-I000002.tif	Deuxième manque de signature
dupont0340-seql.app	Listage des séquences (ST.25)
dupont0340-appb.xml	Demande
dupont0340-appb-C000001.tif	Première structure chimique, format TIFF
dupont0340-appb-C000001.cdx	Première structure chimique, format ChemDraw
dupont0340-appb-C000001.mol	Première structure chimique, format MOL
dupont0340-appb-M000001.tif	Première formule mathématique, format TIFF

dupont0340-appb-M000002.tif	Deuxième formule mathématique, format TIFF
dupont0340-appb-T000001.tif	Premier tableau, format TIFF
dupont0340-appb-T000002-000001.tif	Deuxième tableau, première page, format TIFF
dupont0340-appb-T000002-000002.tif	Deuxième tableau, deuxième page, format TIFF

4.3.3 Identifiant de l'office

L'identifiant de l'office est défini par celui-ci avec ou sans l'aide de son système. Le nom de chaque fichier doit commencer par 'pct|code RO|numéro de la demande', comme par exemple : 'pctib2004012345'.

Exemple de paquet d'office récepteur contenant un exemplaire original (pctib2004012345-reco.wsp)

Fichier	*Contenu*
pctib2004012345-pkda.xml	Paquet de données
pctib2004012345-requ.xml	Requête
pctib2004012345-rrri.xml	Informations apportées par l'office récepteur
pctib2004012345-fees.xml	Feuille de taxes
pctib2004012345-biod.xml	Dépôt biologique
pctib2004012345-decl-000001.xml	Première déclaration
pctib2004012345-decl-000002.xml	Deuxième déclaration
pctib2004012345-poat-000001.xml	Premier pouvoir
pctib2004012345-poat-I000001.tif	Première image du premier pouvoir
pctib2004012345-poat-I000002.tif	Deuxième image du premier pouvoir
pctib2004012345-poat-000002.xml	Deuxième pouvoir
pctib2004012345-poat-I000003.tif	Première image du deuxième pouvoir
pctib2004012345-lacs-I000001.tif	Premier manque de signature
pctib2004012345-lacs-I000002.tif	Deuxième manque de signature
pctib2004012345-seql.app	Listage des séquences (ST.25)
pctib2004012345-exoc.xml	Correction *ex-officio*
pctib2004012345-appb.xml	Demande
pctib2004012345-appb-C000001.tif	Première structure chimique, format TIFF
pctib2004012345-appb-M000001.tif	Première formule mathématique, format TIFF
pctib2004012345-appb-M000002.tif	Deuxième formule mathématique, format TIFF
pctib2004012345-appb-T000001.tif	Premier tableau, format TIFF
pctib2004012345-appb-T000002-000001.tif	Deuxième tableau, première page, format TIFF
pctib2004012345-appb-T000002-000002.tif	Deuxième tableau, deuxième page, format TIFF

5. TRANSMISSION

Le paquet de documents constitutifs de la demande internationale peut être transmis par des voies sécurisées ou non, selon le type de paquet. La présente partie décrit le protocole à suivre ainsi que les combinaisons paquet/transmission autorisées dans les secteurs de communication entre le déposant et l'office (phase internationale),

entre offices, et des offices désignés. Bien qu'il soit question d'autres secteurs dans la présente norme (voir la section 2.3), les combinaisons transmission/paquet autorisées peuvent être classées selon les trois secteurs susmentionnés.

5.1 Protocole sur l'interopérabilité en matière de dépôt électronique

La présente section décrit le protocole sur la couche de transmission entre les clients et le serveur et prévoit un cadre pour la conduite à suivre à la fois par le client et par le serveur.

Le protocole est conçu pour supporter des communications de type HTTP à travers un tunnel SSL (ou TLS) pour toutes les formes de dépôt électronique fondées sur une ICP.

Vue d'ensemble du protocole de transmission en ligne :

a) Permet la transmission des demandes volumineuses grâce à plusieurs requêtes "POST" HTTP afin de répondre aux priorités liées à la sécurité et à l'intégrité

b) Détection et correction efficace des erreurs

c) Permet aux offices de s'assurer de la taille optimale des échanges

On remarquera que ceci est un protocole appelé à évoluer, du fait de systèmes de production en développement dans un certain nombre d'offices de propriété industrielle, et qu'ainsi des révisions seront probablement réalisées à terme.

5.1.1 Principes

Le protocole sur l'interopérabilité répond aux principes suivants :

a) Les communications entre le client et le serveur sont toutes réalisées sous forme de requêtes HTTP "POST" initiées par le client.

b) Les requêtes "POST", et les réponses y relatives, utilisent toutes les mêmes en-têtes de gestion des échanges suivi d'un bloc de données optionnelles.

c) Les transmissions utilisent toutes le mécanisme de division pour séparer des blocs de données afin de les transformer en paquets gérables grâce à un protocole qui permet de faire des essais.

5.1.2 Protocole sur les couches du système applicatif pour la demande

Au plus haut niveau applicatif, le protocole prévoit que le logiciel client et le serveur suivent les cinq actions suivantes :

a) Début de la transaction

b) Envoi de l'en-tête du paquet

c) Envoi du paquet de données

d) Demande d'un accusé de réception

e) Fin de la transaction

Entre le début et la fin de l'échange, trois types de WASPs sont échangés entre le logiciel client et le serveur, à savoir

i) L'en-tête du paquet contient les informations essentielles pour le traitement initial relatif à l'identification de la demande envoyée. Il s'agit d'un WASP qui contient l'en-tête du paquet en format XML.

ii) Le paquet de données contient les informations pour envoyer une demande. C'est un WASP qui comprend plusieurs types de fichiers.

iii) L'accusé de réception est une acceptation de la demande envoyée. Le contenu de cet accusé de réception (données en format XML avec un certificat optionnel en format PDF ou TIFF lisible par un être humain), qui est signé par l'office récepteur, est défini dans l'appendice I.

5.1.2.1 Utilisation du tunnel SSL (ou TLS) pour la demande

Ces actions sont toutes mises en œuvre à travers le tunnel SSL (ou TLS) établi avant d'entamer l'action "Début de la transaction". Le tunnel SSL (ou TLS), construit en utilisant à la fois l'authentification du client et celle du serveur, peut être fermé à la fin de l'échange. Si une série de transmissions est prévue, le tunnel SSL (ou TLS) peut aussi être laissé ouvert et n'être fermé qu'à la fin des échanges. Le tunnel SSL utilise la version 3.0 du protocole SSL.

L'office récepteur a tout pouvoir quant au choix du protocole à utiliser, SSL ou TLS.

Lorsque l'authentification du client est réalisée par le serveur, en plus de la fonction fondée sur la version 3.0 du protocole SSL (ou le protocole TLS) qui confirme le fait que le certificat numérique transmis par le logiciel client est effectivement délivré par l'autorité de certification reconnue, la déconnexion du tunnel SSL (ou TLS) peut être contrôlée par le serveur en fonction de la procédure suivante :

a) Les informations relatives au(x) certificat(s) numérique(s) du déposant ou de l'agent obtenu(s) auparavant par l'office récepteur sont conservées dans le serveur.

b) Au moment de l'authentification du client par la version 3.0 du protocole SSL (ou le protocole TLS), le serveur vérifie si les informations relatives au certificat numérique du déposant ou de l'agent envoyé par le logiciel client se trouvent dans les informations conservées dans le serveur conformément à l'étape a) mentionnée ci-avant.

c) Si le résultat de la vérification effectuée selon l'étape b) est négatif, le serveur déconnecte le tunnel SSL (ou TLS).

Afin de mener à bien la fonction précédemment décrite, l'office récepteur peut conduire une procédure de pré-enregistrement afin d'obtenir auparavant, de sa propre initiative ou à l'initiative du déposant ou de l'agent, les informations suivantes : i) informations (ou mises à jour) relatives au(x) certificat(s) numérique(s) employé(s) par le déposant ou l'agent; et, si le besoin s'en fait sentir, ii) informations supplémentaires relatives au déposant ou à l'agent.

Le présent protocole prévoit que chaque échange individuel doit toujours être suivi d'un accusé de réception individuel, sauf dans le cas où le tunnel SSL (ou TLS) est déconnecté durant la procédure précédemment décrite.

5.1.2.2 Actions prévues par le système applicatif pour la demande

Commencer la session SSL (ou TLS) (voir Figure 5)

Étape 0 : Début de la transaction

Action du client :

Obtenir des informations sur l'échange

Réponse du serveur :

Renvoyer les valeurs dans les éléments de l'en-tête de gestion de la transaction (*transaction_id, max_division_size*)

transaction_id est un identifiant unique attribué par le serveur et qui associe toutes les transactions liées au dépôt de la demande

max_division_size est le nombre maximum d'octets permis par le serveur pour la taille de chaque division

Étape 1 : Envoi de l'en-tête du paquet

Action du client :

Envoi de l'en-tête du paquet

Réponse du serveur :

a) OK

b) Erreur (opération annulée, retourner à l'étape 0)

c) Paquet déjà reçu; aller à l'étape 3 afin de demander un accusé de réception.

Après avoir reçu la dernière division du WASP contenant l'en-tête du paquet, le serveur doit vérifier la signature du WASP. Si la signature n'est pas admissible (ce qui est le cas, par exemple, lorsque sa date d'expiration est dépassée), le code de réponse de la demande (ou ARC) demeure valable mais le serveur saisit automatiquement l'erreur et appose un message y relatif sur l'accusé de réception.

Étape 2 : Envoi du paquet de données

Action du client :

Envoi du paquet de données

Réponse du serveur :

a) OK

b) Erreur (opération annulée, retourner à l'étape 0)

Après avoir reçu la dernière division du WASP contenant le paquet de données, le serveur doit vérifier la signature du WASP et comparer le message condensé du paquet non-signé au condensé du message prévu dans l'en-tête du paquet tel qu'à l'étape 1 de la transaction, avant de renvoyer l'ARC au client. Si les deux conditions sont réunies, le serveur doit renvoyer un ARC indiquant OK. Si les données hachées dans l'en-tête du paquet et le WAD du paquet de données ne correspondent pas, l'ARC doit être FFF7. Si la signature n'est pas admissible (lorsque sa date d'expiration est dépassée par exemple), l'ARC demeure valable mais le serveur saisit automatiquement l'erreur et appose un message y relatif sur l'accusé de réception.

Étape 3 : Demande d'un accusé de réception

Action du client :

Envoi de la demande

Réponse du serveur :

a) OK (l'objet de l'accusé de réception est inclus dans la réponse)

b) Erreur (opération annulée, retourner à l'étape 0)

Étape 4 : Fin de la transaction.

Action du client :

Envoyer au serveur, à la fin de la transmission, un accusé de réception qui contient, le cas échéant, des informations sur les problèmes auxquels le client est confronté.

Réponse du serveur :

a) OK

b) Erreur (le client peut ignorer cette réponse)

Fermer la session SSL (ou TLS)

Dans tous les cas prévus dans le tunnel SSL (ou TLS), le présent protocole prévoit que chaque échange individuel soit accepté par un accusé de réception individuel.

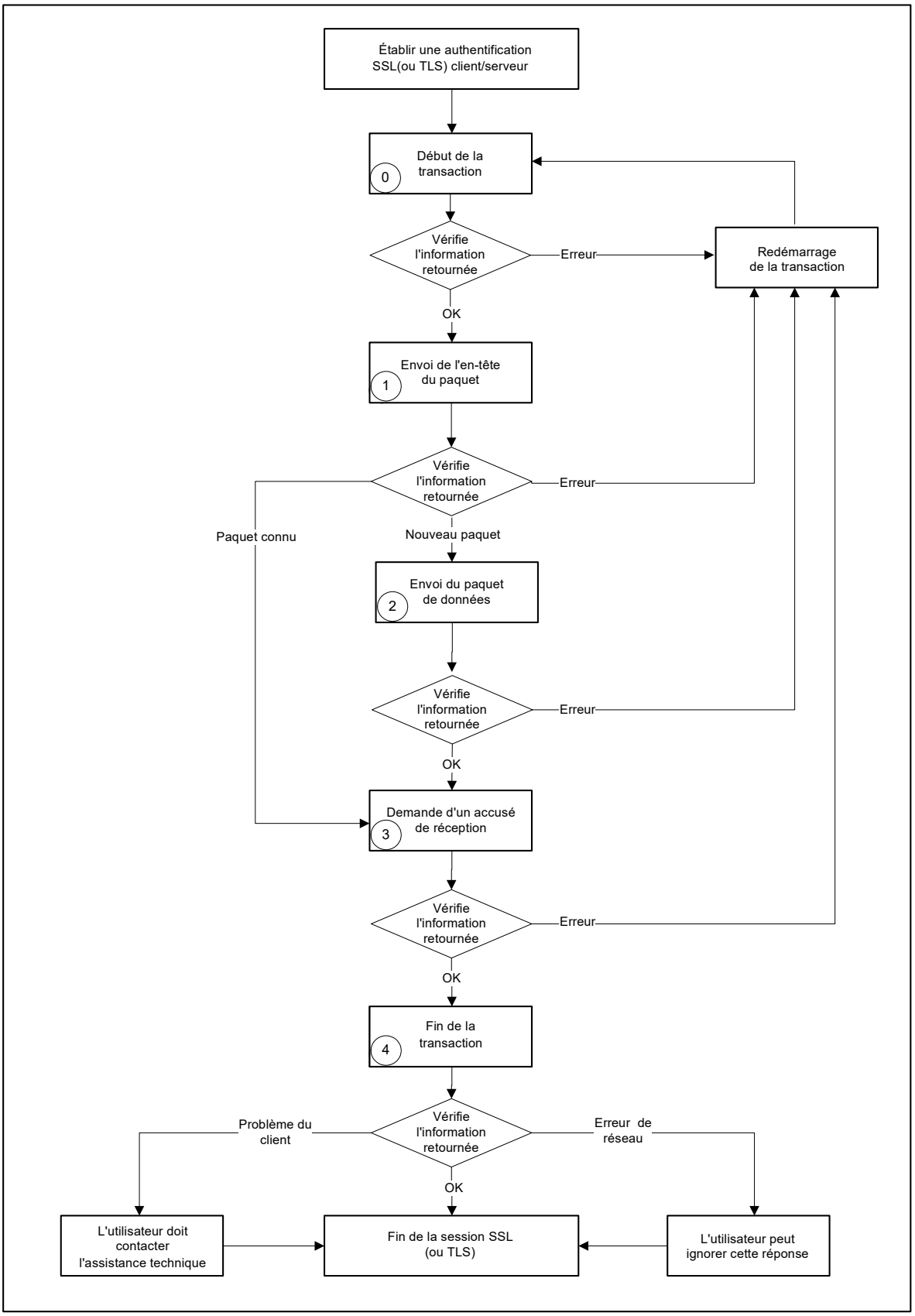


Figure 5 – Conduite à suivre selon le protocole sur le système applicatif en ce qui concerne la demande

5.1.3 Protocole sur les couches du système applicatif en matière de notification

Au plus haut niveau du système applicatif en matière de notification, le protocole prévoit que le logiciel client et le serveur suivent les cinq actions[9] suivantes :[10]

a) Début de la transaction

b) Envoi de l'en-tête du paquet (pour le notification, il s'agit de la liste de distribution ou de la liste de réception de la demande)[11]

c) Envoi du paquet de données (pour le notification, il s'agit de la liste de distribution ou de la liste de réception de la demande)[12]

d) Demande d'un accusé de réception (pour le notification, il s'agit de la liste de distribution ou de la liste de réception de la demande)[12]

e) Fin de la transaction

Entre le début et la fin de l'échange, deux types de WASPs et un type de C-WASP sont envoyés entre le logiciel client et le serveur, à savoir :

i) L'en-tête du paquet envoyé par le logiciel client contient les informations essentielles pour le traitement initial relatif à l'identification de la demande pour une notification. Il s'agit d'un WASP qui contient l'en-tête du paquet en format XML. Cela s'applique à la requête du logiciel client au serveur.

ii) L'en-tête du paquet envoyé par le serveur contient des informations sommaires concernant la notification (telles que le numéro d'envoi et le nombre de notifications à envoyer) pour le traitement initial relatif à l'identification de la demande pour une notification. Il s'agit d'un WASP qui contient l'en-tête du paquet en format XML. Cela s'applique à la réponse du serveur au logiciel client.

iii) Le paquet de données contient les informations contenues dans la notification qui est envoyée. Il s'agit d'un WASP qui comprend un ou plusieurs WASPs.

5.1.3.1 Utilisation du tunnel SSL (ou TLS) pour la notification

Voir la section 5.1.2.1, "Utilisation du tunnel SSL (ou TLS) pour la demande".

---

[9] L'office peut informer le déposant de l'existence de notifications avant ces cinq actions par le biais d'autres moyens de communication tels que le courriel.

[10] Le présent protocole peut être utilisé pour transmettre le répertoire d'envoi, le répertoire de réception de la demande et la notification. La transmission du répertoire d'envoi, du répertoire de réception de la demande et de la notification est laissée à l'appréciation de l'office. Le répertoire d'envoi contient des numéros d'envoi correspondant aux notifications envoyées par l'office au déposant. Le répertoire de réception de la demande contient des numéros de demandes correspondant aux documents de demandes reçus par l'office en provenance du déposant.

[11] Le serveur utilise la valeur de l'attribut "transaction-type" (voir la section 5.1.4) afin d'identifier le type de document demandé, p. ex. notification, répertoire d'envoi, répertoire de réception de la demande.

5.1.3.2 Actions prévues par le système applicatif pour la notification

Commencer la session SSL (ou TLS) (voir Figure 6)

Étape 0 : Début de la transaction

Action du client :

Obtenir des informations sur l'échange

Réponse du serveur :

Renvoyer les valeurs dans les éléments de l'en-tête de gestion de la transaction (*transaction_id, max_division_size*)

transaction_id est un identifiant unique attribué par le serveur et qui associe toutes les transactions liées à l'envoi de la notification

max_division_size est le nombre maximum d'octets permis par le serveur pour la taille de chaque division

Étape 1 : Envoi de l'en-tête du paquet

Action du logiciel client :

Envoi d'une demande pour l'en-tête du paquet (Contient le WASP de l'en-tête du paquet pour une demande de notification)

Réponse du serveur :

a) OK (La réponse comprend le WASP de l'en-tête du paquet contenant des informations sommaires sur le notification telles que le numéro d'envoi ou le nombre de notification)[12]

b) Erreur (opération annulée, retourner à l'étape 0)

Après avoir reçu la dernière division du WASP contenant l'en-tête du paquet, le serveur doit vérifier la signature du WASP. Si la signature n'est pas admissible (ce qui est le cas, par exemple, lorsque sa date d'expiration est dépassée), la valeur du code de réponse de la demande (ou ARC) est FFF6.

Si le nombre de notifications pouvant être envoyées dans l'en-tête de la réponse du serveur est "0(zero)" (aucune notification susceptible d'être envoyée), aller à l'étape 4.

Étape 2 : Envoi du paquet de données

Action du logiciel client :

Envoi du paquet de données

Réponse du serveur :

a) OK (la réponse contient le C-WASP qui consiste en un ou plusieurs WASPs)

[12] Si le C-WASP contient plusieurs WASPs, cette information figure dans l'en-tête du paquet contenant la notification.

b) Erreur (opération annulée, retourner à l'étape 0)

Étape 3 : Demande d'un accusé de réception

Action du logiciel client :

Envoi de l'accusé de réception

Réponse du serveur :

a) OK

b) Erreur (opération annulée, retourner à l'étape 0)

Étape 4 : Fin de la transaction.

Action du logiciel client :

Envoyer au serveur, à la fin de la transmission, un accusé de réception qui contient des informations sur les problèmes auxquels le client est confronté.

Réponse du serveur :

a) OK

b) Erreur (le client peut ignorer cette réponse)

Fermer la session SSL (ou TLS)

Dans tous les cas prévus dans le tunnel SSL (ou TLS), le présent protocole prévoit que chaque échange individuel soit accepté par le logiciel client en envoyant un accusé de réception au serveur.

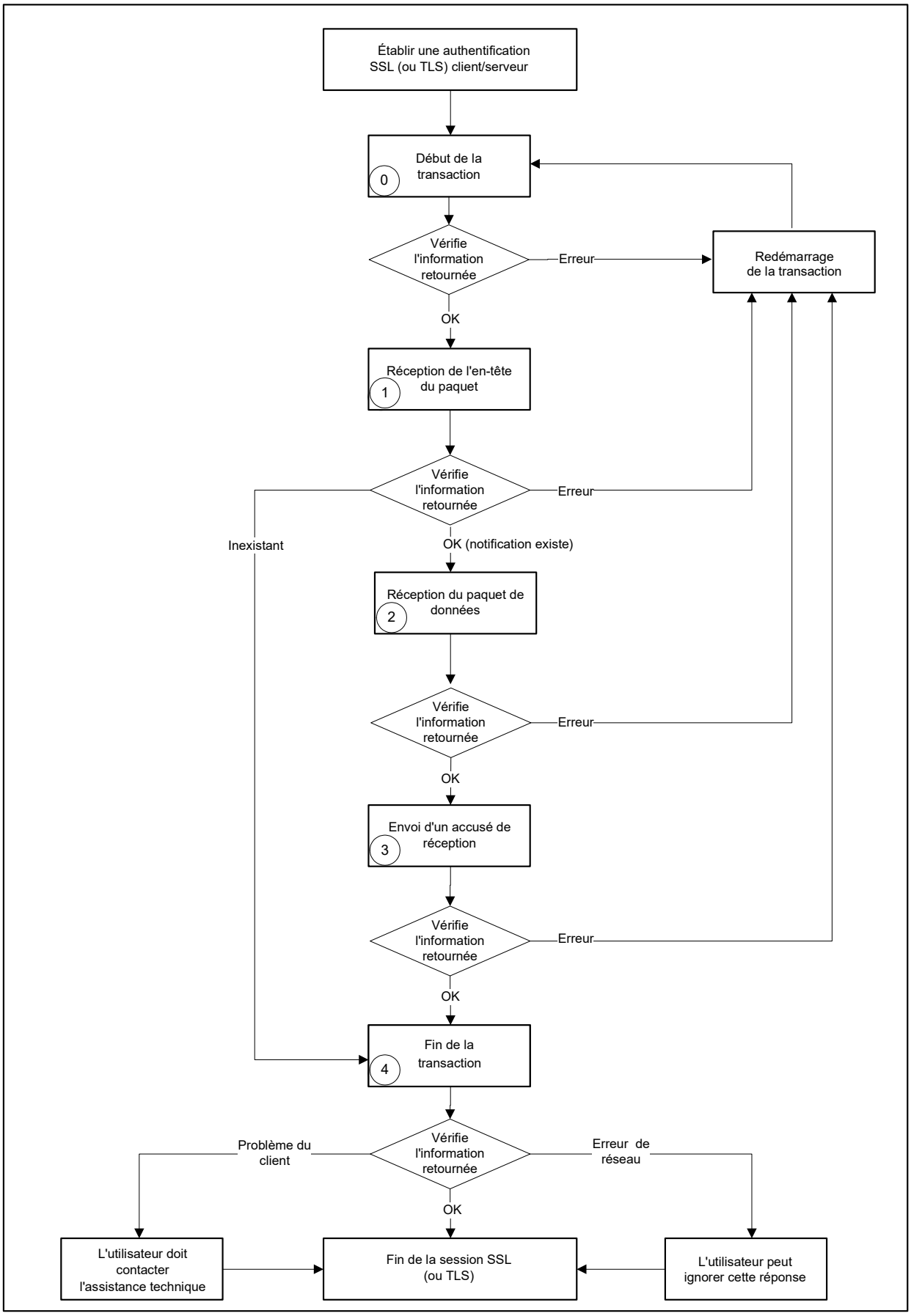


Figure 6 – Conduite à suivre selon le protocole de niveau applicatif pour la notification

5.1.4 Éléments de l'en-tête de gestion des échanges

Les éléments suivants, qui ont tous une taille fixe, sont inclus dans toutes les requêtes "POST" et les réponses y relatives. Les paramètres non utilisés des éléments de l'en-tête sont représentés par un espace (ASCII '20').

Élément	division_hash
Valeurs	représentation ASCII majuscule hexadécimale d'un indice de hachage de 160-bit
Taille du corps d'entité	40 octets (40 x 8 bit caractères)
Description	Hachage de la présente division, grâce à l'algorithme SHA-1 (il y aura un espace lorsque l'algorithme SHA-1 n'est pas utilisé).

Élément	protocol_version
Valeurs	Unique
Taille du corps d'entité	4 octets (caractères ASCII 4 x 8bit)
Description	Un identifiant unique pour la version du protocole utilisé pour créer l'échange de données (p. ex. 0100 pour la version 1.0). Les deux premiers octets sont réservés au numéro identifiant la version principale et les deux derniers sont réservés au numéro identifiant les versions révisées de cette version.

Élément	transaction_type	
Valeurs	pbeg, ebeg,	
	pend, eend	
	ehdr, phdr,	
	edat, pdat,	
	erct, prct,	
	ephn, pphn	Get package header for notification
	epdn, ppdn	Get package data for notification
	ercn, prcn	Send receipt check notice for notification
	ephd, pphd	Get package header for dispatch list
	epdd, ppdd	Get package data for dispatch list
	ercd, prcd	Send receipt check notice for dispatch list
	epha, ppha	Get package header for application receipt list
	epda, ppda	Get package data for application receipt list
	erca, prca	Send receipt check notice for application receipt list
	ASCII miniscule 7-bit ISO 646 e- signifie chiffré, p- signifie texte clair	
Taille du corps d'entité	4 octets	
Description	Élément de l'en-tête de l'échange qui identifie la nature des données transmises La valeur commençant par la lettre d ou z n'est pas disponible.	

Remarque : la valeur commençant par une lettre d ou z est réservée pour les demandes nationales ou d'autres types d'échanges.

Élément	transaction_id

Valeurs	Unique
Taille du corps d'entité	36 octets
Description	Un identifiant unique assigné par le serveur et associé à tous les échanges liés à l'envoi de la demande. Pour l'événement "Début Transaction", celui-ci est blanc (ASCII x'20').

Élément	reserved_use
Valeurs	Reservée à l'usage national (p. ex. la date et l'heure du serveur : YYYYMMDDHHMMSS)
Taille du corps d'entité	32 octets
Description	Cette zone de données est laissée à la discrétion de chaque office récepteur. (p. ex. pour informer un client de l'horaire du serveur de l'office récepteur).

Élément	total_bytes
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche (p. ex. 0000000123456789)
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	La taille totale, en octets, des objets envoyés (le WASP contenant l'en-tête du paquet, le WASP contenant le paquet de données et le WASP contenant l'accusé de réception).

Élément	division_size
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche (p. ex. 0000000123456789)
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	La taille, en octets, de la composante "données" de l'objet transféré

Élément	division_offset
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche (p. ex. 0000000123456789)
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	- Valeur représentant le point de départ des données au sein de l'objet transféré - Division_offset commence à 0

<table>
<tr><td>Élément</td><td colspan="2">division_response_code</td></tr>
<tr><td>Valeurs</td><td colspan="2"><table>
<tr><th>Division RCs</th><th>Signification</th></tr>
<tr><td>0000</td><td>OK</td></tr>
<tr><td>FFFF</td><td>Erreur générale</td></tr>
<tr><td>FFFE</td><td>Renvoyer</td></tr>
<tr><td>FFFD</td><td>Attendre</td></tr>
<tr><td>FFFC</td><td>Erreur de séquence du protocole</td></tr>
</table>4 octets (caractères ASCII 4 x 8bit)</td></tr>
<tr><td>Taille du corps d’entité</td><td colspan="2">4 octets</td></tr>
<tr><td>Description</td><td colspan="2">Le code de retour du serveur ou du client est utilisé pour gérer le mécanisme de division</td></tr>
</table>

<table>
<tr><td>Élément</td><td colspan="2">application_response_code</td></tr>
<tr><td>Valeurs</td><td colspan="2"><table>
<tr><th>Application RCs</th><th>Signification</th></tr>
<tr><td>0000</td><td>OK</td></tr>
<tr><td>FFFF</td><td>Erreur générale</td></tr>
<tr><td>0001</td><td>OK, paquet connu</td></tr>
<tr><td>0002</td><td>OK, nouveau paquet</td></tr>
<tr><td>0003</td><td>OK, Inexistant</td></tr>
<tr><td>1000</td><td>En attente</td></tr>
<tr><td>FFFB</td><td>Problème du client</td></tr>
<tr><td>FFFA</td><td>Erreur de réseau</td></tr>
<tr><td>FFF9</td><td>Erreur de version du protocole</td></tr>
<tr><td>FFF8</td><td>La valeur de hachage de la division dans la transaction de gestion de l’en-tête est une erreur.</td></tr>
<tr><td>FFF7</td><td>Les valeurs de hachage dans le paquet de l’en-tête et le WAD du paquet de données ne correspondent pas..</td></tr>
<tr><td>FFF6</td><td>La signature n’est pas valable (par exemple, en raison d’une erreur de vérification de la signature ou une validation de données expirées).[13]</td></tr>
</table>4 octets (caractères ASCII 4 x 8bit)</td></tr>
<tr><td>Taille du corps d’entité</td><td colspan="2">4 octets</td></tr>
<tr><td>Description</td><td colspan="2">Code de retour du serveur ou du client utilisé pour gérer les étapes d’envoi de la demande</td></tr>
</table>

[13] Ce code s’applique lorsque le serveur ne peut pas établir l’authentication prévue dans la fonction “Obtenir l’en-tête du paquet”.

Élément	encoding_method		
Valeurs		*Demande RCs*	*Signification*
		UTF8	UNICODE UTF8
		SJIS	UNICODE Shift-JIS
		KS X	UNICODE KS X 1001
	caractères ASCII 4 x 8bit		
Taille du corps d'entité	4 octets		
Description	Plan de chiffrement pour la traduction des messages d'erreur.		

Élément	error_message
Valeurs	UNICODE UTF8, UNICODE Shift-JIS, UNICODE KS X 1001
Taille du corps d'entité	256 octets (caractères 256 x 8bit)
Description	Texte optionnel expliquant pourquoi les codes de réponse sont erronés. Si un message erroné est nécessaire à la fois pour les codes de réponse de la division et de la demande, ces derniers doivent être liés. Chaque serveur choisit l'un des plans de chiffrement spécifiés pour traduire le message d'erreur dans un format lisible par un être humain.

Élément	Algorithm_name
Valeurs	ASCII avec remplissage d'espaces sur la droite
Taille du corps d'entité	10 octets (caractères 10 x 8bit)
Description	le nom de l'algorithme utilisé, par exemple : SHA-256

Élément	division_hash2_length
Valeurs	ASCII avec remplissage de zéros sur la gauche
Taille du corps d'entité	4 octets (caractères 4 x 8bit)
Description	length of division_hash2.

Élément	division_hash2
Valeurs	représentation ASCII majuscule hexadécimale
Taille du corps d'entité	variable (taille définie par division_hash2_length)
Description	valeur de hachage calculée en utilisant l'algorithme défini par le nom d'algorithme

5.1.5 Éléments relatifs aux données de gestion des échanges

Élément	max_division_size
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	Nombre maximum d'octets permis par division
Exemple	0000000000008192 (8 kilo-octets)

5.1.6 Paramètres du serveur

Élément	server_timeout
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche (p. ex. 0000000123456789)
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	Le temps, en secondes, avant que le serveur ne comprenne qu'un client n'est plus connecté au réseau et que l'échange est interrompu.
Exemple	0000000000000120 (2 minutes)

Remarque : chaque office détermine la valeur pour server_timeout au niveau du protocole.

5.1.7 Paramètres du client

Élément	client_preferred_division_size
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	Nombre choisi d'octets par division
Exemple	0000000000004096 (8 k)

Élément	client_retry_limit
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	Nombre de fois que le client doit renvoyer la division avant d'abandonner définitivement l'échange
Exemple	0000000000000005 (5 tentatives)

Remarque : le nombre maximal d'attributs pour client_retry_limit est NN (16 fois). Lorsqu'un serveur effectue 16 tentatives, la transmission peut être terminée.

Élément	client_retry_wait
Valeurs	ASCII numérique avec remplissage de zéros sur la gauche (p. ex. 0000000123456789)
Taille du corps d'entité	16 octets (caractères 16 x 8bit)
Description	Le temps, compté en secondes, que le client doit attendre avant de faire un nouvel essai
Exemple	0000000000000005 (5 secondes)

Remarque : il revient au logiciel de déterminer la valeur pour client_retry_wait.

5.1.8 Mécanisme de division

Les données qui transitent entre le client et le serveur sont divisées en paquets de données gérables qui, avec l'en-tête de gestion des échanges, forment ce que l'on appelle des divisions. Sous le contrôle du client, la taille de ces divisions peut varier au fur et à mesure des échanges. Ceci permet la mise en œuvre d'un mécanisme de contrôle des

communications qui peut être utilisé pour surmonter les difficultés de transmission via l'Internet.

La taille initiale du message contenant une division de données est établie par rapport au plus petit des messages suivants :

a) max_division_size renvoyé par le serveur en tant que réponse à la demande d'ouverture de l'échange

b) client_preferred_division_size placé dans les paramètres d'initialisation du client

Le logiciel client crée une ou plusieurs divisions à partir de l'en-tête de gestion de la transmission et d'un message de données. Comme chaque division est envoyée dans un ordre différent au serveur, celui-ci vérifie si la transmission est complète en calculant la valeur de hachage de la division.

5.1.8.1 Calculer la valeur du hachage de la division

Le hachage est calculé sur la base de tous les champs de l'en-tête ainsi que de tous les messages de données. Le hachage, qui est calculé en utilisant l'algorithme SHA-1, représente le premier élément de chaque division. Toutefois, si ce n'est pas l'algorithme SHA-1 qui est utilisé, tout l'espace est attribué à division_hash et la valeur du hachage calculée en utilisant l'algorithme défini par algorithm_name est attribuée à division_hash2.

Le serveur doit vérifier la version du protocole avant d'examiner la valeur de hachage afin d'éviter de rejeter un paquet du fait qu'il n'est pas valide, au cas où une nouvelle version du protocole adopterait un algorithme de hachage différent.

Les champs suivants de la requête "POST" ou de la réponse HTTP sont ainsi inclus dans le calcul du hachage :

Nom	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	4	4	36	32	16	16	16	4	4	4	256	???

5.1.9 Protocole sur les niveaux du processus

Les transactions décrites dans cette section sont illustrées plus loin dans les figures 7 à 12.

5.1.9.1 Début de la transaction

La requête POST envoyée par le client pour commencer la transaction contient la dernière version du protocole acceptable par le client. Si le serveur peut utiliser la version fournie par le client, il communique avec le client conformément aux règles de cette version du protocole et utilise le numéro d'identification de cette version pour tous les messages de réponse. Si le serveur ne peut pas utiliser la version du protocole spécifiée par le client, le code de réponse de la demande doit indiquer que la version du protocole n'est pas la bonne et le numéro d'identification de la version envoyée dans le

message de réponse doit être la dernière version du protocole acceptable par le serveur. Le client doit pouvoir s'appuyer sur des versions antérieures.

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	pbeg	espace	???	0	0	0	0	0	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	16
Valeur	X	0100	pbeg	nouvelle id	???	16	16	0	0	0	???	???	???

Message de données : max_division_size (16 octets)

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pbeg	espace	???	0	0	0	0	0	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pbeg	nouvelle id	???	16	16	0	0	0	???	???	???	???	???	x

Message de données : max_division_size (16 octets)

5.1.9.2 Envoyer l'en-tête du paquet

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	phdr	tranid	???	X	Y	Z	0	0	???	espace	pkghdr

Message de données : WASP contenant l'en-tête du paquet

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	phdr	tranid	???	0	0	0	a	b	???	espace	aucune

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	phdr	tranid	???	x	y	z	0	0	???	espace	pkghdr	???	???	x

Message de données : WASP contenant l'en-tête du paquet

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	phdr	tranid	???	16	16	0	a	b	???	espace	aucun	???	???	x

5.1.9.3 Envoyer le paquet de données

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	pdat	tranid	???	x	y	z	0	0	???	espace	pkgdata

Message de données : WASP contenant le paquet de données

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	pdat	tranid	???	0	0	0	a	b	???	espace	aucune

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pdat	tranid	???	x	y	z	0	0	???	espace	pkgdata	???	???	x

Message de données : WASP contenant le paquet de données

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pdat	tranid	???	0	0	0	a	b	???	espace	aucun	???	???	x

5.1.9.4 Obtenir un accusé de réception

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	prct	tranid	???	0	0	0	???	0	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	prct	tranid	???	x	y	z	???	0	???	espace	reçu

Message de données : WASP contenant l'accusé de réception

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prct	tranid	???	0	0	0	???	0	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prct	tranid	???	x	y	z	???	0	???	espace	reçu	???	???	x

Message de données : WASP contenant l'accusé de réception

5.1.9.5 Fin de la transaction

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	en attente	tranid	???	0	0	0	0	0	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	en attente	tranid	???	0	0	0	a	b	???	???	aucune

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pend	tranid	???	0	0	0	0	0	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pend	tranid	???	0	0	0	a	b	???	???	aucun	???	???	x

5.1.9.6 Obtenir l'en-tête du paquet pour la notification

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	pphn	tranid	???	X	Y	Z	a	b	???	espace	pkghdr

Message de données : WASP contenant l'en-tête du paquet

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	pphn	tranid	???	X	Y	Z	a	b	???	espace	pkghdr

Message de données : WASP contenant l'en-tête du paquet

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pphn	tranid	???	x	y	z	a	b	???	espace	pkghdr	???	???	x

Message de données : WASP contenant l'en-tête du paquet

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pphn	tranid	???	x	y	z	a	b	???	espace	pkghdr	???	???	x

Message de données : WASP contenant l'en-tête du paquet

5.1.9.7 Obtenir le paquet de données pour la notification

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	ppdn	tranid	???	0	0	0	a	b	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	ppdn	tranid	???	x	y	Z	0	0	???	espace	pkgdata

Message de données : C-WASP contenant un WASP

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppdn	tranid	???	0	0	0	a	b	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppdn	tranid	???	x	y	z	0	0	???	espace	pkgdata	???	???	x

Message de données : C-WASP contenant un WASP

5.1.9.8 Envoyer l'accusé de réception pour la notification

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	prcn	tranid	???	0	0	0	0	0	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	prcn	tranid	???	0	0	0	a	b	???	espace	aucune

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prcn	tranid	???	0	0	0	0	0	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prcn	tranid	???	0	0	0	a	b	???	espace	aucun	???	???	x

5.1.9.9 Obtenir l'en-tête du paquet pour la liste de distribution

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	pphd	tranid	???	X	Y	Z	a	b	???	espace	pkghdr

Message de données : WASP contenant l'en-tête du paquet

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	pphd	tranid	???	X	Y	Z	a	b	???	espace	pkghdr

Message de données : WASP contenant l'en-tête du paquet

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pphd	tranid	???	x	y	z	a	b	???	espace	pkghdr	???	???	x

Message de données : WASP contenant l'en-tête du paquet

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	pphd	tranid	???	x	y	z	a	b	???	espace	pkghdr	???	???	x

Message de données : WASP contenant l'en-tête du paquet

5.1.9.10 Obtenir le paquet de données pour la liste de distribution

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	ppdd	tranid	???	0	0	0	a	b	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	ppdd	tranid	???	x	y	z	0	0	???	espace	pkgdata

Message de données : C-WASP contenant un WASP

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppdd	tranid	???	0	0	0	a	b	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppdd	tranid	???	x	y	z	0	0	???	espace	pkgdata	???	???	x

Message de données : C-WASP contenant un WASP

5.1.9.11 Envoyer l'accusé de réception pour la liste de distribution

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	prcd	tranid	???	0	0	0	0	0	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	prcd	tranid	???	0	0	0	a	b	???	espace	aucune

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prcd	tranid	???	0	0	0	0	0	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prcd	tranid	???	0	0	0	a	b	???	espace	aucun	???	???	x

5.1.9.12 Obtenir l'en-tête du paquet pour la liste de réception de la demande

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	ppha	tranid	???	X	Y	Z	a	b	???	espace	pkghdr

Message de données : WASP contenant l'en-tête du paquet

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	ppha	tranid	???	X	Y	Z	a	b	???	espace	pkghdr

Message de données : WASP contenant l'en-tête du paquet

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppha	tranid	???	x	y	z	a	b	???	espace	pkghdr	???	???	x

Message de données : WASP contenant l'en-tête du paquet

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppha	tranid	???	x	y	z	a	b	???	espace	pkghdr	???	???	x

Message de données : WASP contenant l'en-tête du paquet

5.1.9.13 Obtenir le paquet de données pour la liste de réception de la demande

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	ppda	tranid	???	0	0	0	a	b	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	???
Valeur	X	0100	ppda	tranid	???	x	y	z	0	0	???	espace	pkgdata

Message de données : C-WASP contenant un WASP

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppda	tranid	???	0	0	0	a	b	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	ppda	tranid	???	x	y	z	0	0	???	espace	pkgdata	???	???	x

Message de données : C-WASP contenant un WASP

5.1.9.14 Envoyer l'accusé de réception pour la liste de réception de la demande

Requête POST

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	prca	tranid	???	0	0	0	0	0	???	espace	aucune

Réponse

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0
Valeur	X	0100	prca	tranid	???	0	0	0	a	b	???	espace	aucune

Requête POST, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prca	tranid	???	0	0	0	0	0	???	espace	aucun	???	???	x

Réponse, protocole 2.0

Nom	*Hachage de division*	*Version du protocole*	*Type de transaction*	*Transaction id*	*Utilisation réservée*	*Nombre total d'octets*	*Longueur de la division*	*Début de la division*	*Division RC*	*Demande RC*	*Méthode de codage*	*Message d'erreur*	*Message de données*	*Nom d'algorithme*	*Longueur du hachage de division 2*	*Hachage de division 2*
Longueur	40	4	4	36	32	16	16	16	4	4	4	256	0	10	4	???
Valeur	**espace**	**0200**	prca	tranid	???	0	0	0	a	b	???	espace	aucun	???	???	x

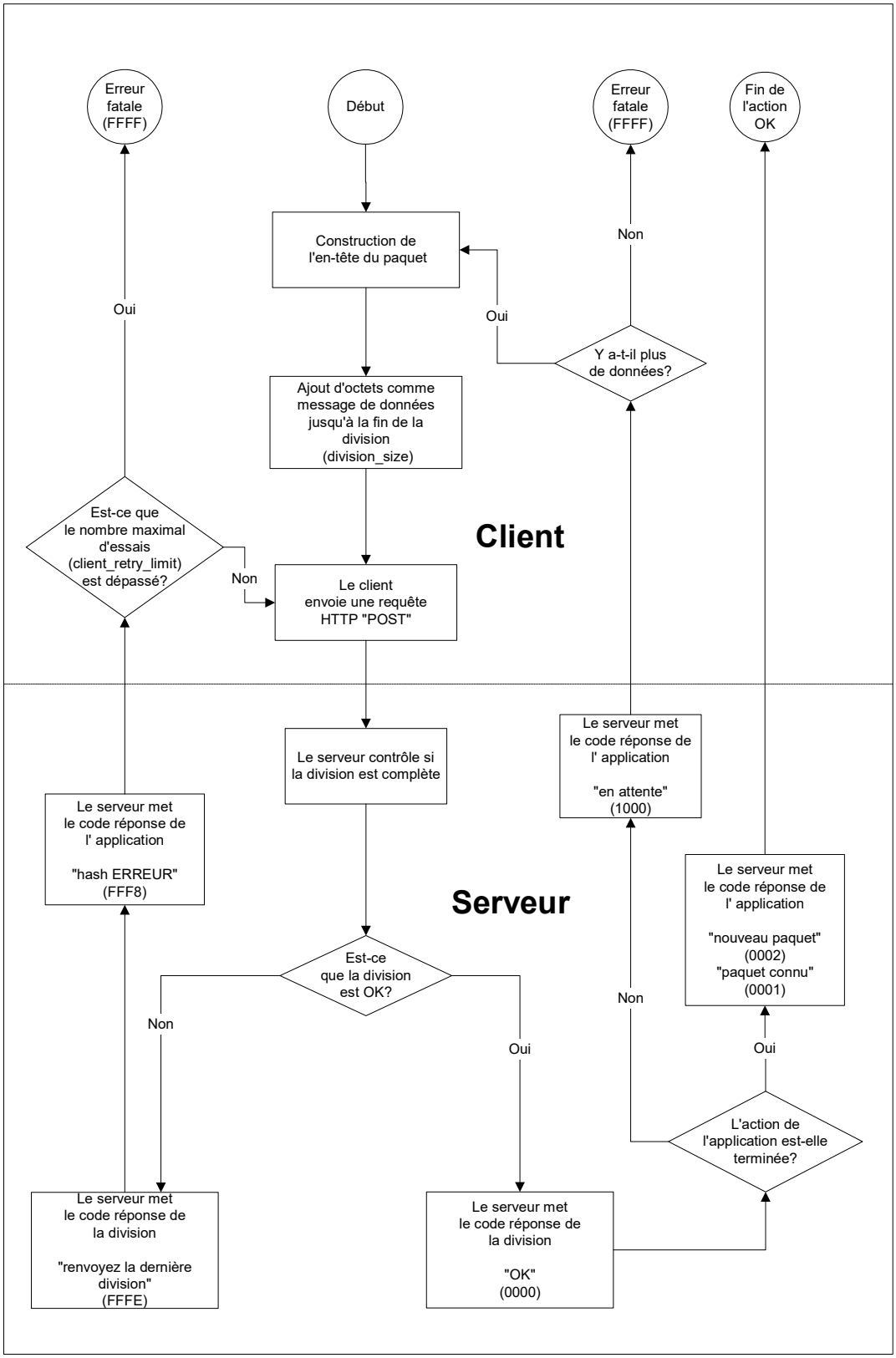


Figure 7 – Conduite à suivre pour l'envoi de l'en-tête du paquet

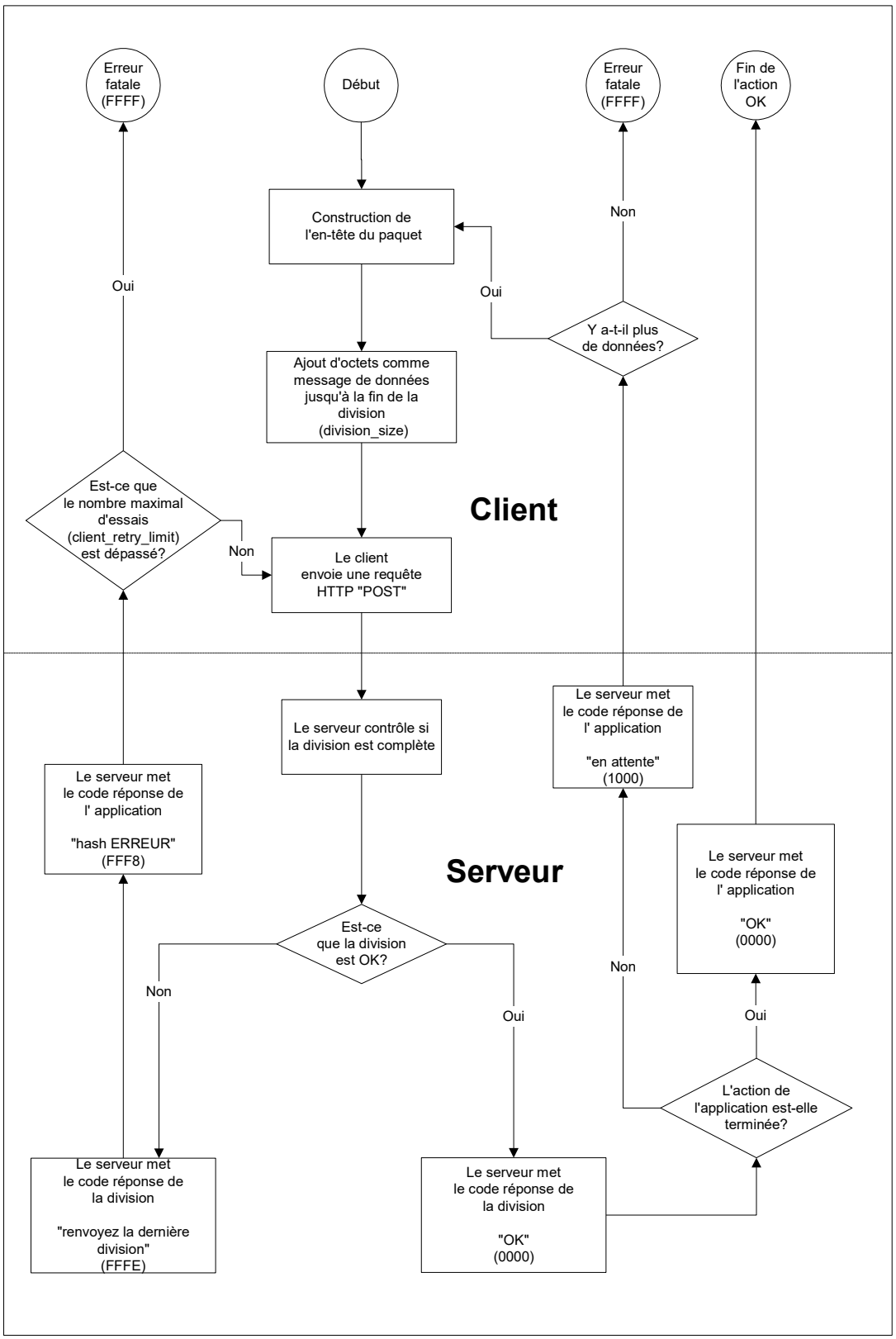


Figure 8 – Conduite à suivre pour l'envoi du paquet de données

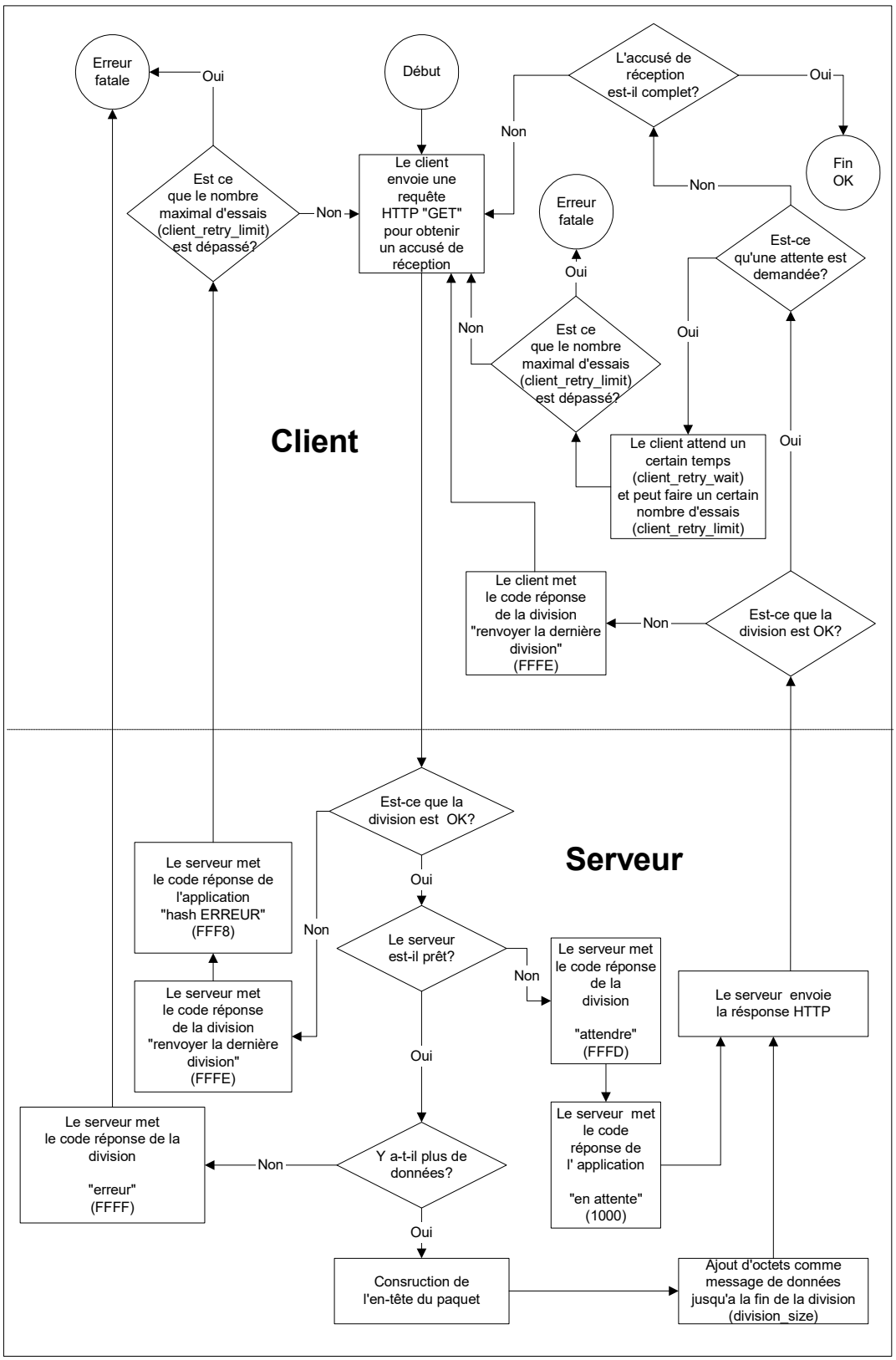


Figure 9 – Conduite à suivre pour l'obtention de l'accusé de réception

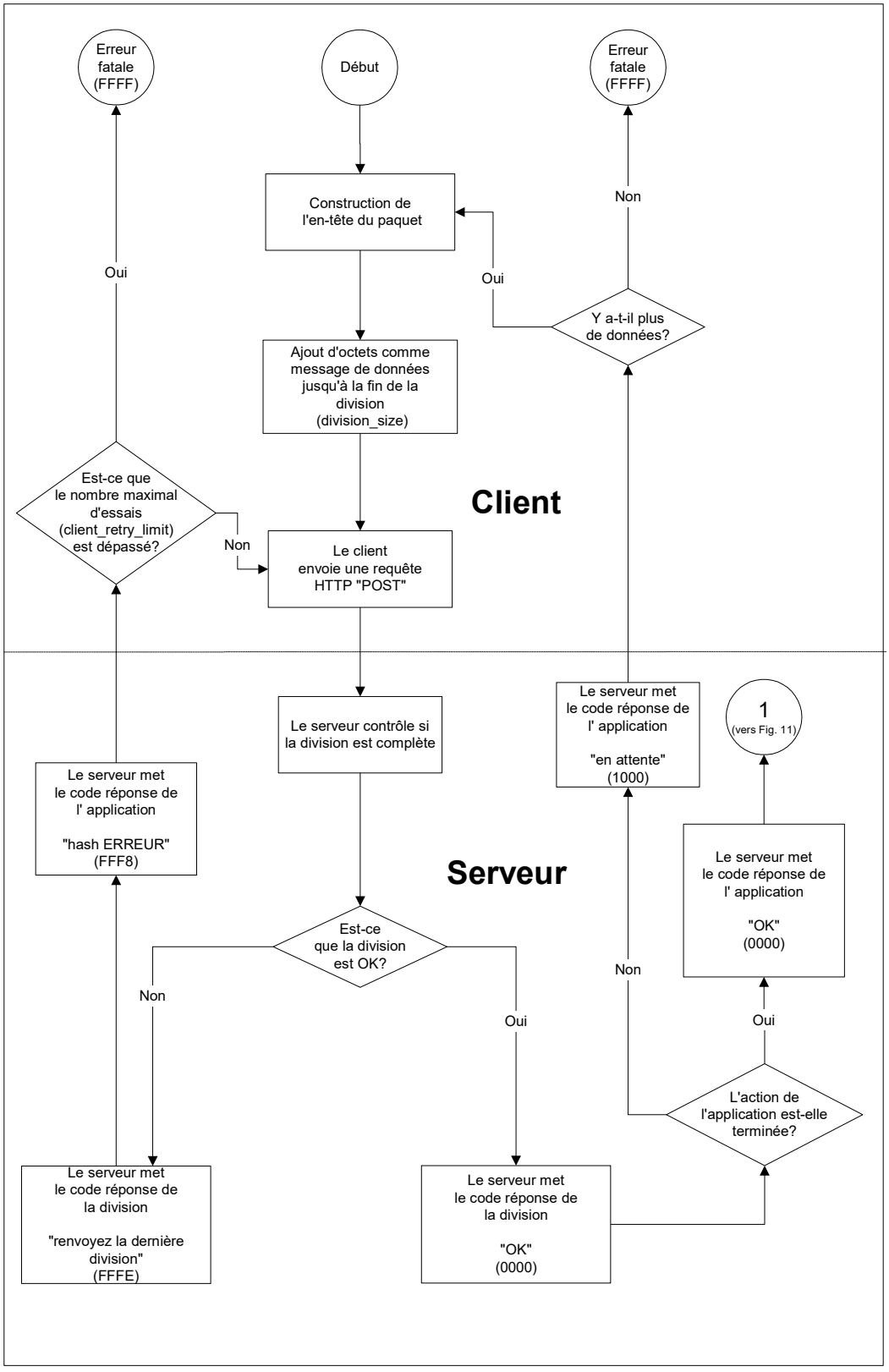


Figure 10 – Conduite à suivre pour l'obtention de l'en-tête du paquet (du déposant à l'office)

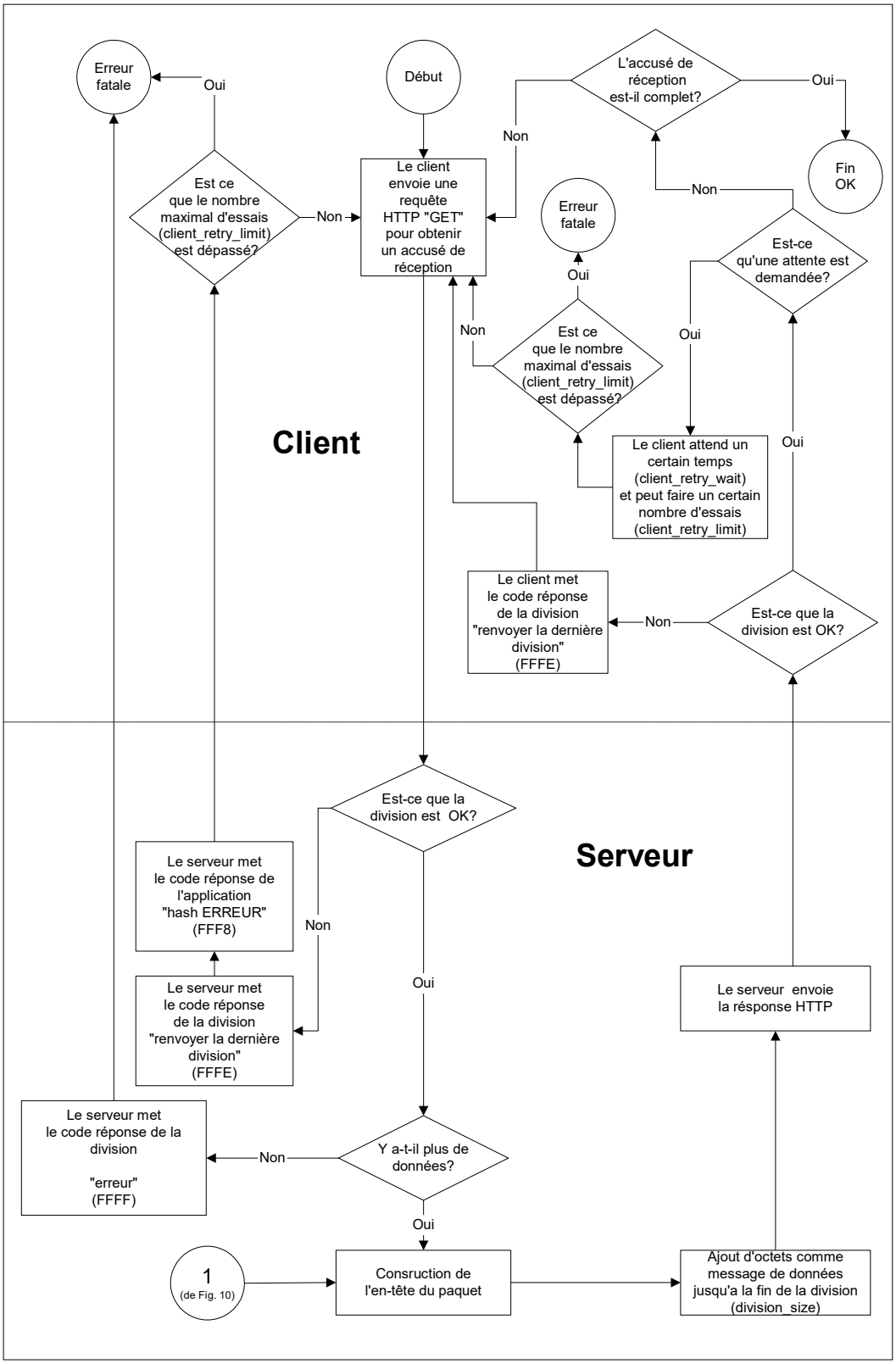


Figure 11 – Conduite à suivre pour l'obtention de l'en-tête du paquet (de l'office au déposant)

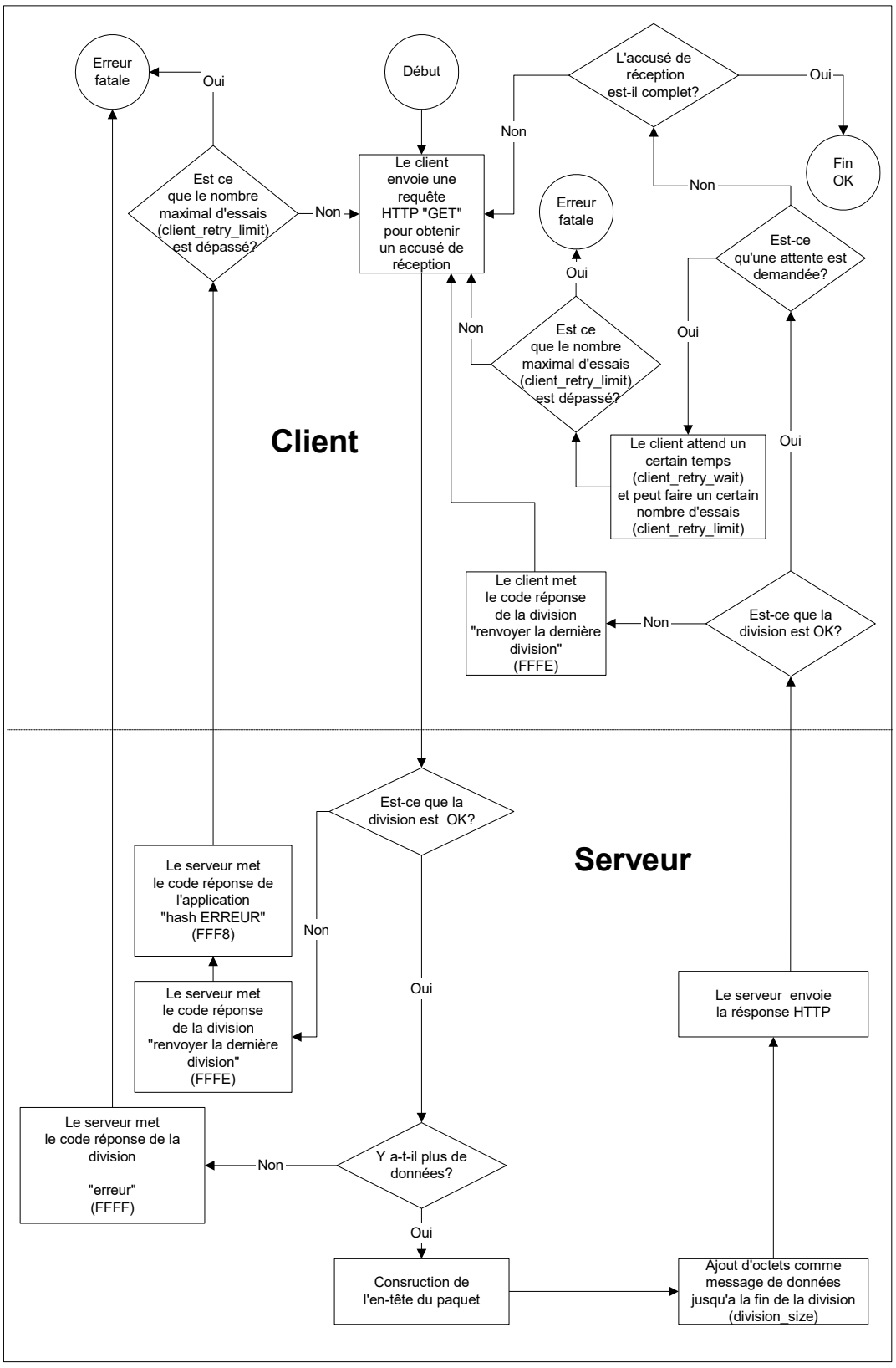


Figure 12 – Conduite à suivre pour l'obtention des données du paquet

5.1bis Modes alternatifs de transmission en ligne

Des modes alternatifs de transmission en ligne peuvent être utilisés, en accord avec le Bureau international, par les offices qui n'utilisent par le protocole sur l'interopérabilité en matière de dépôt électronique, à condition que

a) l'interopérabilité entre le logiciel client de dépôt électronique du PCT et le serveur soit préservée sans qu'il soit nécessaire de procéder à une intervention technique ultérieure, et

b) le résultat de la transmission soit équivalent à celui du protocole sur l'interopérabilité en matière de dépôt électronique (en particulier en ce qui concerne l'accusé de réception et le niveau de sécurité).

5.1ter Autres moyens de transmission sécurisée en ligne avec consultation par le destinataire

Les offices proposant la transmission électronique de documents avec consultation en ligne par un destinataire (qu'il s'agisse du déposant ou de l'office traitant la demande) devraient recourir à un protocole sécurisé. À moins que le déposant ait explicitement demandé un autre mode de transmission (tel que l'envoi des documents directement par courrier électronique), la transmission devrait utiliser une connexion protégée par une version de TLS moderne et sécurisée ou un autre protocole de sécurité similaire prescrit par la législation nationale, et un moyen adapté à la sensibilité des documents concernés afin de garantir que seules les personnes autorisées puissent se procurer ces documents.

Selon une modalité préférée de mise en œuvre :

a) la demande internationale est associée à un ou plusieurs comptes auprès de l'office, sécurisés par une authentification à deux facteurs;

b) des notifications sont envoyées au destinataire lorsqu'un document devient disponible, que ce soit par l'envoi d'un courrier électronique au destinataire ou, s'il en a été ainsi convenu avec le destinataire, par l'accès régulier du destinataire à une liste sécurisée de documents nouvellement mis à sa disposition par l'intermédiaire d'un compte associé, que ce soit manuellement via une connexion sécurisée par navigateur ou automatiquement via un service Web sécurisé RESTful.

c) le destinataire télécharge ces documents à partir d'un compte associé, que ce soit manuellement via une connexion sécurisée par navigateur ou automatiquement via un service Web sécurisé RESTful.

L'association entre la demande internationale et tout compte du déposant devrait de préférence être établie au moyen des informations fournies par le déposant au moment du dépôt à l'aide d'un logiciel de dépôt en ligne compatible. Les offices doivent également prévoir des moyens sécurisés pour l'ajout, la suppression ou la modification de telles associations après le dépôt.

5.2 Combinaisons paquet/transmission

La présente section décrit les combinaisons paquet/transmission autorisées pour chaque secteur de communication PCT. La présente norme n'exclut pas la fourniture de renseignements accessibles au public par d'autres moyens que ceux visés ici. D'autres

types de paquets (par exemple, envoi de documents sur l'Internet) et d'autres combinaisons paquet/transmission sont envisageables pour l'avenir.

5.2.1 Secteur de communication entre le déposant et l'office (phase internationale)

Dans le présent secteur de communication, les documents constitutifs de la demande internationale peuvent être déposés en ligne (dans un environnement ICP) par l'intermédiaire d'un réseau sécurisé, ou transmis hors ligne (dans un environnement ICP ou non ICP) sur support matériel. Le dépôt en ligne d'une demande internationale à l'aide d'une méthode non ICP n'est pas autorisé à l'heure actuelle, sauf dans le cadre de réserves provisoires notifiées en vertu de l'instruction administrative 703.f).

La figure 13 présente une grille des différentes combinaisons paquet/transmission autorisées dans le présent secteur de communication :

a) En ligne/réseau sécurisé : il convient d'utiliser un WASP ou un C-WASP. Ceci est défini comme une connexion de télécommunication établie pour échanger des données à travers un réseau qui est a pour caractéristiques i) d'être un réseau privé, ii) d'utiliser l'Internet avec un niveau élevé de chiffrement (p. ex. SSL (ou TLS)), iii) d'avoir une connexion Internet sur un réseau privé virtuel (VPN).

b) Hors ligne/support matériel : les types de paquets suivants doivent être employés : WASP, C-WASP ou WAD. Les supports matériels (p. ex. disquette, CD-ROM, DVD, etc.) sont employés pour conserver les données des demandes internationales sans échange de données en temps réél.

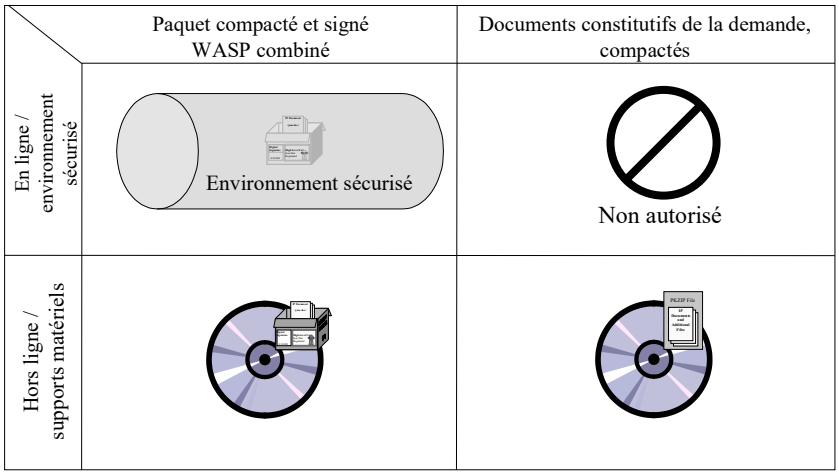


Figure 13 – Combinaisons paquet/transmission autorisées dans le secteur de communication entre le déposant et l'office (phase internationale)

5.2.2 Secteur de communication entre offices (d'office à office)

Dans le présent secteur de communication, les documents constitutifs des demandes internationales peuvent être communiqués en ligne par l'intermédiaire d'un réseau sécurisé, ou envoyés hors ligne sur support matériel. On remarquera que, dans le présent

secteur de communication, lorsque l'office expéditeur et l'office destinataire ont accepté, conformément à la section 4, de ne pas empaqueter les documents constitutifs des demandes internationales déposés sur papier et convertis en documents sous forme électronique, ou de les empaqueter autrement, différents types de combinaisons pour les documents constitutifs des demandes internationales déposés sur papier et convertis en documents sous forme électronique peuvent être employés.

La figure 14 présente une grille des différentes combinaisons paquet/transmission autorisées dans le présent secteur de communication :

a) En ligne/réseau sécurisé : il convient d'utiliser un WASP ou un WAD. Ceci est défini comme une connexion de télécommunication établie pour échanger des données, à travers un réseau qui est a pour caractéristiques i) d'être un réseau privé, ii) d'utiliser l'Internet avec un niveau élevé de chiffrement (p. ex. SSL (ou TLS)), iii) d'avoir une connexion Internet sur un réseau privé virtuel (VPN).

b) Hors ligne/support matériel : un WASP ou un WAD doit être utilisé. Le support matériel (p. ex. disquette, CD-ROM, DVD etc.) est employé pour conserver les données des demandes internationales sans échange de données en temps réel.

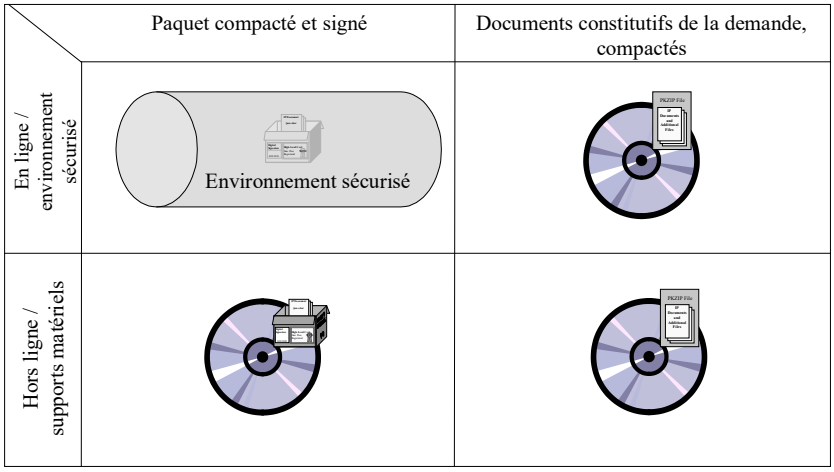


Figure 14 – Combinaisons paquet/transmission autorisées dans le secteur de communication entre offices (d'office à office)

Le paquet électronique préparé par l'office expéditeur qui contient tous les documents et données pertinents (voir les figures 2 et 2*bis* à la section 3.2, et les figures 14*bis* et 14*ter*, ci-après) et qui est envoyé à l'office destinataire porte une identification de l'office selon la capacité avec laquelle il agit, comme suit :

- "paquet RO" pour tout paquet préparé par l'office récepteur,

- "paquet IB" pour tout paquet préparé par le Bureau international,

- "paquet ISA" pour tout paquet préparé par l'administration chargée de la recherche internationale, et

- “paquet IPEA” pour tout paquet préparé par l’administration chargée de l’examen préliminaire international.

Les figures qui suivent montrent des exemples de paquets RO contenant des exemplaires originaux tels qu’ils doivent être envoyés au Bureau international. La figure 14*bis* montre un exemplaire original d’une demande internationale déposée en format PDF; dans ce cas, la copie de travail doit contenir des images en format TIFF converties (voir la section 3.1.2, dernier paragraphe). La figure 14*ter* montre un exemplaire original d’une demande internationale déposée en format XML; dans ce cas, il n’est pas nécessaire que la copie de travail contienne des images en format TIFF converties. La copie de travail à laquelle il est fait référence dans le présent paragraphe doit être entendue comme étant la partie du paquet RO qui est produite par l’office récepteur, en sus du paquet électronique provenant du déposant (“paquet du déposant”), en copiant, convertissant ou modifiant les documents contenus dans le paquet du déposant (p. ex. request.xml) ou en générant de nouveaux documents (p. ex. ex-officio-corrections.xml).

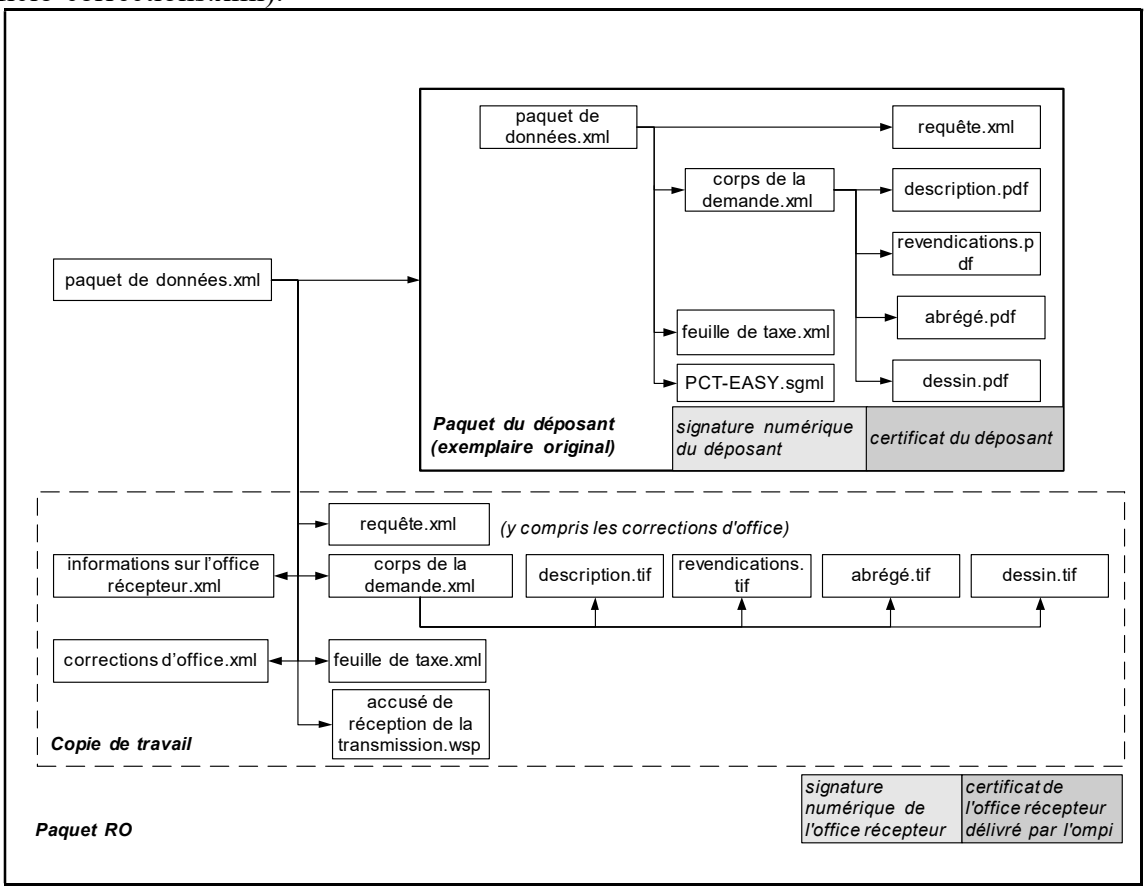


Figure 14*bis* – Exemple d’un paquet RO contenant un exemplaire original lorsque le texte de la description, des revendications et de l’abrégé n’est pas en format à codage de caractères (mais en format PDF)

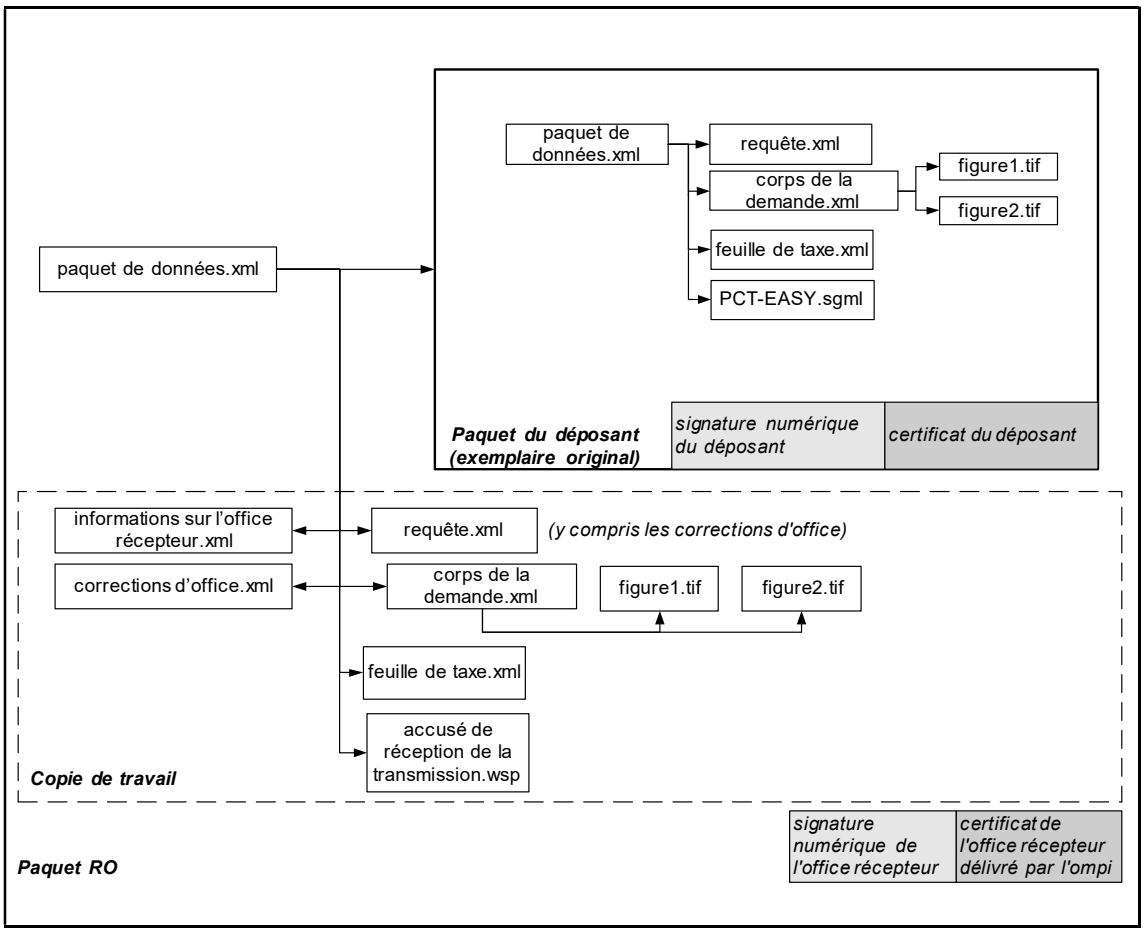


Figure 14*ter* – Exemple d'un paquet RO contenant un exemplaire original dont le texte de la description, des revendications et de l'abrégé est en format à codage de caractères (en format XML)

5.2.3 Secteur de communication des offices désignés

Dans le présent secteur de communication, les documents constitutifs des demandes internationales peuvent être communiqués en ligne par l'intermédiaire d'un réseau sécurisé, hors ligne sur support matériel ou, en ce qui concerne les documents qui ne représentent pas de caractère confidentiel, sur l'Internet.

La figure 15 présente une grille des différentes combinaisons paquet/transmission autorisées dans le présent secteur de communication :

a) En ligne/Internet : il faut utiliser un WASP ou un WAD. La présente combinaison n'est permise que pour la transmission de documents qui ne représentent pas de caractère confidentiel.

b) En ligne/réseau sécurisé : il convient d'utiliser un WASP ou un WAD. Ceci est défini comme une connexion de télécommunication établie pour échanger des données à travers un réseau qui est a pour caractéristiques i) d'être un réseau privé, ii) d'utiliser l'Internet avec un niveau élevé de chiffrement (p. ex. SSL (ou TLS)), iii) d'avoir une connexion Internet sur un réseau privé virtuel (VPN).

c) Hors ligne/support matériel : un WASP ou un WAD. Les supports matériels (p. ex. disquette, CD-ROM, DVD etc.) sont employés pour conserver les données des demandes internationales sans échange de données en temps réel.

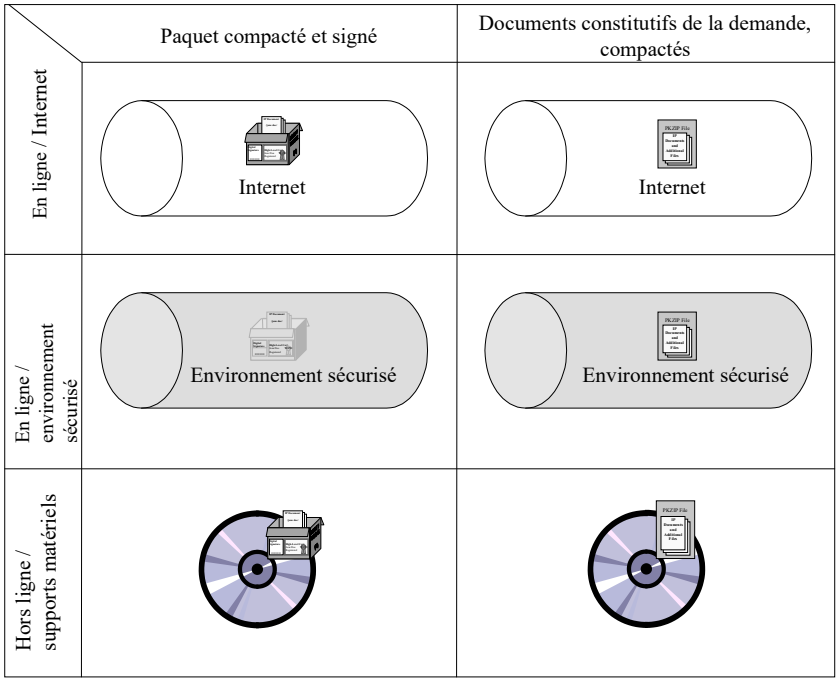


Figure 15 – Combinaisons paquet/transmission autorisées dans le secteur de communication des offices désignés[14]

6. LOGICIEL POUR LE DÉPÔT ÉLECTRONIQUE

Le Bureau international fournit un logiciel[15] qui est conforme à toutes les exigences prévues dans la norme commune de base ainsi qu'à certaines variantes prévues dans la présente annexe. L'utilisation de ce logiciel n'est pas obligatoire, mais tout déposant est en droit de l'utiliser, auquel cas l'office récepteur doit accepter la demande internationale concernée (sauf s'il a émis une réserve transitoire en vertu de l'instruction 703.f) à cet égard). Cependant, les offices récepteurs peuvent également choisir, d'accepter d'autres logiciels de dépôt.

7. [*Supprimée*]

8. PRINCIPES DE GESTION DES DOSSIERS ÉLECTRONIQUES

Le passage au dépôt et au traitement électroniques des documents constitutifs de demandes internationales aura un impact considérable sur les méthodes de gestion des

[14] Voir la section 5.2.3(a): seuls les documents qui ne représentent pas de caractère confidentiel peuvent être transmis sur l'Internet.

[15] Le logiciel actuellement fourni à cet effet par le Bureau international est ePCT. Toutefois, tant que le logiciel PCT-SAFE reste disponible, les offices récepteurs peuvent continuer à accepter PCT-SAFE ou à la fois ePCT et PCT-SAFE pour le dépôt électronique.

dossiers. Les conventions qui s'appliquent aux documents sur papier ne s'appliquant pas, pour la plupart, aux documents électroniques, il conviendra d'établir de nouvelles directives qui permettront de faire face aux nouvelles questions relatives à l'information électronique. La présente partie expose des principes destinés à satisfaire aux exigences d'authenticité, d'intégrité, de confidentialité et de non-répudiation dans le cadre de la gestion des documents constitutifs de demandes internationales sous forme de dossiers électroniques. Ces principes sont les suivants :

i) tous les documents déposés sous forme électronique doivent pouvoir être imprimés sur papier et transférés dans un système de gestion des dossiers électroniques sans perte de contenu ni altération matérielle;

ii) les renseignements concernant l'origine et la destination des dossiers électroniques, leur contexte ainsi que les indications de date et d'heure de création, d'envoi et de réception, souvent appelés "métadonnées", et qui sont systématiquement recueillis par les systèmes automatisés des offices, doivent être considérés comme faisant partie de ces dossiers et conservés par les systèmes automatisés; toutefois, cette exigence ne s'applique pas aux renseignements qui n'ont d'autre objet que de permettre l'envoi ou la réception du dossier;

iii) les copies d'archive doivent être conservées dans le format électronique de document dans lequel elles ont été créées, envoyées ou reçues, ou dans un format dont il peut être démontré qu'il représente avec précision les informations ainsi créées, envoyées ou reçues;

iv) un mécanisme doit être prévu afin de garantir l'authenticité et l'intégrité du document déposé sous forme électronique; cela suppose la possibilité de vérifier l'identité de l'expéditeur (le déposant ou son représentant autorisé responsable du contenu du document) ou de l'auteur d'un document de l'office, ainsi que la possibilité de vérifier qu'un document est resté complet et n'a pas été altéré dans le système, exception faite de l'adjonction de tout endossement et de toute modification pouvant intervenir de manière générale en cours de communication, d'archivage et d'affichage;

v) les systèmes de dépôt, de traitement et d'archivage électroniques doivent prévoir des mécanismes de sauvegarde et de récupération pour protéger les dossiers électroniques contre les défaillances de ces systèmes;

vi) les dossiers électroniques seront conservés de façon à être accessibles à long terme, d'une manière qui garantisse l'accès aux informations sous une forme utilisable pendant le délai de conservation prescrit;

vii) les systèmes de gestion des dossiers électroniques doivent prévoir des mécanismes et des procédures d'assurance et de contrôle de la qualité du matériel et des procédures mis en œuvre pour recevoir, traiter et conserver les documents archivés et gérés;

viii) les systèmes de gestion des dossiers électroniques doivent mettre en œuvre une piste de contrôle permettant de retracer toutes les informations pertinentes relatives aux adjonctions, suppressions ou modifications

apportées au système de gestion des dossiers électroniques ainsi qu'aux dossiers eux-mêmes.

9. ABRÉVIATIONS, INTERPRÉTATIONS ET GLOSSAIRE

D'une manière générale, les termes et expressions utilisés dans le PCT, son règlement d'exécution et ses instructions administratives ont le même sens dans la présente annexe et sont utilisés sans autre forme d'explication (par exemple, "demande internationale", "requête", "office récepteur", etc.)[16]. Les autres termes sont employés dans le sens qu'ils ont dans le domaine des techniques de l'information. Certains termes revêtant une importance particulière dans la présente annexe sont définis dans le paragraphe suivant.

Aux fins de la présente annexe, on entend par

a) "signature électronique de base (ou simple)", une signature électronique[17] qui peut être :

i) une chaîne de caractères particulière entrée par l'utilisateur;

ii) une image reproduisant en fac similé la signature manuscrite;

iii) une signature enveloppée électroniquement selon la méthode dite du "click wrap";

b) "signature électronique renforcée (ou sécurisée)", une signature électronique au sujet de laquelle il peut être prouvé, grâce à l'utilisation d'une procédure de sécurité, qu'elle

i) appartient au seul titulaire de la signature dans le contexte dans lequel elle a été utilisée;

ii) a été créée et jointe – ou associée logiquement – au document électronique par le titulaire de la signature ou avec des moyens dont seul le titulaire de la signature a la maîtrise, et par nulle autre personne;

iii) a été créée et est liée au document électronique d'une façon telle qu'elle permet de garantir que l'intégrité du document a été préservée;

une des applications de la signature électronique renforcée est la "signature numérique" créée grâce à l'utilisation d'un certificat produit par une infrastructure à clé publique (ICP) et d'une clé privée correspondante;

c) "certificat numérique", un dossier publié par une autorité de certification et qui identifie une personne ou une entité qui détient une paire de clés donnée,

---

[16] Voir également les notes 1, 2 et 5.

[17] Voir l'instruction 701.iv)

dans le contexte de l'infrastructure à clé publique; par exemple, un certificat doit, entre autres, identifier l'autorité de certification qui le délivre, identifier l'abonné, contenir la clé publique de l'abonné, identifier sa période de validité, et être signé numériquement par l'autorité de certification qui le délivre;[18]

d) "autorité de certification", une entité qui délivre des certificats numériques et assure d'autres services liés aux signatures électroniques, tels que la gestion des certificats et des clés numériques et la tenue d'un registre y relatif;[19]

e) "certificat simplifié", un certificat numérique qui a été délivré au déposant, par exemple dans le cadre de l'enregistrement du client procédant à un dépôt en ligne, ou obtenu d'une autorité de certification, et qui établit l'identité du déposant sans vérification préalable;

f) "certificat qualifié", un certificat numérique émis par un tiers de confiance qui établit l'identité du déposant avec vérification préalable.

On trouvera des explications supplémentaires concernant les expressions et abréviations suivantes dans le corps de la présente annexe. Voir également l'appendice II concernant la terminologie utilisée dans le contexte de l'ICP.

Bureau international	Bureau international de l'OMPI
C-WASP	WASP combiné
Document inclus par renvoi	fichier qui figure dans le paquet WAD auquel il est fait référence (au moyen de son nom de fichier) dans un ou plusieurs documents en format XML qui figure(nt) dans le même paquet
DTD	définition de type de document
E-PCT (norme)	norme de dépôt électronique des demandes PCT
ICP	infrastructure à clé publique
IETF	*Internet Engineering Task Force*
Instructions administratives	Instructions administratives du PCT
JFIF	*JPEG File Interchange Format* (Format JPEG d'échange de fichiers)

[18] Pour consulter une liste des exigences minimales concernant un certificat numérique, voir 'Certificat' dans le glossaire de l'appendice II.

[19] Voir 'Autorité de certification' dans le glossaire de l'appendice II.

JPEG	*Joint Photograph Experts Group* (Groupe conjoint des experts en photographie)
Office	utilisé dans un contexte général : l'office récepteur, l'administration chargée de la recherche internationale, l'administration chargée de l'examen préliminaire international, l'office désigné, l'office élu, le Bureau international ou l'office de propriété industrielle national ou régional
OMPI	Organisation Mondiale de la Propriété Intellectuelle
PCT	Traité de coopération en matière de brevets
PKCS	norme de cryptographie à clé publique
RFC	appel à commentaires
RNIS	réseau numérique à intégration de services
Secteur de com. entre le déposant et l'office (phase internationale)	voir la section 2.3.1 ci-dessus
Secteur de com. entre le déposant et l'office (phase nationale)	voir la section 2.3.4 ci-dessus
Secteur de com. entre les offices désignés et le BI	voir la section 2.3.3 ci-dessus
Secteur de com. entre offices (d'office à office)	voir la section 2.3.2 ci-dessus
SSL	protocole à couche de ports sécurisés
TCP/IP	protocole de contrôle des transmissions / protocole de l'Internet
TIFF	*Tagged Image File Format* (Format de fichiers d'images balisées)
TLS	protocole TLS (Transport Layer Security)
WAD	documents constitutifs de la demande compactés
WASP	paquet compacté et signé
XML	*eXtensible Mark-up Language* (langage de balisage extensible)

[L'appendice I de l'annexe F suit]

APPENDICE I
DTDS EN XML POUR LA NORME E-PCT

Le contenu du présent appendice figure dans le document PCT/AI/DTD/6 Rev. daté du 26 juin 2009 (ou tout autre document subséquent) qui est reproduit sur le site Internet de l'OMPI à l'adresse suivante : www.wipo.int/pct/fr/texts/index.htm; des exemplaires imprimés peuvent être obtenus auprès du Bureau international de l'OMPI sur simple demande.

[L'appendice II de l'annexe F suit]

APPENDICE II
ARCHITECTURE IPC POUR LA NORME E-PCT

1. INTRODUCTION

Le présent document contient les renseignements techniques relatifs aux éléments d'une infrastructure à clé publique (ICP) qui sont nécessaires dans le cadre de l'annexe F.[20]

2. CHAMP D'APPLICATION

Questions ne relevant pas du présent document :

a) Spécification de l'infrastructure à clé publique – l'annexe F et le présent appendice font référence aux services d'un environnement ICP. Il est cependant envisagé d'exposer la spécification de l'ICP (règles de délivrance de certificats, conception technique, documents relatifs aux opérations, etc.) dans des documents ne faisant pas partie de la présente norme.

b) La certification croisée dans un environnement ICP n'est pas entièrement traitée.

3. EXIGENCES RELATIVES À L'INFRASTRUCTURE À CLÉ PUBLIQUE (ICP)

L'annexe F désigne l'ICP comme la méthode permettant d'assurer la sécurité des échanges en ligne. Le recours à l'ICP répond aux objectifs suivants :

a) Garantir que les offices PCT offrent une sécurité adéquate pour le traitement d'informations confidentielles tout au long de la procédure PCT.

b) Assurer les services nécessaires pour permettre aux opérations du PCT d'être intégrées dans un système de dossiers électroniques sécurisés.

c) Fournir aux offices et administrations du PCT et aux déposants du PCT, à l'aide de la cryptographie, quatre services fondamentaux en matière de sécurité, à savoir :

i) l'authentification, qui est le processus de validation de l'identité revendiquée par ou pour une entité;

ii) l'intégrité des données, qui consiste à veiller à ce que les données ne subissent pas de modification à partir du moment de leur envoi, et à éviter leur modification, altération ou destruction par accident ou par suite d'un acte malveillant;

iii) la non-répudiation, qui permet à l'expéditeur des données de disposer de preuves solides et fondées du fait que les données ont bien été transmises (avec la collaboration du destinataire), et au destinataire de disposer de preuves solides et fondées

---

[20] Les termes et expressions utilisés dans le présent appendice ont le même sens que dans la partie principale de l'annexe F; voir la section glossaire et abréviations figurant à la fin de cette partie principale. Voir aussi le glossaire figurant dans le présent appendice.

concernant l'identité de l'expéditeur, ces preuves devant être suffisantes pour que l'un ou l'autre ne puisse de manière crédible nier avoir été en possession de ces données; comprend la possibilité de vérification de l'intégrité et de l'origine des données par un tiers;

iv) confidentialité, qui consiste à veiller à ce que les informations ne puissent être lues que par les entités autorisées.

4. CARACTÉRISTIQUES DE L'ICP POUR LE PCT

La présente section décrit un environnement ICP interopérable capable de fournir aux déposants et aux offices les services de sécurité exigés pour assurer des échanges sécurisés des documents constitutifs de la demande internationale.

Le modèle de confiance E-PCT repose sur un modèle de répertoire de base. Selon ce modèle, le logiciel lui-même (le logiciel de dépôt électronique PCT par exemple) utilise la liste de confiance des autorités de certification. Le logiciel client ICP traite les certificats (après consultation de la liste des certificats révoqués ou du protocole sur le statut du certificat en ligne) délivrés par l'une des autorités de certification agréée afin de déterminer si le certificat de clé publique d'un utilisateur d'une autre communauté peut être accepté.

Le modèle de répertoire de base de confiance est une architecture de confiance équilibrée dont le fonctionnement ne repose pas sur la certification croisée. Le modèle de confiance est utilisé aujourd'hui dans la communauté des navigateurs Internet mais il peut être mis en œuvre dans d'autres logiciels que les seuls navigateurs Internet (le logiciel de dépôt électronique PCT par exemple).

Le présent modèle utilise un fichier pour archiver les certificats de clé publique de nombreuses autorités de certification (p. ex. l'autorité de certification d'un office de propriété intellectuelle). Les parties qui se fient au système ont donc confiance en tout certificat de clé publique inclus dans le fichier qu'elles reçoivent. Le certificat de clé publique compris dans le répertoire principal peut être une autorité de certification principale d'un autre domaine ou une autorité de certification subordonnée mais, lorsqu'elle est intégrée dans la liste de confiance, elle devient une autorité de certification principale pour la partie qui se fie à la clé.

Dans l'environnement E-PCT, chaque office gère une liste de confiance des autorités de certification qu'il reconnaît. Selon cette architecture, le logiciel de dépôt électronique PCT fait également confiance à toutes les entités inscrites sur la liste de confiance et à leurs subordonnés.

La figure 1 ci-après illustre la façon dont le modèle de répertoire de base sera appliqué au modèle de confiance ICP E-PCT.

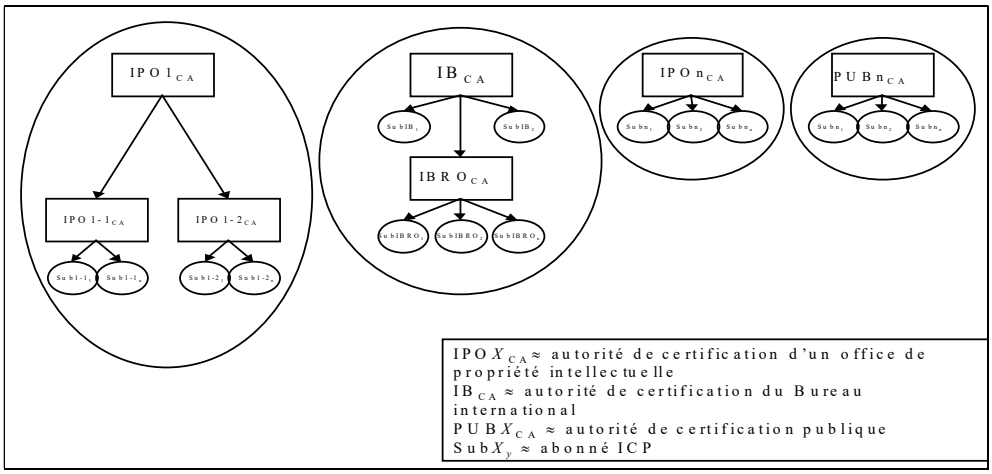


Figure 1 – Modèle de confiance ICP du dépôt électronique PCT

Chaque zone délimitée dans la figure 1 représente un domaine ICP indépendant qui offre des services d'autorité de certification. Les deux types d'autorités de certification reconnues sont les autorités de certification des offices eux-mêmes (p. ex. IPO1 $_{CA}$) et les autorités de certification publiques (p. ex. PUBn $_{CA}$). La liste de confiance utilisée par le logiciel E-PCT est référencée afin d'établir un chemin de sécurisé entre les domaines ICP. Par exemple, dans la figure 1, la liste de confiance comprend les certificats principaux de confiance de IPO1$_{CA}$, IB$_{CA}$, IPOn$_{CA}$ et PUBn$_{CA}$. Dans certains cas, les offices peuvent choisir de ne pas inclure les certificats des autorités de certification publiques (p. ex. PUBn$_{CA}$) lorsqu'ils n'acceptent pas les certificats des autorités de certification publiques lors des phases internationale et/ou nationale.

4.1 Validation du certificat/de la signature dans le modèle de confiance ICP du dépôt électronique PCT

La présente section traite de l'utilisation d'un certificat numérique utilisé pour une signature numérique. La section 4.2 traite de l'utilisation du certificat utilisé aux fins du chiffrement.

Le modèle de confiance ICP du dépôt électronique PCT prévoit la possibilité que les certificats numériques délivrés par une autorité de certification dans un domaine ICP soient validés par des entités d'autres domaines ICP. Par exemple, dans la figure 1, les domaines IPO1$_{CA}$, IB$_{CA}$, et n (IPOn$_{CA}$, PUBn$_{CA}$) peuvent délivrer des certificats qualifiés de même que des certificats simplifiés aux abonnés de la communauté[21]. Pour la validation des certificats et des signatures, il n'est pas indispensable de créer/gérer une banque commune de certificats (ou autre mécanisme d'annuaire interdomaine). La validation des certificats est en effet effectuée à l'aide du certificat de confiance de base à travers la consultation du protocole sur le statut du certificat en ligne ou d'un répertoire étranger contenant la liste des certificats révoqués applicable.

[21] Il est prévu que l'autorité de certification du Bureau international ne délivre de certificats qualifiés qu'aux offices et administrations du PCT. Elle délivrera des certificats simplifiés aux déposants et aux mandataires.

Par exemple, si l'abonné $SubIB_1$ entreprenait la validation d'un certificat reçu de $Sub1\text{-}1_1$ (dans le cas du processus de validation des signatures), les phases de la procédure seraient les suivantes :

1. Chaque certificat figurant sur le chemin sécurisé serait évalué.[22] Dans cet exemple, le premier certificat $Sub1\text{-}1_1$ serait validé une fois vérifié qu'il a été signé à l'aide de la clé privée conservée par le titulaire du certificat $IPO1\text{-}1_{CA}$. En outre, la durée de validité serait vérifiée ainsi que le statut de révocation en utilisant le protocole sur le statut du certificat en ligne ou la liste des certificats révoqués.

2. Ensuite, l'$IPO1\text{-}1_{CA}$ serait validé une fois vérifié que le certificat a été signé à l'aide de la clé privée conservée par le détenteur du certificat $IPO1_{CA}$. En outre, la durée de validité serait vérifiée ainsi que le statut de révocation en utilisant le protocole sur le statut du certificat en ligne ou la liste des certificats révoqués.

3. Enfin, le dernier certificat figurant sur le chemin sécurisé (connu aussi sous le nom de certificat d'ancrage) serait validé par comparaison avec les certificats de confiance de base utilisés par le logiciel E-PCT. Dans cet exemple, le certificat IPO1CA identifié dans le certificat évalué serait comparé au certificat IPO1CA figurant dans la liste de confiance. En outre, la durée de validité et la liste des autorités révoquées seraient vérifiées.

Dans l'exemple ci-dessus, tout le processus de validation peut être opéré localement, à l'exception de la vérification des listes des certificats révoqués et de la liste des autorités révoquées. Ces listes peuvent être conservées indépendamment, pourvu qu'elles soient accessibles à la partie se fiant à la clé.

Le processus décrit plus haut permet aux offices de valider les certificats simplifiés au cours de la phase nationale également. En d'autres termes, si un office désigné autorise l'utilisation de certificats simplifiés au cours de la phase nationale, le mécanisme permettra au déposant d'aborder la phase nationale avec son certificat simplifié existant.

Par exemple, lorsque l'abonné $Sub1\text{-}1_1$ (abonné de l'office désigné) doit valider un certificat reçu de $Subn_1$ (déposant qui a reçu un certificat d'une autorité de certification publique), les phases du processus sont les suivantes :

a) Le déposant signe les documents appropriés pour l'ouverture de la phase nationale avec son certificat simplifié.

b) Chaque certificat figurant sur le chemin sécurisé est évalué. Dans cet exemple, le premier certificat Subn1 est validé en vérifiant que le certificat a été signé en utilisant la clé privée maintenue par l'autorité de certification PUBnCA. En outre, la période de validité est vérifiée, ainsi que le statut de révocation en utilisant le protocole sur le statut du certificat en ligne ou la liste des certificats révoqués.

c) Ensuite, le certificat d'ancrage est validé par comparaison avec les certificats de confiance de base utilisés par le logiciel E-PCT. Dans cet exemple, le certificat

---

[22] Pour mettre en œuvre cette mesure, les certificats doivent comprendre l'intégralité de la chaîne des certificats jusqu'à l'autorité principale.

PUBnCA trouvé dans le certificat évalué est comparé au certificat PUBnCA de la liste de confiance. En outre, la durée de validité et la liste des autorités révoquées sont vérifiées.

Afin d'établir un lien entre la demande internationale reçue du Bureau international et le déposant, le nom et l'adresse électronique figurant dans les documents de la demande internationale seront comparés avec le nom et l'adresse électronique figurant dans le certificat reçu du déposant. L'office désigné pourra aussi obtenir, au besoin, l'authentification par les moyens traditionnels (procédure sur papier).

Si l'office désigné ne prévoit pas l'utilisation d'un certificat simplifié ou d'un certificat (qu'il soit simplifié ou qualifié) délivré par une autorité de certification publique au cours de la phase nationale, le déposant devra obtenir un certificat accepté par cet office.

4.2 Chiffrement dans le modèle de confiance du PCT

Le chiffrement des paquets préparés selon la présente norme est réalisé par le SSL (ou le TLS) (voir l'annexe F, section 5.1, Protocole sur l'interopérabilité en matière de dépôt électronique). Pour les paquets envoyés en utilisant le SSL (ou le TLS), le côté client de l'authentification comprend l'utilisation du certificat numérique du client. Le certificat est validé en utilisant la même méthode que celle qui est décrite dans la section 4.1.

4.3 Autorité de certification

Chaque office récepteur doit indiquer quelles sont les autorités de certification qu'il a agréé pour la délivrance des certificats aux fins de l'E-PCT. La liste peut inclure des autorités de certification publiques ou des offices eux-mêmes. Le Bureau international publiera cette liste d'autorités de certification reconnues avec un lien vers la politique de certification publiée par ces autorités de certification.

Dans le même temps, les offices PCT œuvreront avec le Bureau international à la définition d'un ensemble coordonné de directives permettant d'évaluer ces énoncés de politiques ICP. À plus long terme, ces directives devraient permettre d'établir une liste des autorités de certification acceptables pour tous les offices récepteurs. Le Bureau international publiera alors cette liste avec les certificats de base de l'autorité de certification de confiance, qui seront disponibles pour être téléchargés via le SSL (ou le TLS).

Une autorité de certification reconnue est chargée de veiller à l'exactitude des certificats électroniques qui "prouvent" qu'une partie est bien qui elle prétend être. L'autorité de certification conserve les informations relatives à tous les certificats qu'elle délivre dans une structure d'annuaire conforme à la recommandation X.500 de l'UIT. Ces systèmes comprennent, pour la publication et l'extraction de certificats numériques d'utilisateurs, une interface externe conforme au protocole allégé d'accès annuaire (*Lightweight Directory Access Protocol* (LDAP)) utilisant l'appel à commentaires RFC 1777 (mars 1995) du groupe de travail de l'IETF sur les réseaux. De plus, l'autorité de certification publie conformément à la recommandation X.509 des informations concernant la révocation des certificats.

Chaque office de propriété industrielle a besoin d'accéder aux informations concernant la révocation des certificats établies conformément à la recommandation X.509, pour toutes les autorités de certification qu'il accepte. Chaque fois qu'un certificat est utilisé aux fins d'identification, l'office de propriété industrielle consulte les informations concernant la révocation des certificats publiées par l'autorité de certification concernée pour s'assurer que le certificat n'a pas été révoqué.

Aux fins du respect du principe de non-répudiation, les offices et les autorités de certification doivent s'assurer que, dans le système qu'ils proposent, l'abonné génère sa propre paire de clés de signature avec son propre système et n'envoie aux tiers que sa clé de vérification publique (comme par exemple à l'autorité de certification pendant l'enregistrement).

4.4 Certificats numériques

Les certificats numériques doivent être conformes à la recommandation X.509 de l'Union internationale des télécommunications (UIT), version 3, en ce qui concerne le format du certificat.

Deux formes de certificats ont été définies : les certificats simplifiés et les certificats qualifiés.

4.4.1 Configurations du certificat E-PCT

Les configurations du certificat E-PCT, fondées sur les normes RFC 2459 (*Basic Certificate Fields*) et X.509 version 3, seront incluses dans la présente norme lorsqu'elles seront disponibles. La norme devra inclure au minimum les profils des certificats pour la signature et l'abonné de l'autorité de certification, d'une part, et la liste des certificats révoqués, d'autre part.

4.4.2 Certificat simplifié

Le processus de certification simplifiée ne nécessite pas, en règle générale, d'enregistrement préalable. Cependant, l'abonné est tenu de donner au moins son nom et une adresse de courrier électronique vérifiable (voir glossaire). Il ne lui est pas demandé de présenter des preuves supplémentaires de son identité. L'abonné utilise un système disponible sur l'Internet pour obtenir à bref délai un certificat simplifié auprès du Bureau international (Autorité de certification de l'OMPI pour les utilisateurs) ou il suit un processus similaire d'abonnement auprès de toute autre autorité de certification reconnue qui assure le même service.

4.4.3 Certificat qualifié

Un certificat qualifié correspond à un certificat numérique qui a été délivré à l'abonné par une tierce partie de confiance et qui permet d'établir l'identité de l'abonné après vérification préalable. Un certificat qualifié peut servir à authentifier l'identité de l'abonné.

Chaque autorité de certification délivrera des certificats conformément à ses normes (publiées) relatives à la confirmation de l'identité. Le Bureau international publiera une liste d'autorités de certification reconnues pour la délivrance de certificats qualifiés.

4.4.4 Cycle de vie des certificats

Cette section donne un aperçu du cycle de vie du certificat. Elle ne porte toutefois que sur le cycle de vie dans un environnement ICP tant pour les déposants que pour les offices PCT.

Chaque certificat a une durée de vie déterminée avant l'expiration de sa validité et il faut le renouveler. Le certificat d'un abonné peut être révoqué pour différentes raisons par l'abonné, l'autorité d'enregistrement ou l'autorité locale d'enregistrement, et par toute personne autorisée dans le cadre de la gestion du certificat.

4.4.5 Obtention des certificats

Il est demandé aux offices et aux administrations du système du PCT d'obtenir et d'utiliser des certificats qualifiés délivrés par le Bureau international pour des échanges de données entre offices. Les déposants peuvent obtenir et utiliser un certificat simple aux fins du dépôt électronique. Cependant, les offices peuvent exiger que les déposants obtiennent et utilisent un certificat qualifié après le dépôt initial.

4.4.5.1 Certificat simplifié

Les abonnés de ce type de certificat sont uniquement les déposants de demandes internationales, les cessionnaires et leur mandataire.

Le processus de certification peut varier en fonction des modalités de mise en œuvre et des principes généraux applicables, mais il comporte généralement les phases suivantes :

1. Dans le logiciel fourni par le Bureau international ou l'office récepteur, le déposant/mandataire choisit l'option de demander un certificat simplifié.

2. Le déposant/mandataire saisit les renseignements suivants : nom, adresse de courrier électronique, mot de passe aux fins d'une contestation, autorité de certification reconnue choisie.[23]

3. L'ordinateur du déposant/mandataire génère des paires de clés publiques/privées pour le certificat de signature et le certificat de chiffrement.

4. L'ordinateur du déposant/mandataire produit une demande de certification PKCS #10 et l'envoie à l'autorité de certification choisie.

5. L'autorité de certification procède à une validation de base des données reçues (le nom indiqué doit être unique, la formule de contestation doit satisfaire aux critères de sécurité, etc.) et établit un certificat ou signale une erreur.

6. Si une erreur est signalée, le déposant/mandataire est invité à rectifier sa demande et à la renouveler. Sinon, il reçoit un message (à l'adresse de courrier électronique indiquée au cours de la procédure de dépôt) l'invitant à retirer le nouveau

[23] Si le logiciel permet une interaction avec une pluralité d'autorités de certification, l'utilisateur pourra obtenir une liste d'autorités de certification parmi lesquelles il choisira.

certificat. Un code d'autorisation généré par une autorité de certification sera inclus dans le message.

7. Le déposant récupère le nouveau certificat (via un canal sécurisé, p. ex. SSL (ou TLS)) après validation du code d'autorisation et du mot de passe aux fins d'une contestation.

4.4.5.2 Certificat qualifié

Des certificats numériques qualifiés sont délivrés par le Bureau international afin de faciliter l'échange de données entre offices. Le Bureau international traite les demandes de certificat et délivre ceux-ci au cas par cas.

Les offices (autres que le Bureau international) qui délivrent des certificats qualifiés aux déposants commencent généralement par la procédure d'enregistrement. Celle-ci peut varier selon l'office ou l'autorité de certification choisie, mais comporte généralement les phases suivantes :

1. Le déposant/mandataire remplit et signe une demande sur papier.

2. Le déposant/mandataire envoie cette demande sur papier à l'autorité d'enregistrement pour contrôle.

3. Si la demande est approuvée, le déposant reçoit normalement confirmation de l'enregistrement par courrier classique avec tous les renseignements requis pour passer à la procédure de certification.

4. L'autorité d'enregistrement peut exiger que le déposant/mandataire se présente en personne avec des documents d'identification.

Les modalités d'application du processus de certification peuvent varier d'un cas à l'autre, mais celle-ci sera généralement comparable à celle qui a été décrite pour le certificat simplifié. Les principales différences pour ce qui concerne le certificat qualifié sont les suivantes :

a) Le déposant donne les informations figurant dans la confirmation de l'enregistrement (au lieu de donner simplement son nom, adresse de courrier électronique, etc.).

b) L'établissement et la mise en mémoire des clés privées peuvent varier selon les procédures de l'autorité de certification choisie. Par exemple, les paires de clés peuvent être établies ou mises en mémoire à l'aide de cartes à puce.

c) L'autorité de certification peut exiger que la clé privée utilisée pour le chiffrement soit sauvegardée.

4.4.6 Utilisation des certificats

Les certificats délivrés par une autorité de certification reconnue peuvent être utilisés aux fins de l'encryptage des données et de l'envoi des signatures numériques.

Avant utilisation, tous les certificats doivent être validés.[24] C'est le logiciel client ICP de la partie se fiant à la clé qui obtient le certificat de clé publique et la liste existante des certificats révoqués. Le logiciel client ICP vérifie alors la signature de l'autorité de certification sur le certificat et s'assure, en consultant la liste précitée (ou le protocole sur le statut du certificat en ligne), que le certificat n'a pas été révoqué. Il est prévu que ces opérations seront accomplies automatiquement par le logiciel client ou des systèmes d'arrière-plan.

4.4.6.1 Signature numérique PKCS # 7 (signature électronique sécurisée)

Les abonnés signent numériquement les paquets correspondant aux demandes internationales en utilisant leurs clés privées. Les parties se fiant aux clés peuvent vérifier la signature d'un abonné et l'intégrité du paquet signé en obtenant la clé publique de vérification du signataire qui figure sur le certificat de vérification, lequel est fourni avec le paquet signé.

Les signatures numériques utilisées pour signer les paquets de données relatives aux demandes internationales doivent respecter le format et la pratique spécifiés dans la norme PKCS #7 de RSA Laboratories relative à la syntaxe du message cryptographique intitulé *Cryptographic Message Syntax Standard,* version 1.5, en ce qui concerne la définition du contenu du type *SignedData* (données signées).

La construction de ces signatures nécessite un certificat répondant aux exigences énoncées dans la section 4.4 ci-dessus.

Toutes les signatures numériques doivent être codées selon les règles de codage DER (*Distinguished Encoding Rules*) définies dans la recommandation X.690 de l'UIT.

4.4.6.2 Chiffrement

Les abonnés chiffrent les paquets de données relatives à la demande internationale au moyen du protocole SSL (ou TLS) (voir l'annexe F, section 5.1, protocole) ou, de façon optionnelle, de la clé publique de chiffrement du destinataire. Pour de plus amples informations sur le chiffrement des paquets de données relatives à la demande internationale, voir la section 4.2.

4.4.7 Expiration et renouvellement des certificats

Chaque certificat a une durée de vie déterminée, à l'issue de laquelle il vient à expiration et doit être renouvelé. Cette durée limitée a pour but d'éviter la vulnérabilité aux attaques : quelqu'un qui disposerait d'un grand nombre de messages signés ou chiffrés au moyen de la même clé pourrait en effet chercher à "casser" cette clé, ce qui demande du temps. Normalement, un certificat d'abonné est automatiquement renouvelé avant expiration, avec production de nouvelles paires de clés et délivrance d'un nouveau certificat. Un abonné peut être tenu de demander le renouvellement. Le logiciel E-PCT de l'abonné doit notifier à l'utilisateur final l'imminence de l'expiration.

[24] Les navigateurs Internet génériques ne mettent pas en œuvre des procédures de validation des certificats ; des moyens supplémentaires doivent donc être prévus pour mettre en œuvre cette fonction.

Lors de la mise à jour d'une paire de clés, celle-ci est remplacée par une nouvelle paire de clés et un nouveau certificat de clé publique est créé. Si un certificat d'abonné doit être mis à jour pour tout motif autre que son expiration en temps normal, l'intervention de l'abonné et celle de l'autorité d'enregistrement sont nécessaires. Des modifications à apporter aux données d'identification de l'abonné, ou une suspicion d'usage abusif ou de compromission de clé peuvent notamment motiver une mise à jour.

4.4.8 Révocation des certificats

Un certificat d'abonné peut être révoqué pour plusieurs motifs. La procédure de révocation du certificat peut être engagée par l'abonné, par l'autorité d'enregistrement ou l'autorité locale d'enregistrement, et par toute personne autorisée dans le cadre de la gestion du certificat. Tout abonné doit aviser l'autorité d'enregistrement ou autorité locale d'enregistrement compétente des circonstances suivantes :

a) il n'a plus besoin du certificat (par exemple en cas de cessation d'emploi ou de changement de responsabilité dans le cadre de sa fonction),

b) il a appris ou il suspecte une compromission de sa clé privée,

c) il a changé de nom. En l'absence de demande formulée par l'abonné, l'autorité d'enregistrement ou l'autorité locale d'enregistrement compétente est tenue de demander la révocation d'un certificat d'abonné pour l'un ou l'autre des motifs ci-dessus. L'autorité d'enregistrement ou l'autorité locale d'enregistrement compétente doit aussi engager la procédure de révocation d'un certificat d'abonné en cas de violation substantielle de l'accord d'abonnement.

4.4.9 Recouvrement de clés

Les autorités de certification pourront, de manière optionnelle, prévoir le recouvrement des (seules) clés de déchiffrement des abonnés. Le mécanisme qui garantit la non-répudiation est le suivant : l'abonné produit sa paire de clés de signature sur son propre système et transmet uniquement sa clé publique de vérification à l'autorité de certification lors de la procédure d'enregistrement.

4.5 Algorithmes cryptographiques

En fonction des besoins, on pourra utiliser aussi bien des algorithmes symétriques (à clé secrète) que des algorithmes asymétriques (à clé publique). Un algorithme qui serait interdit en vertu de la loi nationale d'un pays ne devra pas être utilisé pour l'échange de documents constitutifs de la demande internationale provenant de ce pays. Les algorithmes mis en œuvre dans un matériel ou un logiciel ne devront pas être employés d'une manière contraire aux restrictions à l'exportation imposées par le pays d'origine pour les matériels ou les logiciels considérés. Tout algorithme employé entre deux offices de propriété industrielle devra être communiqué aux deux parties.

Dans la mesure du possible, l'algorithme *rsaEncryption* sera utilisé comme algorithme de chiffrement asymétrique et l'algorithme dES-EDE3-CBC comme algorithme de chiffrement symétrique. Le même algorithme de chiffrement asymétrique devrait être utilisé pour créer les certificats, signatures et enveloppes numériques. D'autres algorithmes de chiffrement (comme la norme de chiffrement avancé –ou

Advanced Encryption Standard–) seront inclus dans cette section lorsqu'ils seront disponibles et après accord général de la part des offices.

4.6 Algorithmes de compression

À la chaîne de caractères du message devra être appliqué l'algorithme de compression à sens unique SHA-1 ou le groupe SHA-2, aux fins de créer une empreinte du message. D'autres algorithmes de chiffrement seront inclus dans cette section après consultation et accord général de la part des offices.

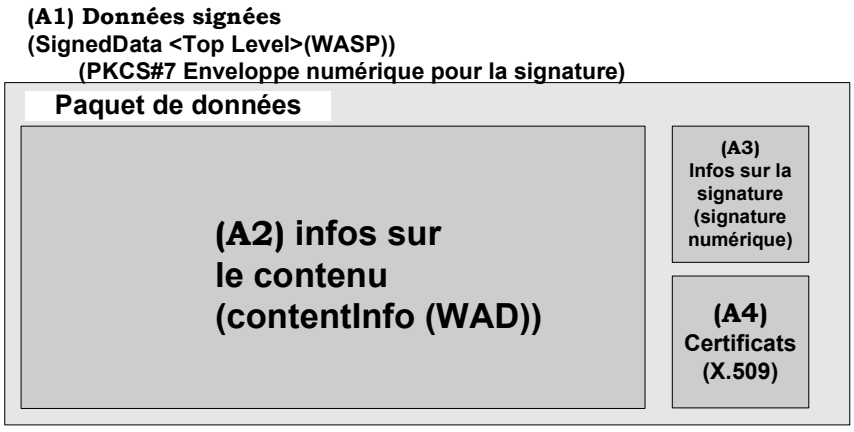
4.7 Enveloppement des données

Les données d'un document électronique qui font l'objet d'un chiffrement destiné à en assurer la confidentialité aux fins de l'échange de documents de demande internationale doivent respecter le format et la pratique spécifiés dans la partie consacrée à la définition du contenu du type *Signed and Enveloped Data* (données signées et enveloppées) figurant dans la version 1.5 de la norme PKCS#7 de RSA Laboratories relative à la syntaxe du message cryptographique.

5. TYPES DE PAQUETS ICP SELON LA NORME E-PCT

5.1 Paquet compacté et signé (WASP)

Les spécifications PKCS#7 sont appliquées pour la production d'un type "données signées" pour la signature.



Règles de production des données signées PKCS#7 aux fins de certification

(SHA-1 est indiqué à titre d'exemple ci-dessous bien que le groupe SHA-2 soit aussi utilisé parallèlement à SHA-1)

Identificateur d'objet pour sha-1	L'identificateur d'objet que nous adoptons pour sha-1 est défini dans les protocoles d'interconnexion OIW, partie 12. La définition est la suivante : **Sha-1 OBJECT IDENTIFIER ::= {iso (1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}**
Identificateur d'objet pour le chiffrement RSA	L'identificateur d'objet pour le chiffrement RSA est défini dans la *norme de chiffrement RSA PKCS#1.* La définition est la suivante : **Pkcs-1 OBJECT IDENTIFIER ::= iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1}** **RsaEncryption OBJECT IDENTIFIER ::={pkcs-1 1}**
Identificateur d'objet pour triple DES	dES-EDE3-CBC OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7}

Tableau A1 Données signées (SignedData)(WASP), premier niveau

Nom d'article	Article PKCS#7	Contenu
Version	Version	Mettre la valeur entière '1'
Jeu d'identificateurs d'algorithme	DigestAlgorithms	
Identificateur d'algorithme	AlgorithmIdentifier	Mettre UN SEUL **jeu** d'identificateurs d'algorithme {sha-1}
Information sur le contenu	ContentInfo	Mettre un élément d'information sur le contenu (voir le tableau A2)
Certificats	Certificates	Mettre un élément Certificats (voir le tableau A4)
Listes de certificats révoqués	Crls	Vide (ne rien mettre)
Information sur le signataire	SignerInfos	Mettre un élément d'information sur le signataire (voir le tableau A3)

Tableau A2 Informations sur le contenu (contentInfo) (WAD), premier niveau

Nom d'article	Article PKCS#7	Contenu
Type de contenu	ContentType	Mettre un identificateur d'objet {pkcs-7 1}
Contenu	Content	Mettre les données utilisateur (binaires)

Tableau A3 Informations sur le signataire (signerInfos), premier niveau

Nom d'article	Article PKCS#7	Contenu
Version	Version	Mettre la valeur entière '1'
Émetteur et numéro d'ordre	IssuerAndSerialNumber	Émetteur du certificat et numéro d'ordre de celui-ci selon la spécification X.509 (concernant le certificat du signataire)
Jeu d'algorithmes de compression	DigestAlgorithm	
Identificateur d'algorithme	AlgorithmIdentifier	Mettre UN SEUL **jeu** d'identificateurs d'algorithme {sha-1} pour la production d'une empreinte de signature numérique
Attributs authentifiés	AuthenticatedAttributes	Vide (ne rien mettre)
Algorithme de chiffrement du condensé	DigestEncryptionAlgoritm	Identificateur d'OBJET de l'algorithme de chiffrement du condensé (algorithme recommandé : rsaEncryption[2])
Condensé chiffré	EncryptedDigest	Condensé des données du message; le contenu est chiffré au moyen de la clé privée du signataire
Attributs non authentifiés	UnauthenticatedAttributes	Vide (ne rien mettre)

Tableau A4 Certificats (certificates), premier niveau

Nom d'article	Article PKCS#7	Contenu
Jeu de certificats	ExtendedCertificatesAndCertificates	
Le certificat X.509	Certificate (défini dans la spécification X.509)	Mettre UN SEUL **jeu de** données de certificat X.509

Si l'algorithme de chiffrement, qui est utilisé dans les certificats numériques en adjonction à une signature numérique, diffère de l'algorithme décrit dans la présente spécification, l'office récepteur doit notifier cet algorithme au Bureau international.

6. TYPES DE CERTIFICATS/SIGNATURES

Les figures 2 à 6 illustrent les différences entre les types de "certificats numériques" et de "signatures électroniques" disponibles. Chaque schéma illustre une "boîte" qui représente le paquet compacté et signé. Les schémas ont été délibérément simplifiés pour exclure les détails techniques qui ne se rapportent pas directement aux éléments essentiels. Ainsi, les détails relatifs aux paquets chiffrés et signés ne sont pas illustrés.

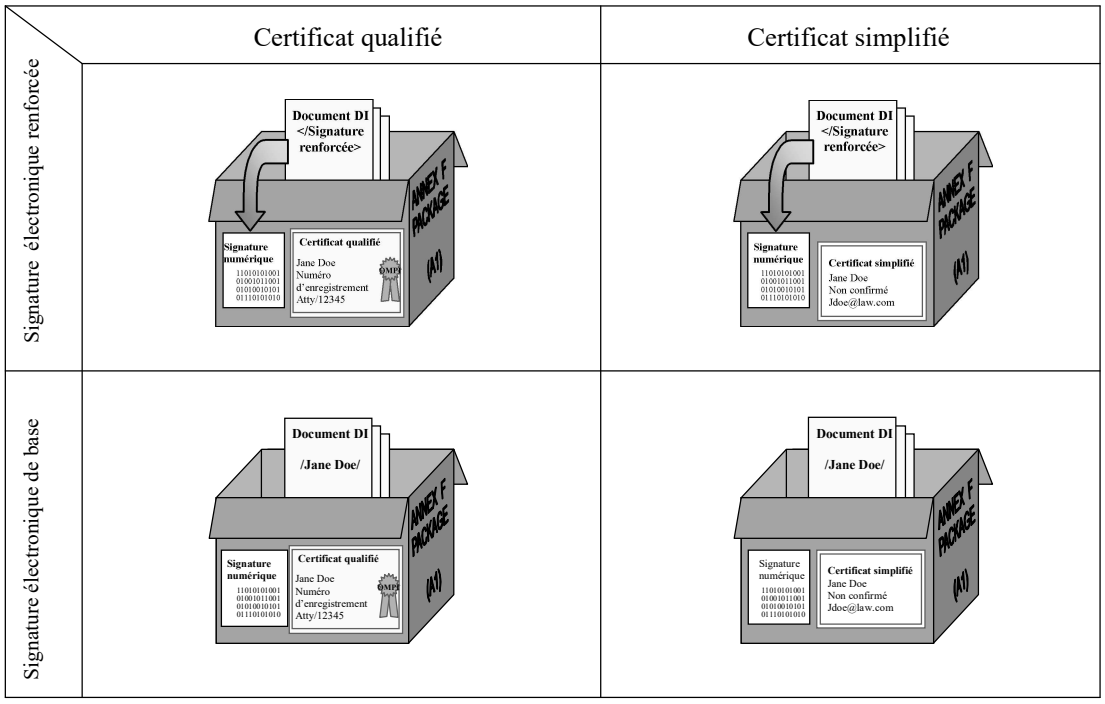


Figure 2 – Types de certificats/signatures

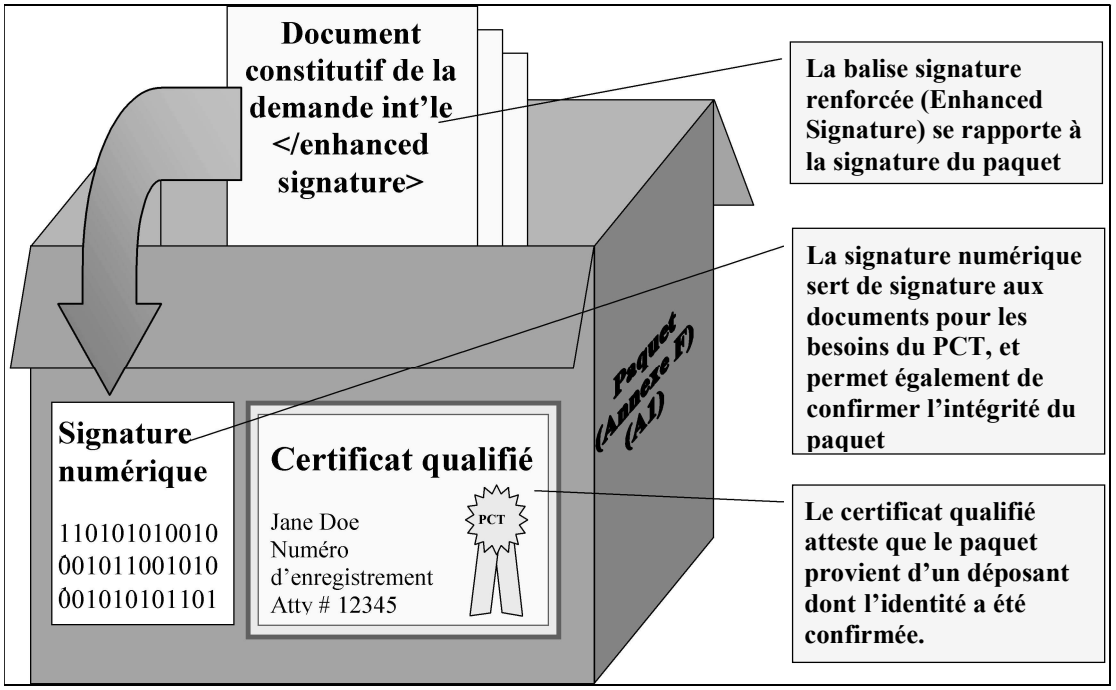


Figure 3 – Signature électronique renforcée / certificat qualifié

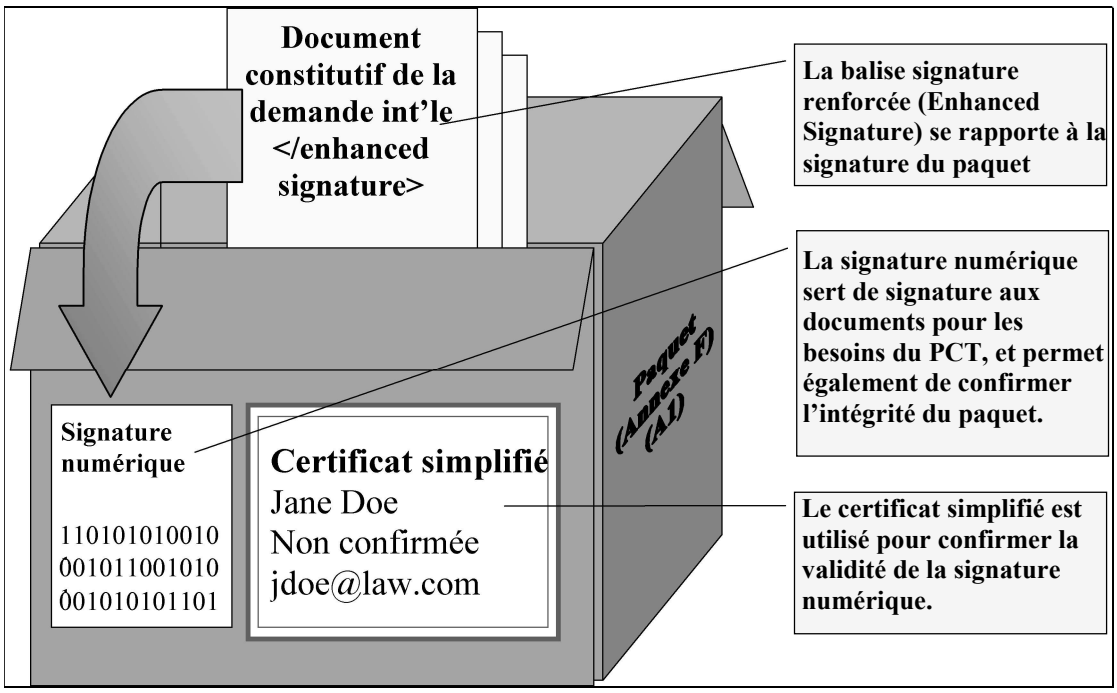


Figure 4 – Signature électronique renforcée / certificat simplifié

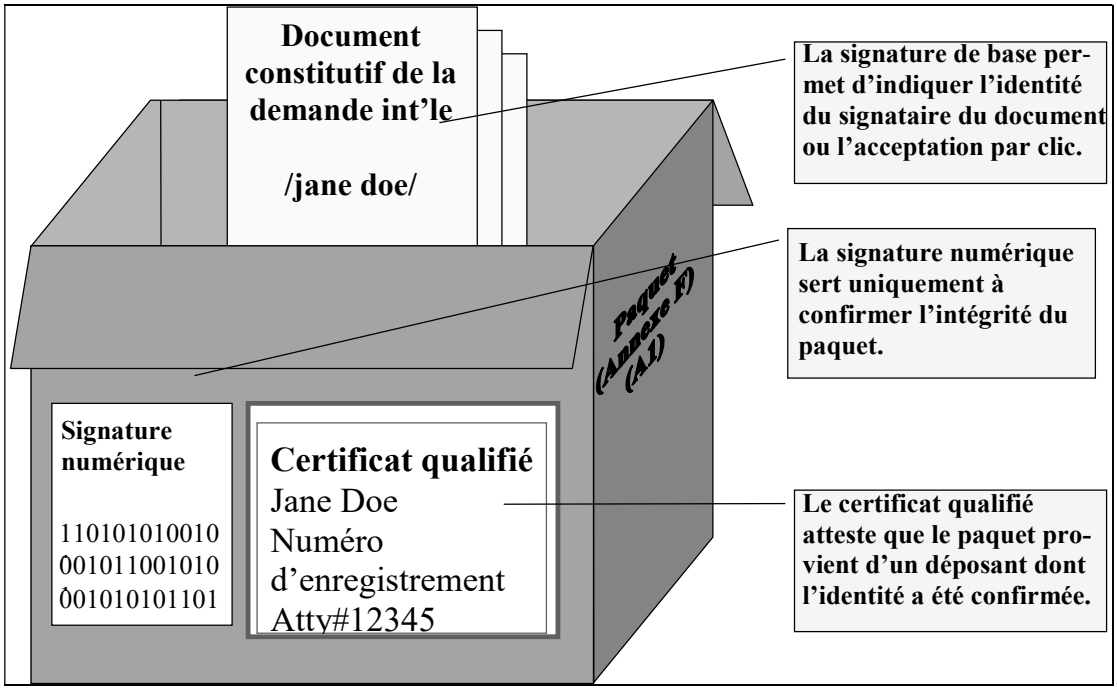


Figure 5 – Signature électronique de base / certificat qualifié

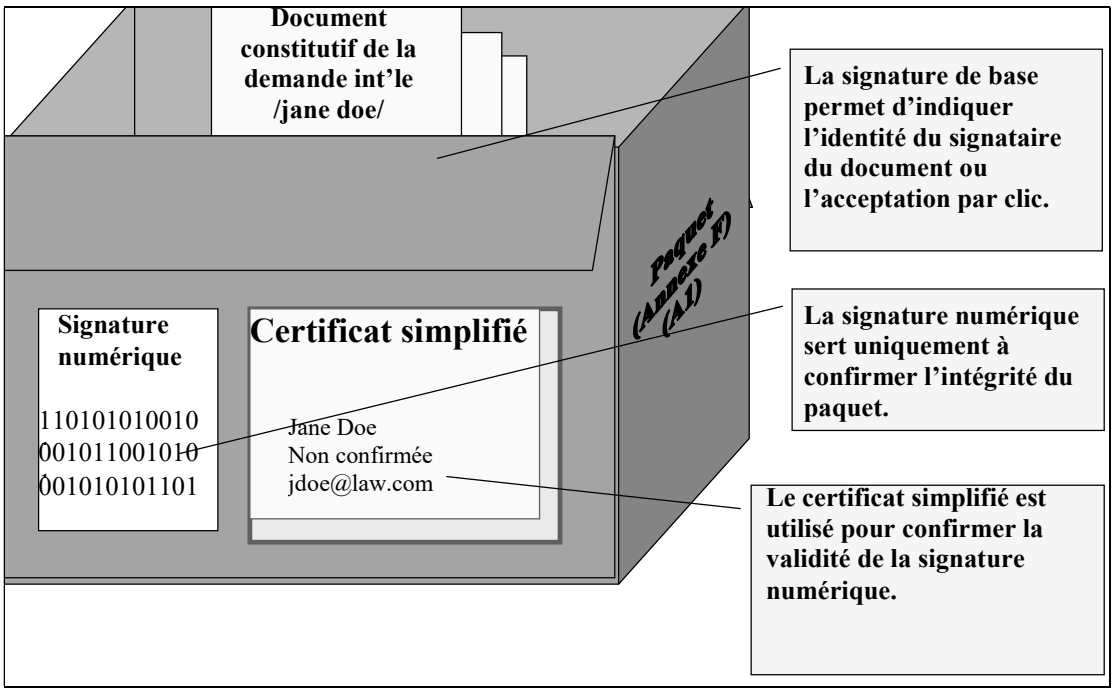


Figure 6 – Signature électronique de base / certificat simplifié

7. GLOSSAIRE

Abonné

Entité qui 1) est le sujet nommé ou identifié dans un certificat émis à son intention, 2) détient une clé privée qui correspond à une clé publique indiquée dans le certificat, et 3) est la personne à laquelle des messages signés numériquement et vérifiés par le biais du certificat doivent être attribués. Aussi appelée “sujet”.

Adresse de courrier électronique vérifiable

Une adresse de courrier électronique dont il peut être vérifié qu’elle appartient à l’abonné qui est titulaire d’un certificat numérique. La vérification sera réalisée en envoyant par exemple un courrier électronique contenant l’information requise pour la récupération du certificat par l’abonné. Si l’adresse de courrier électronique est incorrecte, l’autorité de certification n’envoie pas à l’abonné l’information nécessaire pour obtenir le certificat.

Algorithme cryptographique (asymétrique) à clé publique

Algorithme cryptographique qui utilise deux clés liées, une clé publique et une clé privée. Les deux clés ont pour caractéristique qu’il n’est pas possible de déduire la clé privée de la clé publique.

Algorithme cryptographique (symétrique) à clé secrète

Algorithme cryptographique qui utilise une clé unique et secrète à la fois pour le chiffrement et le déchiffrement.

Autorité de certification

Une autorité de certification est une partie de confiance qui émet et révoque des certificats de clé publique pour une communauté d’utilisateurs. L’autorité de certification doit vérifier les informations qui figurent sur les certificats de clé publique. L’autorité de certification recourt à ses propres serveurs ou systèmes informatiques et respecte les politiques et les procédures applicables à l’exploitation de ces serveurs. Le terme “serveur” désigne le matériel et le logiciel qui produisent les certificats et les listes de certificats révoqués.

Deux types d’autorités de certification sont permises par la norme E-PCT, à savoir les autorités de certification des offices ou les autorités de certification publiques. L’autorité de certification d’un office est une autorité de certification qui délivre des certificats qui portent le nom de cet office (que le certificat soit produit à l’intérieur ou à l’extérieur de l’office). Une autorité de certification publique est une autorité de certification qui délivre des certificats qui ne portent pas le nom de l’office, mais qui est reconnue par certains offices comme remplissant les conditions pour délivrer des certificats pour des transactions E-PCT.

Autorité de certification de l’office

Voir Autorité de certification

Autorité de certification publique

Voir Autorité de certification

Autorité d'enregistrement

Entité responsable de l'identification et de l'authentification des sujets détenteurs des certificats, mais pas de la signature ou de l'émission des certificats (en d'autres termes, une autorité d'enregistrement est habilitée à procéder à certaines tâches liées au contrôle de l'identité au nom d'une autorité de certification). L'autorité d'enregistrement peut déléguer ses fonctions et le pouvoir correspondant à des autorités locales d'enregistrement (voir *Autorité locale d'enregistrement*).

Autorité locale d'enregistrement

Autorité qui agit au nom de l'autorité d'enregistrement en se portant garante de l'identité des abonnés (c'est-à-dire en procédant à une validation au moyen d'une forme de contrôle de l'identité). L'autorité locale d'enregistrement intervient aussi en ce qui concerne d'autres éléments relatifs à la durée de vie du certificat au nom de ses abonnés, tels que renouvellement, recouvrement des clés et services d'assistance pour les fonctions ICP.

Banque

Système servant à stocker et à rechercher des certificats et d'autres informations relatives aux certificats.

Certificat

Un certificat lie le nom d'une entité (et d'autres attributs) avec la clé publique correspondante. Aux fins de l'annexe F, un certificat doit être conforme à la recommandation X.509 de l'IUT, version 3, et doit remplir au minimum les conditions suivantes :

a) contenir une clé publique qui correspond à une clé privée sous le contrôle exclusif du sujet

b) nommer ou identifier d'une autre façon son sujet

c) identifier l'autorité de certification qui l'émet

d) indiquer sa période de validité

e) contenir un numéro d'ordre du certificat

f) inclure l'adresse de courrier électronique des entités finales

g) être signé numériquement par l'autorité de certification qui l'émet.

Certificat de clé publique

Série de données qui identifie sans ambiguïté une entité, contient la clé publique de l'entité et est signée numériquement par une partie de confiance.

Certificat valide

Certificat qui 1) a été émis par une autorité de certification, 2) a été accepté par l'abonné qui y est indiqué, 3) n'est pas expiré, et 4) n'a pas été révoqué. Par conséquent, un certificat n'est pas considéré comme valide s'il n'a pas été émis par une autorité de certification et accepté par l'abonné.

Chiffrement

En cryptographie de clé publique, la protection privée des données est obtenue grâce au chiffrement des données en utilisant la clé publique du prétendu destinataire. Dans la mesure où celui-ci est le seul à avoir accès à la clé privée correspondante, il est le seul à pouvoir déchiffrer les données.

Clé—Voir *Clé cryptographique*

Clé cryptographique (clé)

Paramètre utilisé en association avec un algorithme cryptographique, qui commande la transformation de données textuelles en clair en données textuelles chiffrées, la transformation de données textuelles chiffrées en données textuelles en clair, une signature numérique obtenue à partir de données, la vérification d'une signature numérique obtenue à partir de données, ou un code d'authentification de données obtenu à partir de données.

Clé privée

Dans le cadre de la cryptographie à clé publique, la clé privée est la partie d'une paire de clés publique et privée appartenant à un utilisateur qui n'est connue que de cet utilisateur. La clé privée d'un utilisateur sert à signer numériquement des données et à déchiffrer des données qui ont été chiffrées avec la clé publique de l'utilisateur.

Clé publique

Dans le cadre de la cryptographie à clé publique, la clé publique est la partie d'une paire de clés publique et privée appartenant à un utilisateur qui est portée à la connaissance d'autres membres de la communauté des utilisateurs par un certificat de clé publique. La clé publique d'un utilisateur est utilisée par d'autres personnes pour chiffrer des données destinées à cet utilisateur, ou pour vérifier la signature numérique de l'utilisateur.

Clé secrète

Clé cryptographique utilisée avec un algorithme cryptographique à clé secrète, qui est associée de façon univoque à une ou plusieurs entités et qui ne sera pas rendue publique. Le terme "secret" employé dans ce contexte n'indique pas un niveau de classement mais la nécessité de protéger la clé d'une éventuelle divulgation ou substitution.

Compromission

Divulgation, modification, substitution ou utilisation sans autorisation de données confidentielles (y compris les clés cryptographiques en texte clair et d'autres paramètres de sécurité fondamentaux).

Confidentialité

Caractéristique des informations confidentielles qui ne sont pas divulguées à des personnes ou entités non autorisées ou dans le cadre de fonctions non autorisées.

Connaissances partagées

Situation dans laquelle au moins deux entités détiennent séparément des éléments de clé qui, pris individuellement, ne donnent aucun renseignement sur la clé en texte clair qui sera produite lorsque les éléments de la clé seront mis ensemble dans le module cryptographique.

Cryptographie de clé publique

Technique cryptographique dans laquelle des paires de clés sont utilisées pour chiffrer et déchiffrer des données. Une paire de clé est attribuée à chaque utilisateur. L'une des clés de l'utilisateur est publique, ce qui signifie qu'elle est rendue publique à tous ceux qui en ont besoin. L'autre clé est une clé privée qui est reliée à la clé publique par un algorithme mathématique et qui n'est connue que par l'utilisateur lui-même. Les données chiffrées par l'une ou l'autre de ces clefs peuvent être déchiffrées seulement par l'autre clé de la paire de clé.

Distribution manuelle des clés

Distribution des clés cryptographiques – souvent sous la forme d'un texte clair exigeant une protection matérielle – par des moyens non électroniques, tels qu'un service de messagerie contracté à cet effet.

Domaine d'infrastructure à clé publique

Entité indépendante consistant en une ou plusieurs autorités de certification auprès desquelles les abonnés détiennent le même certificat de base ou certificat principal.

Domaine ICP – Voir *Domaine d'infrastructure à clé publique*

Horodatage

Notation indiquant, au moins, la date et l'heure exactes d'une action et l'identité de la personne qui a créé la notation.

ICP – Voir *Infrastructure à clé publique*

Identificateur d'objet

Numéro spécialement formaté enregistré auprès d'une organisation de normalisation internationalement reconnue. Il peut et devrait servir à identifier une série de documents relatifs aux politiques et aux pratiques d'une organisation en matière d'ICP.

Information d'état

Information provenant d'un module cryptographique et indiquant certaines caractéristiques de fonctionnement ou certains états du module.

Infrastructure à clé publique

Une ICP comprend au moins les services ci-après :

a) Autorité de certification

b) Autorité d'enregistrement

c) Banque de certificats et de listes de certificats révoqués

d) Logiciel client ICP de l'utilisateur

e) Politique, pratiques, procédures et normes d'exploitation

f) Plan de soutien à l'exploitation de l'infrastructure à clé publique

g) Tous les services et installations connexes

Intégrité

Propriété qui signifie que les données confidentielles n'ont pas fait l'objet de modifications ou de suppressions non autorisées et passées inaperçues.

Intégrité du message

Assurance de la transmission et de la réception non altérées d'un message de l'expéditeur vers le destinataire prévu.

Interface

Section logique d'un module cryptographique qui définit une série de points d'entrée ou de sortie donnant accès au module, y compris le flux d'informations ou l'accès physique.

Introduction manuelle de clés

Introduction de clés cryptographiques dans un module cryptographique à partir d'un formulaire imprimé, au moyen de dispositifs tels que boutons, molettes ou clavier.

Liste de certificats révoqués

Liste horodatée de certificats révoqués qui portent la signature numérique d'une autorité de certification.

Liste des autorités révoquées

Une forme de liste des certificats révoqués (voir ci-avant) qui contient des informations sur la révocation des autorités de certification.

Logiciel système

Logiciel spécial (par exemple système d'exploitation, compilateurs ou programme utilitaire) conçu pour un système informatique ou une famille de systèmes informatiques déterminé et visant à faciliter l'exploitation et la maintenance du système informatique, des programmes et des données.

Matériel

Équipement servant à traiter les programmes et les données dans un module cryptographique.

Message

Représentation numérique d'informations, y compris textes, graphiques, images et sons.

Microprogramme

Programmes et données (c'est-à-dire logiciel) stockés en permanence dans du matériel (par exemple mémoire morte, mémoire morte programmable ou mémoire morte programmable effaçable) de manière que les programmes et les données ne puissent pas être écrits ou modifiés dynamiquement pendant l'exécution (les programmes et les données stockés dans une mémoire morte programmable électroniquement effaçable sont considérés comme des logiciels et non comme des microprogrammes).

Module cryptographique

Ensemble de matériels, logiciels et microprogrammes, ou combinaisons de ces éléments, qui met en application une logique ou des fonctions cryptographiques, y compris des algorithmes cryptographiques, et qui s'inscrit dans le champ cryptographique du module.

Mot de passe

Chaîne de caractères servant à authentifier une identité ou vérifier l'autorisation d'accès.

Nom de l'émetteur

Identificateur unique de l'autorité signant le certificat. La syntaxe du nom de l'émetteur est un nom distinctif selon la recommandation X.500.

Nom distinctif

Nom particulier à chaque titulaire de certificat ou abonné. Chaque entité du domaine ICP doit avoir un nom distinctif qui soit facilement reconnaissable et qui lui soit spécifique dans le champ d'identification du sujet du certificat.

Non-répudiation

Éléments attestant l'identité du signataire d'un message et l'intégrité du message suffisamment solides et fondés pour empêcher qu'une partie ne nie de façon crédible l'origine, l'envoi ou la livraison du message et l'intégrité de son contenu.

Numéro d'identification personnel (code PIN)

Chaîne de caractères alphanumériques servant à authentifier une identité (couramment utilisés dans les applications bancaires).

Opérateur

Personne ayant accès à un module cryptographique soit directement soit par le biais d'une fonction s'exécutant pour son compte, quel que soit le rôle précis de cette personne.

Paire de clés

Deux clés reliées par un algorithme mathématique, avec pour caractéristique le fait

a) que l'une ou l'autre clé peut être utilisée pour chiffrer des données, étant entendu que seule l'autre clé de la paire peut déchiffrer les données en question; et

b) qu'il est théoriquement [pratiquement] impossible de retrouver l'une des clés si on connaît l'autre clé.

Normalement, une paire de clés est créée à la seule fin de chiffrer des données et une autre paire à la seule fin de la signature.

Paramètres de sécurité fondamentaux

Informations relatives à la sécurité (par exemple clés cryptographiques et données d'authentification telles que mots de passe et numéro d'identification personnel (code PIN)) formulées en clair ou sous une autre forme non protégée dont la divulgation ou la modification pourrait compromettre la sécurité d'un module cryptographique ou la sécurité de l'information protégée par le module.

Parrain

Organisation à laquelle l'abonné est lié (en tant qu'employé, utilisateur d'un service, partenaire commercial en qualité de client, etc.). Un parrain établit la preuve de l'identité au nom d'une autorité locale d'enregistrement ou d'une autorité d'enregistrement en ce qui concerne une personne qui lui est liée.

Période d'effet d'un certificat

Durée de validité d'un certificat. Cette période commencera normalement à la date à laquelle le certificat a été émis (ou à une date ultérieure indiquée dans le certificat) pour se terminer (ou expirer) à la date et à l'heure notées sur le certificat (sauf si le certificat a été révoqué antérieurement).

Personne responsable

Personne désignée par l'autorité d'enregistrement pour authentifier des déposants qui souhaitent obtenir des certificats en se prévalant de leur appartenance à une autorité locale d'enregistrement.

Port

Élément d'un module cryptographique par lequel des données ou des signaux peuvent entrer dans le module ou en sortir. Différents ports ne partagent pas les mêmes broches ou câbles.

Protection matérielle

Préservation d'un module cryptographique ou de clés cryptographiques ou d'autres paramètres de sécurité fondamentaux par des moyens matériels.

Protocole sur le statut du certificat en ligne

Comme cela est défini dans la norme RFC 2560, le protocole sur le statut du certificat en ligne permet aux applications de déterminer l'état (de révocation) d'un certificat identifié. Le protocole sur le statut du certificat en ligne peut être utilisé pour satisfaire certaines exigences opérationnelles afin de fournir une information sur les révocations plus à jour que celle fournie par les listes des certificats révoqués, et elle peut aussi être utilisée pour obtenir une information supplémentaire sur le statut du certificat. Un client de protocole sur le statut du certificat en ligne émet une requête de statut au gestionnaire du protocole sur le statut du certificat en ligne et il suspend son acceptation du certificat en question jusqu'à ce que ledit gestionnaire lui fournisse une réponse.

Recouvrement des clés

Accès à des informations suffisantes pour récupérer les données chiffrées.

Révocation d'un certificat

Expiration prématurée de la validité d'un certificat à compter d'une date déterminée.

Signature numérique

Transformation infalsifiable de données permettant d'établir la source (sans répudiation possible) et la vérification de l'intégrité de ces données. Transformation d'un message utilisant un système cryptographique asymétrique et une fonction de hachage de telle sorte qu'une personne disposant du message initial et de la clé publique du signataire peut déterminer avec exactitude : a) si la transformation a été réalisée au moyen de la clé privée qui correspond à la clé publique du signataire, et b) si le message initial a été modifié depuis que la transformation a été réalisée.

Sujet

Personne dont la clé publique est attestée dans un certificat. Également appelée "abonné".

Système fiable

Ensemble de matériel informatique, de logiciels et de procédures qui 1) sont raisonnablement à l’abri de tout intrusion ou usage abusif, 2) offrent un degré raisonnable de disponibilité et de fiabilité et fonctionnent correctement, 3) sont raisonnablement en mesure d’assumer les fonctions qui leur sont attribuées et 4) sont conformes aux procédures de sécurité généralement acceptées.

[L’appendice III de l’annexe F suit]

APPENDICE III
NORME COMMUNE DE BASE POUR LE DÉPÔT ÉLECTRONIQUE

1. INTRODUCTION

a) Le présent appendice contient la “norme commune de base” pour le dépôt électronique des demandes internationales, dont il est question dans les instructions 701.v) et 703.b) et c).

b) Chaque office récepteur qui accepte le dépôt de demandes internationales par la voie électronique définit ses exigences conformément à l’annexe F et à l’instruction 703.b) (en ce qui concerne les conditions matérielles) et c) (en ce qui concerne la signature). L’office récepteur est tenu d’accepter toute demande internationale remplissant ces conditions.

c) En outre, en vertu de l’instruction 703.b) et c), chaque office récepteur qui accepte le dépôt des demandes internationales sous forme électronique est dans l’obligation d’accepter, en plus de toute demande internationale remplissant les exigences prévues au paragraphe b) ci-dessus, toute demande internationale remplissant les exigences de la présente norme commune de base, sous réserve de toute réserve transitoire présentée selon l’instruction 703.f) convient de noter que la norme commune de base elle-même comporte un certain nombre d’options parmi lesquelles l’office récepteur doit effectuer un choix.

d) En vertu de l’article 27.1, les dispositions de la septième partie et de l’annexe F relatives à la forme ou au contenu de la demande internationale, y compris la norme commune de base, seront automatiquement applicables par les offices désignés. Les communications entre les déposants et les offices désignés ne seront cependant pas soumises, en général, à l’annexe F.

2. EXIGENCES DE LA NORME COMMUNE DE BASE

Toute demande internationale est conforme à la norme commune de base

– *en ce qui concerne le format électronique de document, lorsqu’elle remplit les critères suivants :*[25]

a) les documents constitutifs de la demande sont codés en format XML (voir Annexe F, section 3.1.1.1), à l’aide, au choix, conformément aux prescriptions de l’office récepteur,

i) du jeu de caractères Unicode 3.0 (norme internationale ISO/IEC 10646:2000) selon la norme de codage de caractères UTF-8 ou

[25] Voir l’instruction 703.b)i) et d).

ii) d'un jeu de caractères décrit dans le répertoire d'Unicode 3.0 et d'une norme de codage spécifiés par l'office récepteur conformément à ce qui est prévu dans les appels à commentaires RFC 2277 et 2130 de l'*Internet Engineering Task Force* (IETF) (voir l'annexe F, section 3.1.1.1) à condition que ce schéma de codage de caractères soit inscrit dans le registre Charset de l'autorité chargée de l'attribution des numéros de l'Internet (Internet Assigned Numbers Authority – IANA) et que l'utilisation de ce schéma de codage est permis par le logiciel de dépôt électronique mentionné dans le paragraphe g).[26]

b) Les listages des séquences sont présentés dans le format électronique de document indiqué au paragraphe 40 de la Norme relative à la présentation du listage des séquences de nucléotides et d'acides aminés dans les demandes internationales de brevet déposées selon le PCT ("fichier texte selon l'annexe C et la norme ST.25"; voir le paragraphe 40 de l'annexe C des instructions administratives et la norme ST.25 de l'OMPI; voir aussi la section 3.1.1.2 de l'annexe F);

c) les dessins sont en format TIFF, selon ce que prévoit l'office récepteur (voir la section 3.1.3.1 de l'annexe F);

– *en ce qui concerne les moyens de transmission, lorsqu'elle remplit les critères suivants :*[27]

d) lorsque l'office récepteur accepte le dépôt en ligne de demandes internationales et que c'est ainsi que la demande internationale en question est déposée : la demande internationale est transmise à l'aide du protocole sur l'interopérabilité en matière de dépôt électronique (voir la section 5.1 de l'annexe F);

e) lorsque l'office récepteur accepte le dépôt de demandes par des moyens physiques et que c'est ainsi que la demande internationale est déposée : la demande internationale est archivée sur disquette 3,5 pouces ou sur disque compact enregistrable, selon ce qu'a prévu l'office récepteur (voir l'appendice IV de l'annexe F);

– *en ce qui concerne l'empaquetage électronique, lorsqu'elle remplit les critères suivants :*[28]

f) la demande internationale est empaquetée sous la forme d'un paquet compacté et signé (WASP), établi à l'aide d'un certificat numérique simplifié délivré par l'office récepteur ou le Bureau international (voir la section 4.2.1 de l'annexe F);

– *en ce qui concerne le logiciel de dépôt électronique, lorsqu'elle remplit les critères suivants :*[29]

---

[26] L'introduction d'autres schémas de codage par l'office récepteur doit faire l'objet d'un accord préalable entre l'office récepteur et le Bureau international (qui produit le logiciel auquel il est fait référence au paragraphe g)).

[27] Voir l'instruction 703.b)ii) et d).

[28] Voir l'instruction 703.b)iii) et d).

[29] Voir l'instruction 703.b)iv) et d).

g) la demande internationale est établie et déposée à l'aide du logiciel mis à disposition à cette fin par le Bureau international[30] (voir la section 6 de l'annexe F);

– *en ce qui concerne les virus, etc., lorsqu'elle remplit les critères suivants* :[31]

h) la demande internationale ne comporte aucun virus ni autre forme d'éléments malveillants (voir la section 3.1 de l'annexe F);

– *en ce qui concerne la signature, lorsqu'elle remplit les critères suivants* :[32]

i) la demande internationale est signée au moyen d'une signature électronique de base conforme à l'annexe F (voir la section 3.3 de l'annexe F).

[L'appendice IV de l'annexe F suit]

[30] Le Bureau international fournit un logiciel qui est conforme à toutes les exigences prévues dans la norme commune de base ainsi qu'à certaines variantes prévues dans la présente annexe. L'utilisation de ce logiciel n'est pas obligatoire, mais tout déposant est en droit de l'utiliser, auquel cas l'office récepteur doit accepter la demande internationale concernée conformément à l'instruction 703.b)iv) (sauf s'il a émis une réserve en vertu de l'instruction 703.f à cet égard) (voir la section 6 de l'annexe F).

[31] Voir l'instruction 703.b)v) et d).

[32] Voir l'instruction 703.c) et d). Il convient de noter que s'il suffit, aux fins du dépôt, que la signature soit conforme à la norme de base commune, il peut être exigé ultérieurement que les exigences de l'office récepteur soient respectées conformément à l'instruction 704.g).

APPENDICE IV
UTILISATION DE SUPPORTS MATÉRIELS AUX FINS DE LA NORME E-PCT

1. INTRODUCTION

a) Le présent appendice définit les prescriptions applicables par les déposants pour le dépôt de documents sous forme électronique sur support matériel lorsque l'office récepteur a notifié au Bureau international en vertu de l'instruction administrative 710.a) qu'il est prêt à accepter le dépôt sous forme électronique sur support matériel[33]

i) de demandes internationales en vertu de l'instruction 703 (voir l'instruction administrative 710.a)i)), ou

ii) d'autres types de documents en vertu de l'instruction 703 (voir l'instruction administrative 710.a)iii)).

a-*bis*) Le présent appendice définit aussi les prescriptions à respecter par les déposants pour le dépôt des listages des séquences sous forme électronique sur un support matériel lorsque l'administration chargée de la recherche internationale ou l'administration chargée de l'examen préliminaire international (ci-après dénommée "administration") a notifié au Bureau international en vertu des instructions administratives 513.f) et 610.e), respectivement, qu'elle exige que ces listages des séquences lui soient remis, aux fins de la recherche internationale et de l'examen préliminaire international, respectivement, sous forme électronique sur un support matériel.

b) Tout office récepteur qui a notifié au Bureau international en vertu de l'instruction administrative 710.a) qu'il est prêt à accepter le dépôt de documents sous forme électronique sur un support matériel et toute administration qui a notifié au Bureau international en vertu des instructions administratives 513.f) ou 610.e) qu'elle exige que les listages des séquences lui soient fournis sous forme électronique sur un support matériel doit, en sus des indications requises dans ces instructions, indiquer les types de support matériel et le nombre d'exemplaires de supports matériels exigés.

c) Ne sont acceptables que les types de support matériel et les formats indiqués dans la section 4 du présent appendice, étant entendu que tout office récepteur visé à l'alinéa a) accepte, lorsque l'administration chargée de la recherche internationale ou, le cas échéant, au moins une des administrations chargées de la recherche internationale compétentes pour effectuer la recherche internationale concernant les demandes internationales déposées auprès de cet office récepteur a notifié au Bureau international en vertu de l'instruction 513.f) qu'elle exige que les listages des séquences lui soient fournis sous forme électronique sur un support matériel aux fins de la recherche internationale, au moins un type de support matériel accepté par cette administration ou, le cas échéant, par au moins une de ces administrations.

d) Les formats électroniques de document sont limités à ceux indiqués dans la partie principale de la présente annexe.

---

[33] Les mots et expressions utilisés dans le présent appendice ont la même signification que ceux qui sont utilisés dans la partie principale de l'annexe F; voir le glossaire et la liste des abréviations à la fin de cette partie.

2. PRESCRIPTIONS APPLICABLES AU DÉPÔT ÉLECTRONIQUE SUR UN SUPPORT MATÉRIEL

a) Tout support matériel doit être conforme aux normes indiquées à la section 4 du présent appendice et son contenu doit être codé dans l'un des formats électroniques de document indiqués dans la partie principale de la présente annexe.

b) Le contenu de chaque support matériel doit :

i) sous réserve de l'alinéa b-bis), être empaqueté conformément à la section 4.1 ou 4.2 de la partie principale de la présente annexe; et

ii) sous réserve de l'alinéa c), figurer dans un fichier unique qui sera placé dans le répertoire de base du support matériel.

b-*bis*) Lorsque le support matériel contient un listage des séquences fourni en vertu de la règle 13*ter*, il n'est pas nécessaire que le contenu du support matériel soit empaqueté, à moins que le fichier contenant ce listage soit compressé conformément à l'alinéa c-*bis*).

c) L'office récepteur ou l'administration peut limiter la taille des fichiers inscrits sur le support matériel. Si, pour satisfaire à cette prescription, un document doit être scindé en plusieurs fichiers inscrits sur un seul support matériel, ou si un document doit être scindé en plusieurs fichiers à inscrire sur plusieurs supports matériels, cette scission doit être faite de telle sorte que les fichiers puissent être réunis pour former un fichier contigu unique sans contenu reproduit ou manquant, conformément à la norme de scission de fichier ZIP ou à la commande de "scission" Unix/Linux. Dans les deux cas, les noms de fichier doivent correspondre aux normes par défaut de scission et de recréation d'un fichier avec un nom d'origine particulier, par exemple, pour "sequence-list.txt" concernant les fichiers ZIP scindés : "sequence-list.z01", "sequence-list.z02", "sequence-list.zip"; ou, s'agissant des fichiers Unix scindés : "sequence-listaa.txt", "sequence-listab.txt", etc.

c-*bis*) La compression des fichiers est acceptable dans la mesure où elle est faite, conformément à la section 4.1.1 de la partie principale de la présente annexe, selon la norme ZIP (cette norme donne au logiciel de compression le choix parmi un certain nombre d'algorithmes de compression; la méthode de compression sera la "déflation" avec l'option compression normale).

d) Chaque support matériel doit être placé dans un boîtier rigide, envoyé dans une enveloppe postale matelassée non scellée et accompagné d'une lettre de transmission sur papier. La lettre de transmission doit mentionner le contenu du support matériel (par exemple : "demande internationale déposée en vertu de l'instruction 703" ou "[*nom d'un autre type de document*] déposé en vertu de l'instruction 703"). La lettre de transmission doit également indiquer, pour chaque support matériel, le format machine (par exemple : IBM-PC), le système d'exploitation compatible (par exemple : MS-DOS, MS-Windows, Unix), la liste des fichiers contenus sur le support, avec indication de leur nom, de leur taille en octets et de leur date de création, ainsi que tout autre renseignement supplémentaire nécessaire pour identifier, conserver et interpréter les informations figurant sur le support matériel. Les supports matériels envoyés à l'office ne sont pas retournés au déposant.

e) Lorsque l'office récepteur exige, en vertu de la règle 11.1.b), qu'une demande internationale déposée sous forme électronique sur un support matériel soit déposée en deux ou trois exemplaires, ou lorsqu'une administration présente une telle exigence en ce qui concerne la fourniture d'un listage des séquences aux fins de la recherche internationale ou de l'examen préliminaire international, la lettre de transmission accompagnant les supports matériels doit comporter une déclaration indiquant que les exemplaires des supports matériels sont identiques. Dans l'hypothèse où les exemplaires des supports matériels ne seraient pas identiques, l'office ou l'administration utilise le support matériel portant l'étiquette "EXEMPLAIRE 1" (voir l'alinéa f)vi)) aux fins de la poursuite du traitement.

f) Tout support matériel doit également porter une étiquette contenant les renseignements suivants :

i) le nom du ou des inventeurs (voir aussi l'instruction administrative 105);

ii) le titre de l'invention;

iii) le numéro de la demande internationale et la date du dépôt international ou, s'il ou si elle n'est pas connu du déposant, le nom de l'office récepteur auprès de qui la demande a été déposée et la référence du dossier utilisée par la personne qui a effectué le dépôt de la demande afin de l'identifier;

iv) la date à laquelle les fichiers qui figurent dans le support matériel ont été créés ou modifiés pour la dernière fois;

v) lorsque le document figure sur plus d'un support matériel, la numérotation de chacun de ces supports matériels comme suit (exemple : le document est contenu sur trois supports matériels) : 'DISQUE 1/3', 'DISQUE 2/3', 'DISQUE 3/3';

vi) lorsque l'office récepteur ou l'administration exige plus d'un exemplaire du support matériel, la numérotation de chaque exemplaire remis, comme suit (exemple : trois exemplaires du support matériel sont remis) : "EXEMPLAIRE 1", "EXEMPLAIRE 2", "EXEMPLAIRE 3" (voir aussi l'alinéa e)); et

vii) une mention du contenu du support matériel (par exemple : "DEMANDE INTERNATIONALE – INSTRUCTION 703"; "MODIFICATIONS ARTICLE 19"; "MODIFICATIONS ARTICLE 34"; "LISTAGE DES SÉQUENCES – RÈGLE 13*ter*"; "LISTAGE DES SÉQUENCES – CORRECTION – RÈGLE 13*ter*"; "LISTAGE DES SÉQUENCES – RECTIFICATION – RÈGLE 13*ter*"; "LISTAGE DES SÉQUENCES – MODIFICATION – RÈGLE 13*ter*").

3. REFERENCES

ISO/IEC 9529-1:1989 Systèmes de traitement de l'information -- Échange de données sur cartouches à disquettes de 90 mm (3,5 in) utilisant un enregistrement à modulation de

fréquence modifiée à 15 916 ftprad sur 80 pistes sur chaque face -- Partie 1 : Caractéristiques dimensionnelles, physiques et magnétiques

ISO/IEC 9529-2:1989 Systèmes de traitement de l'information -- Échange de données sur cartouches à disquettes de 90 mm (3,5 in) utilisant un enregistrement à modulation de fréquence modifiée à 15 916 ftprad sur 80 pistes sur chaque face -- Partie 2 : Schéma de piste

ISO 9660:1988 Traitement de l'information -- Structure de volume et de fichier des disques optiques compacts à mémoire fixe (CD-ROM) destinés à l'échange d'information

Norme ECMA-119, Structure de volume et de fichier de CD-ROM pour l'échange d'information

ISO/IEC 13346 Technologies de l'information -- Structure de volume et de fichier de moyens d'écriture unique et de réécriture utilisant un enregistrement non séquentiel pour l'échange d'information

Norme ECMA-167, Structure de volume et de fichier pour des moyens d'écriture unique et de réécriture utilisant un enregistrement non séquentiel pour l'échange d'information

Optical Storage Technology Association Universal Disk Format Specification (OSTA UDF)

ISO/IEC 10149:1995 Technologies de l'information -- Échange de données sur des disques optiques de diamètre 120 mm à lecture seule (CD-ROM)

Norme ECMA-130, Echange de données sur des disques de données optiques à lecture seule de diamètre 120 mm (CD-ROM)

ISO/IEC 16448:1999 Technologies de l'information -- Disque DVD à lecture seule de diamètre 120 mm

Norme ECMA-267, Disque DVD à lecture seule de diamètre 120 mm

Norme ECMA-279, Disque DVD enregistrable (DVD-R) de diamètre 80 mm (1,23 giga-octets par face) et de diamètre 120 mm (3,95 giga-octets par face)

4. TYPES ET FORMATS DES SUPPORTS ACCEPTÉS

4.1 Disquette de 3,5 pouces

Type

Disquette de 3,5 pouces double face, haute densité, 135 TPI, 80 pistes par face, conforme à la norme ISO/IEC 9529

Spécification de format

1.44MB, format DOS compatible IBM PC

4.2 CD-ROM

Type

CD-ROM de diamètre 120 mm, conforme à la norme ISO/IEC 10149:1995

Spécification de format

ISO 9660, 650MB

4.3 CD-R

Type

Disque compact enregistrable (CD-R) de diamètre 120 mm

Spécification de format

ISO 9660, 650MB

4.4 DVD

Type

Disque DVD de diamètre 120 mm à lecture seule, conforme à la norme ISO/IEC 16448:1999

Spécification de format

4,7GB, conforme à la norme ISO 9660 ou à la norme OSTA UDF (à partir de la version 1.02)

4.5 DVD-R

Type

Disque DVD enregistrable (DVD-R) de diamètre 120 mm (3,95 giga-octets par face), conforme à la norme ECMA-279

Spécification de format

3,95GB, conforme à la norme ISO 9660 ou à la norme OSTA UDF (à partir de la version 1.02)

[Fin de l'appendice, de l'annexe
et du document]