



C. PCT 920
– 07.2

Le 16 juin 2003

Madame,
Monsieur,

Modifications des Instructions administratives du PCT

*Norme concernant le dépôt et le traitement électroniques
des demandes internationales :*

Modifications de l'annexe F, y compris l'appendice I

1. La présente circulaire concerne les modifications apportées à l'annexe F des instructions administratives du Traité de coopération en matière de brevets (PCT), y compris l'appendice I, qui sont promulguées avec effet au 19 juin 2003.
2. La septième partie et l'annexe F relatives, respectivement, au cadre juridique et à la norme technique nécessaires à la mise en œuvre du dépôt et du traitement électroniques des demandes internationales sont entrées en vigueur le 7 janvier 2002 (voir le document PCT/AI/1 Rev.1 Add.2 du 20 décembre 2001 et le numéro spécial S-04/2001, du 27 décembre 2001, de la *Gazette du PCT*). L'annexe F a par la suite fait l'objet de modifications qui sont entrées en vigueur le 12 décembre 2002 (voir le document PCT/AI/1 Rev.1 Add.5 du 25 novembre 2002 et le numéro 50/2002, du 12 décembre 2002, de la *Gazette du PCT*).
3. Les présentes modifications sont fondées sur le texte des propositions de modification de l'annexe F qui ont été reçues ou préparées par le Bureau international en 2002. Ces propositions sont disponibles sur le site Web de l'OMPI (voir http://pcteasy.wipo.int/efiling_standards/EFPPageF.htm). Un certain nombre de modifications ont été apportées aux propositions après consultation, conformément à la règle 89.2.b), des offices de brevets nationaux ou régionaux des États contractants du PCT, ou agissant en leur nom, des administrations internationales du PCT, des organisations intergouvernementales intéressées, ainsi que de certaines organisations non-gouvernementales représentant les utilisateurs du système du PCT (voir la circulaire C. PCT 885 datée du 25 novembre 2002).

/...

4. Suite à cette consultation, l'annexe F est modifiée comme suit :

- i) section 3.1.1.1.1 – nouvelle section “Numérotage des paragraphes dans les documents XML (description)”;
- ii) section 3.2 – document de référence ajouté à la figure 2;
- iii) section 4.2.1 – modifications relatives à la description des signataires;
- iv) section 4.2.3 – nouvelle section “WASP combiné (C-WASP)”;
- v) section 4.3 – nouvelle section “Convention recommandée de nommage des dossiers”;
- vi) section 5.1.3 – nouvelle section “Protocole sur les couches du système applicatif en matière de notification” (y compris les nouvelles figures 6, 10, 11, et 12);
- vii) sections 5.1.4 à 5.1.9 – quelques modifications et ajouts au protocole sur l'interopérabilité en matière de dépôt électronique;
- viii) sections 5.2.1 à 5.2.3 – quelques modifications et ajouts en ce qui concerne les combinaisons paquet/transmission.

5. En outre, l'appendice I de l'annexe F est modifié comme suit :

- i) section 3.9 – nouvelle section “Tableau”;
- ii) section 3.10 – nouvelle “Correction d'office”;
- iii) section 4.1 – modifications apportées à la section “En-tête du paquet”;
- iv) sections 4.3 et 4.4 – nouvelles sections “Répertoire d'envoi” et “Répertoire de réception”;
- v) section 5 – nouvelle section “Autres DTDs de la norme E-PCT” comprenant:
 - section 5.1 “Formulaire de demande d'examen préliminaire international”,
 - section 5.2 “Informations reçues par l'administration chargée de l'examen préliminaire international à partir du formulaire de demande d'examen préliminaire international”,
 - section 5.3 “Feuille de taxes du chapitre II”,

/...

- section 5.4 “Données bibliographiques du document de priorité”,
- section 5.5 “Corps du document de priorité”,
- section 5.6 “Données bibliographiques publiées par le Bureau international”,
- section 5.7 “Publication par le Bureau international”, et
- section 5.8 “Dépôt de modifications, et le cas échéant de déclarations, selon les articles 19 et 34.2)b)” (ancienne section 3.5);

vi) corrections et ajouts mineurs apportés aux DTDs existantes.

6. Le texte des modifications de la partie principale de l’annexe F et de son appendice I figure, respectivement, dans le document PCT/AI/1 Rev.1 Add.7, ci-joint, et dans le document PCT/AI/1 Rev.1 Add.8 (qui est disponible, avec le document PCT/AI/1 Rev.1 Add.7, sur le site Web de l’OMPI à l’adresse suivante : <http://www.wipo.int/pct/fr/texts/index.htm>). Des copies papier du document PCT/AI/1 Rev.1 Add.8 sont fournies par le Bureau international sur demande.

7. Les modifications seront promulguées dans le numéro 25/2003, du 19 juin 2003, de la *Gazette du PCT*.

Veillez agréer, Madame, Monsieur, l’assurance de ma considération distinguée.



Francis Gurry
Sous-directeur général

Pièce jointe : document PCT/AI/1 Rev.1 Add.7

OMPI



PCT/AI/1 Rev.1 Add.7

ORIGINAL : anglais

DATE : 28 mai 2003

F

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) : MODIFICATIONS DE L'ANNEXE F

texte en vigueur à partir du 19 juin 2003

1. Le présent document contient le texte de modifications, prenant effet au 19 juin 2003, des instructions administratives du Traité de coopération en matière de brevets (PCT), telles qu'elles sont entrées en vigueur à compter du 1^{er} janvier 2003 (voir les documents PCT/AI/1 Rev.1 du 23 août 2001, PCT/AI/1 Rev.1 Add.1 du 26 octobre 2001, PCT/AI/1 Rev.1 Add.2 du 20 décembre 2001, PCT/AI/1 Rev.1 Add.3 du 2 septembre 2002, PCT/AI/1 Rev.1 Add.4 du 14 octobre 2002, PCT/AI/1 Rev.1 Add.5 du 25 novembre 2002 et PCT/AI/1 Rev.1 Add.6 du 10 décembre 2002 ; voir aussi d'autres modifications prenant effet au 19 juin 2003, figurant dans le document PCT/AI/1 Rev.1 Add.8 du 28 mai 2003, qui est publié sur le site Web de l'OMPI à l'adresse suivante : <http://www.wipo.int/pct/fr/texts/index.htm> ; des copies papier sont fournies par le Bureau international de l'OMPI sur demande). Les modifications contenues dans le présent document, qui sont promulguées après consultation des offices et des administrations intéressés conformément à la règle 89.2.b) du règlement d'exécution du PCT, concernent la modification et l'ajout d'un certain nombre de dispositions de la partie principale de l'annexe F des instructions administratives.
2. Le texte des présentes modifications sera publié dans le numéro 25/2003, du 19 juin 2003, de la *Gazette du PCT*.

MODIFICATIONS DES INSTRUCTIONS ADMINISTRATIVES

(texte en vigueur à compter du 19 juin 2003)

ANNEXE F

NORME CONCERNANT LE DÉPÔT ET LE TRAITEMENT ÉLECTRONIQUES
DES DEMANDES INTERNATIONALES

TABLE DES MATIÈRES

1. et 2. [Sans changement]
3. Structure et format de la demande internationale présentée sous forme électronique (demande E-PCT)
 - 3.1 Formats de document électronique acceptables
 - 3.1.1 Formats à codage de caractères
 - 3.1.1.1 XML
 - 3.1.1.1.1 Numérotage des paragraphes dans les documents en XML (description) [Nouvelle]
 - 3.1.1.2 et 3.1.1.3 [Sans changement]
 - 3.1.2 et 3.1.3 [Sans changement]
 - 3.2 Structure de la présentation et des documents constitutifs d'une demande internationale déposée sous forme électronique (demande E-PCT).
 - 3.3 et 3.4 [Sans changement]
4. Empaquetage des documents constitutifs de demandes internationales
 - 4.1 [Sans changement]
 - 4.2 Types de paquets basés ICP
 - 4.2.1 Paquet compacté et signé (WASP)
 - 4.2.2 [Sans changement]
 - 4.2.3 WASP combiné (C-WASP) [Nouvelle]
 - 4.3 Convention recommandée de nommage des dossiers [Nouvelle]
 - 4.3.1 Tableaux
 - 4.3.2 Identifiant du déposant
 - 4.3.3 Exemples
5. Transmission
 - 5.1 Protocole sur l'interopérabilité en matière de dépôt électronique
 - 5.1.1 Principes
 - 5.1.2 Protocole sur les couches du système applicatif pour la demande
 - 5.1.2.1 Utilisation du tunnel SSL pour la demande
 - 5.1.2.2 Actions prévues par le système applicatif pour la demande
 - 5.1.3 Protocole sur les couches du système applicatif en matière de notification [Nouvelle]
 - 5.1.3.1 Utilisation du tunnel SSL pour la notification
 - 5.1.3.2 Actions prévues par le système applicatif pour la notification
 - 5.1.4 Eléments de l'en-tête de gestion des échanges
 - 5.1.5 Eléments relatifs aux données de gestion des échanges
 - 5.1.6 Paramètres du serveur
 - 5.1.7 Paramètres du client
 - 5.1.8 Mécanisme de division
 - 5.1.9 Protocole sur les niveaux du processus
 - 5.1.9.1 Début de la transaction
 - 5.1.9.2 Envoyer l'en-tête du paquet

- 5.1.9.3 Envoyer le paquet de données
 - 5.1.9.4 Obtenir un accusé de réception
 - 5.1.9.5 Fin de la transaction
 - 5.1.9.6 Obtention de l'en-tête du paquet pour la notification
 - 5.1.9.7 Obtenir le paquet de données pour la notification
 - 5.1.9.8 Envoyer l'accusé de réception pour la notification
 - 5.1.9.9 Obtenir l'en-tête du paquet pour la liste de distribution
 - 5.1.9.10 Obtenir le paquet de données pour la liste de distribution
 - 5.1.9.11 Envoyer l'accusé de réception pour la liste de distribution
 - 5.1.9.12 Obtenir l'en-tête du paquet pour la liste de réception de la demande
 - 5.1.9.13 Obtenir le paquet de données pour la liste de réception de la demande
 - 5.1.9.14 Envoyer l'accusé de réception pour la liste de réception de la demande
- 5.2 Combinaisons paquet/transmission
- 5.2.1 Secteur de communication entre le déposant et l'office (phase internationale)
 - 5.2.2 Secteur de communication entre offices (d'office à office)
 - 5.2.3 Secteur de communication des offices désignés
6. à 9. [Sans changement]

1. et 2. [Sans changement]

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

[Sans changement au texte introductif]

3.1 *Formats de document électronique acceptables*

[Sans changement au texte introductif]

3.1.1 *Formats à codage de caractères*

3.1.1.1 *XML*

[Sans changement au texte introductif]

3.1.1.1.1 *Numérotage des paragraphes dans les documents en XML (description)* *[Nouveau]*

Si la partie de la demande internationale correspondant à la description codée est 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 et 3.1.1.3 [Sans changement]

3.1.2 et 3.1.3 [Sans changement]

3.2 *Structure de la présentation et des documents constitutifs d'une demande internationale déposée sous forme électronique (demande E-PCT).*

[Sans changement au texte introductif]

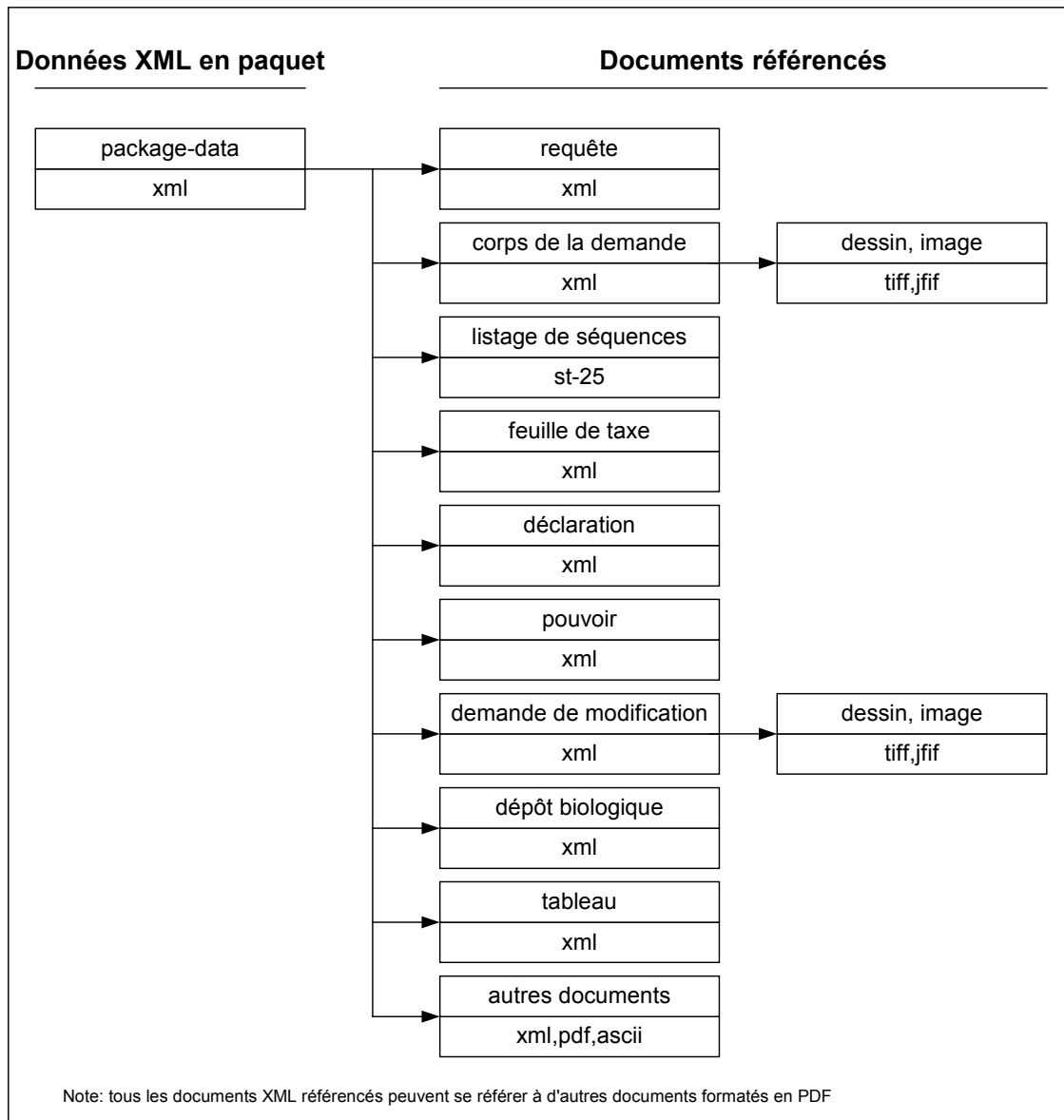


Figure 2 - Exemple de structure de document d'une demande internationale déposée sous forme électronique (demande E-PCT).

3.3 et 3.4 [Sans changement]

4. EMPAQUETAGE DES DOCUMENTS CONSTITUTIFS DE DEMANDES INTERNATIONALES

[Sans changement au texte introductif]

4.1 [Sans changement]

4.2 *Types de paquets basés ICP*

[Sans changement au texte introductif]

4.2.1 Paquet compacté et signé (WASP)

Lorsqu'une 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 paquet compacté et signé. 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, l'office prépare, signe et envoie le WASP qui contient ladite notification.

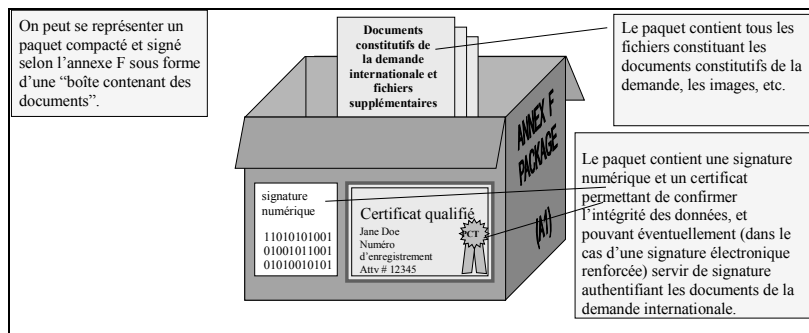


Figure 3 - Paquet compacté et signé (WASP)

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

4.2.2 [Sans changement]

4.2.3 WASP combiné (C-WASP) [Nouvelle]

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 recommandée de nommage des dossiers [Nouvelle]

Un dépôt électronique d'une demande de brevet comporte un certain nombre de dossiers associés. L'établissement de conventions de nommage des dossiers permet 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 meilleure compréhension par les utilisateurs du système. La série de tableaux qui suit constitue la convention recommandée de nommage des dossiers et les logiciels clients devraient produire de manière automatique les suffixes et les extensions des dossiers en conséquence. Chacun de ces tableaux représente un niveau de la convention, le dernier tableau présentant des exemples.

4.3.1 Tableaux

Tableau 1

<i>Codes à utiliser en fonction des descriptifs</i>	
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

<i>Codes à utiliser à chaque fois</i>		
A...	identifiant du déposant, ne peut pas dépasser 50 numéros	Recommandé
-	séparateur (tiret)	
A...	nature du document (<i>voir tableau 6</i>)	
.	séparateur (point)	
AAA	nature du dossier (<i>voir tableau 5</i>)	

Tableau 3

<i>Codes des dossiers externes référencés dans les documents</i>		
A...	identifiant du déposant, ne peut pas dépasser 50 caractères	Recommandé
-	séparateur (tiret)	
A...	nature du document (<i>voir tableau 6</i>)	
-	séparateur (tiret)	
A	nature de l'entité (<i>voir tableau 8</i>)	
NNNNNN	numéro de la séquence de l'entité, justifié à droite, avec des zéros à gauche pour remplir le vide	Optionnel
-	séparateur (tiret)	
NNNNNN	numéro de la séquence de la page, justifié à droite, avec des zéros à gauche pour remplir le vide	Recommandé
.	séparateur (point)	
AAA	nature du dossier (<i>voir tableau 5</i>)	

Tableau 4

<i>Dossiers non référencés dans les documents</i>		
A...	identifiant du déposant, ne peut pas dépasser 50 caractères	Recommandé
-	séparateur (tiret)	
A...	nom du document tel que fourni par le déposant, ne peut pas dépasser 50 caractères	
.	séparateur (point)	
AAA	nature du dossier (<i>voir tableau 5</i>)	

Tableau 5

<i>Extensions de noms de dossiers acceptées</i>	
txt	dossier contenant du texte, voir la section 3.1.1.3
xml	Voir la section 3.1.1.1
tif	format TIFF, voir la section 3.1.3.1
jpg	format JFIF, voir la section 3.1.3.2
zip	dossier contenant un ou plusieurs dossiers qui pourrait être compressés ou pas
app	ST.25, voir la section 3.1.1.2
pdf	Portable Document Format (Adobe), voir la section 3.1.2

Tableau 6

<i>Documents acceptés pour la phase initiale du dépôt électronique du PCT</i>	
<i>Documents</i>	<i>Code</i>
modifications apportées à la requête	amnd
corps de la demande	appb
dépôt biologique	biod
déclaration	decl
paquet de données	pkda
feuille de taxes	fees
pouvoir	poat
document de priorité	pdoc
requête	requ
informations contenues dans la requête après examen de l'office récepteur (ro-request-receiving-info)	rri
reçu xmit (xmit-receipt)	xmre
en-tête pkg (pkgheader)	pkgh
documents propres à l'office	[code-pays à 2 caractères]AA
ST.25 CRF	seql
tableau contenant plus de cinquante pages imprimées	mtbl

Tableau 7

<i>Sous-documents acceptés pour la phase initiale du dépôt électronique du PCT</i>	
<i>Sous-documents</i>	<i>Code</i>
description	desc
revendications	clam
abrégé	abst
dessins	draw

Tableau 8

<i>Formes des documents</i>	
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 dossiers 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 dossiers 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 dossiers relatifs à un dépôt, à une demande internationale ou à un déposant apparaissent ensemble dans le répertoire.

4.3.3 Exemples

<i>Dossier</i>	<i>Contenu</i>
dupont003340-appb.xml	Demande internationale
dupont003340-appb-C000001.CDX	Première structure chimique, format ChemDraw
dupont003340-appb-C000001.MOL	Première structure chimique, format MOL
dupont003340-appb-C000001.TIF	Première structure chimique, format TIFF
dupont003340-pkda.xml	Paquet de données
dupont003340-fees.xml	Feuille de taxes
dupont003340-poat.xml	Pouvoir
dupont003340-requ.xml	Requête
dupont003340-appb-T000001.TIF	Premier tableau, format TIFF
dupont003340-appb-T000002-000001.TIF	Deuxième tableau, première page, format TIFF
dupont003340-appb-T000002-000002.TIF	Deuxième tableau, deuxième page, format TIFF
dupont003355-appb.xml	Demande
dupont003355-appb-D000001.TIF	Première page de dessin, format TIFF
dupont003355-pkda.xml	Paquet de données
dupont003355-fees.xml	Feuille de taxes
dupont003355-appb-M000001.TIF	Première formule mathématique, format TIFF
dupont003355-appb-M000002.TIF	Deuxième formule mathématique, format TIFF
dupont003355-requ.xml	Requête
dupont003355-appb-T000001.TIF	Premier tableau, format TIFF

5. TRANSMISSION

[Sans changement au texte introductif]

5.1 *Protocole sur l'interopérabilité en matière de dépôt électronique*

[Sans changement au texte introductif]

5.1.1 *Principes*

[Sans changement au texte introductif]

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 de l'annexe F. La date de réception est déterminée conformément aux principes habituellement appliqués au dépôt des demandes sur papier, y compris le dépôt par des moyens électroniques (comme la télécopie), c'est-à-dire qu'elle est fondée sur la date en cours au siège de l'office au moment où la transmission complète de la demande est finalisée.

5.1.2.1 *Utilisation du tunnel SSL pour la demande*

Ces actions sont toutes mises en oeuvre à travers le tunnel SSL établi avant d'entamer l'action "Début de la transaction". Le tunnel SSL, 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 peut aussi être laissé ouvert et n'être fermé qu'à la fin des échanges. Le tunnel SSL utilise la version 3 de la norme standard.

5.1.2.2 *Actions prévues par le système applicatif pour la demande*

Commencer la session SSL (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

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

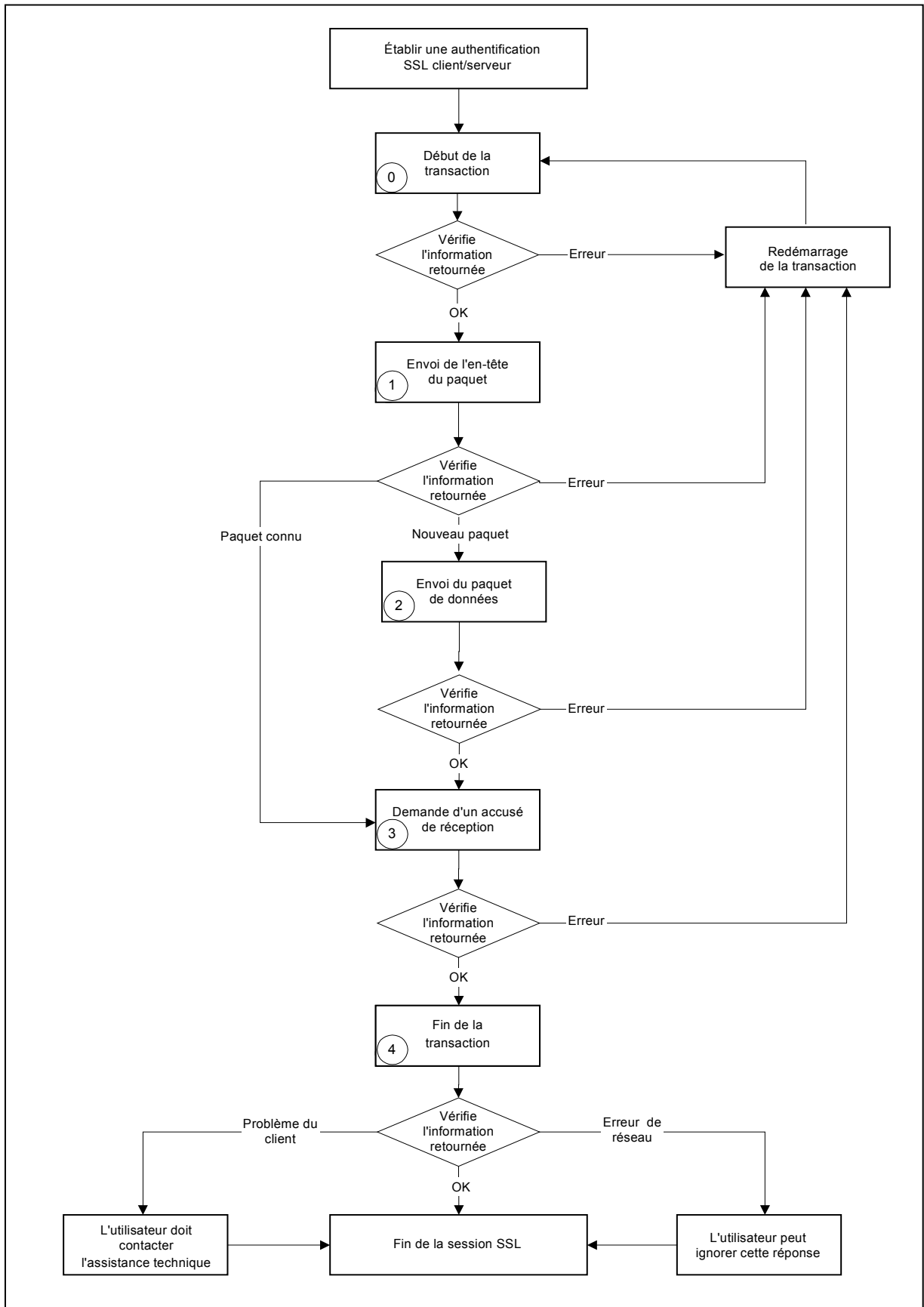


Figure 5 – Conduite à suivre selon le protocole sur le système applicatif en ce qui concerne la demande

5.1.3 *Protocole sur les couches du système applicatif en matière de notification* [Nouveau]

Au plus haut niveau du système applicatif en matière de notification, le protocole prévoit que le logiciel client et le serveur suivent les cinq actions¹⁰ suivantes:¹¹

- 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)¹²
- 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 pour la notification*

Cf. section 5.1.2.1, "Utilisation du tunnel SSL pour la demande".

¹⁰ 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 courrier électronique.

¹¹ 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.

¹² Le serveur utilise la valeur de l'attribut "transaction-type" (voir la section 5.1.4) afin d'identifier le type de document demandé, par 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 (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 (??)

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)¹³
- 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)
- 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

¹³ Si le C-WASP contient plusieurs WASPs, cette information figure dans l'en-tête du paquet contenant la notification.

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

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

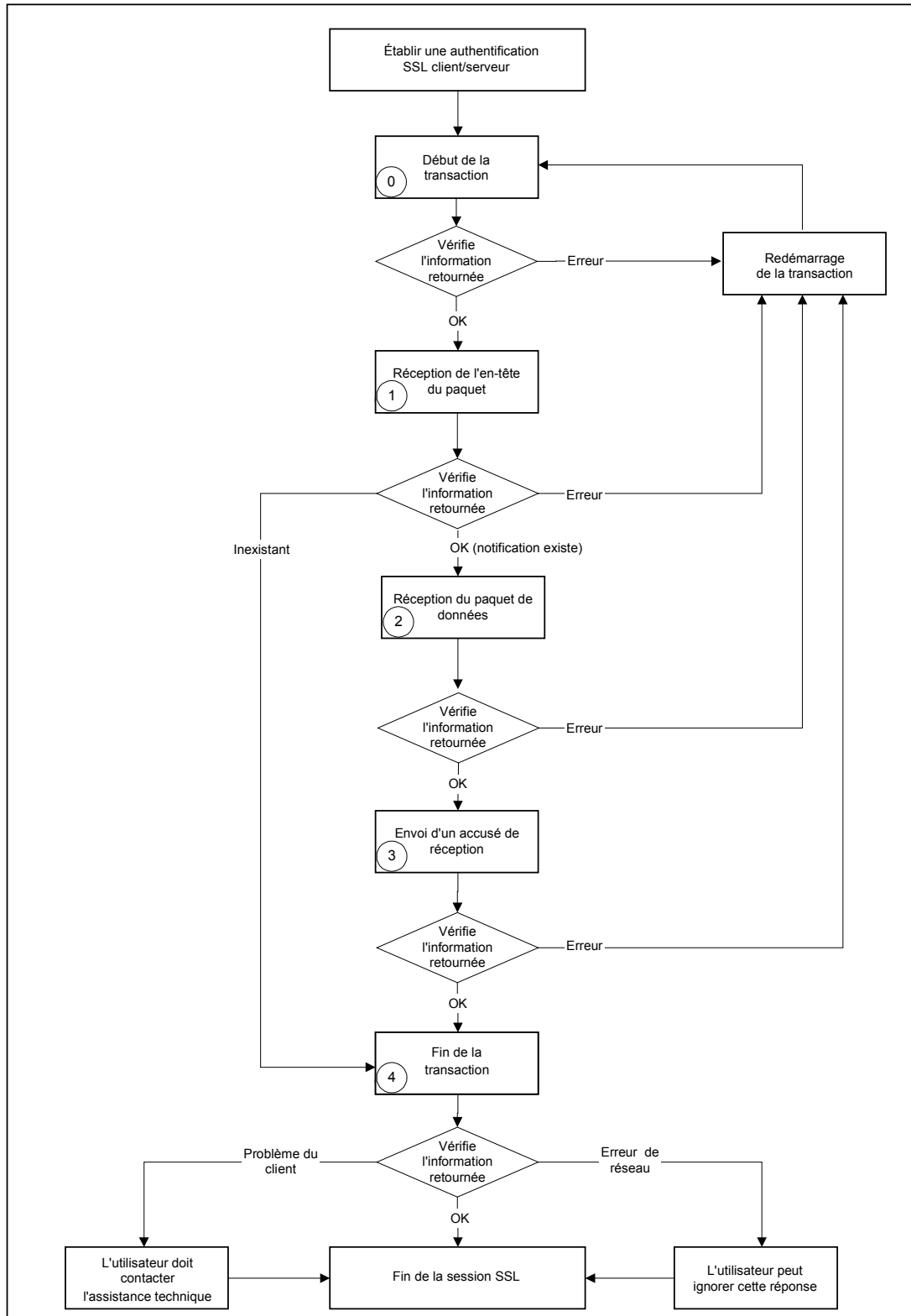


Figure 6 – Conduite à suivre selon le protocole de niveau applicatif pour la notification

5.1.4 *Eléments 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').

Elément	Division_hash
Valeurs d'ARC	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.

Elément	protocol_version
Valeurs d'ARC	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 (par 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.

Elément	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
	ern, prn	Send receipt check notice for notification
	ephd, pphd	Get package header for dispatch list
	epdd, ppdd	Get package data for dispatch list
	ered, pred	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	Elément 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.

Elément	transaction_id
Valeurs d'ARC	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').

Elément	reserved_use
Valeurs d'ARC	Reservée à l'usage national (par 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. (par ex. pour informer un client de l'horaire du serveur de l'office récepteur).

Elément	total_bytes
Valeurs d'ARC	ASCII numérique avec remplissage de zéros sur la gauche (par 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).

Elément	division_size
Valeurs d'ARC	ASCII numérique avec remplissage de zéros sur la gauche (par 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

Elément	division_offset
Valeurs d'ARC	ASCII numérique avec remplissage de zéros sur la gauche (par 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

Elément	division response code		
Valeurs d'ARC		<i>Division RCs</i>	<i>Signification</i>
		0000	OK
		FFFF	Erreur générale
		FFFE	Renvoyer
		FFFD	Attendre
		FFFC	Erreur de séquence du protocole
	4 octets (caractères ASCII 4 x 8bit)		
Taille du corps d'entité	4 octets		
Description	Le code de retour du serveur ou du client est utilisé pour gérer le mécanisme de division		

Elément	application response code		
Valeurs d'ARC		<i>Application RCs</i>	<i>Signification</i>
		0000	OK
		FFFF	Erreur générale
		0001	OK, paquet connu
		0002	OK, nouveau paquet
		0003	OK, Inexistant
		1000	En attente
		FFFB	Problème du client
		FFFA	Erreur de réseau
		FFF9	Erreur de version du protocole
		FFF8	La valeur de hachage de la division dans la transaction de gestion de l'en-tête est une erreur.
		FFF7	Les valeurs de hachage dans le paquet de l'en-tête et le WAD du paquet de données ne correspondent pas..
		FFF6	La signature n'est pas valable (par exemple, en raison d'une erreur de vérification de la signature ou une validation de données expirées). ¹⁴
	4 octets (caractères ASCII 4 x 8bit)		
Taille du corps d'entité	4 octets		
Description	Code de retour du serveur ou du client utilisé pour gérer les étapes d'envoi de la demande		

¹⁴ Ce code s'applique lorsque le serveur ne peut pas établir l'authentification prévue dans la fonction Obtenir l'en-tête du paquet.

Elément	Encoding_method		
Valeurs d'ARC		<i>Demande RCs</i>	<i>Signification</i>
		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.		

Elément	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 expliquent 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.

5.1.5 Eléments relatifs aux données de gestion des échanges

Elément	max_division_size
Valeurs d'ARC	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	00000000000008192 (8 kilo-octets)

5.1.6 Paramètres du serveur

Elément	server_timeout
Valeurs d'ARC	ASCII numérique avec remplissage de zéros sur la gauche (par 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 a 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 d'ARC	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 d'ARC	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	000000000000005 (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 d'ARC	ASCII numérique avec remplissage de zéros sur la gauche (par 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	000000000000005 (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 oeuvre 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.

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 de 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 de 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 de 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)

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 de 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 de 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

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 de 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 de 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

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 de 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 de 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

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 de 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 de 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

5.1.9.6 *Obtention de 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 de 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 de 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

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 de 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 de 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

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 de 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 de 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

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 de 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 de 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

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 de 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 de 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

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 de 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	pred	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 de 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	pred	tranid	???	0	0	0	a	b	???	espace	aucune

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 de 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 de 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

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 de 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 de 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

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 de 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	prea	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 de 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	prea	tranid	???	0	0	0	a	b	???	espace	aucune

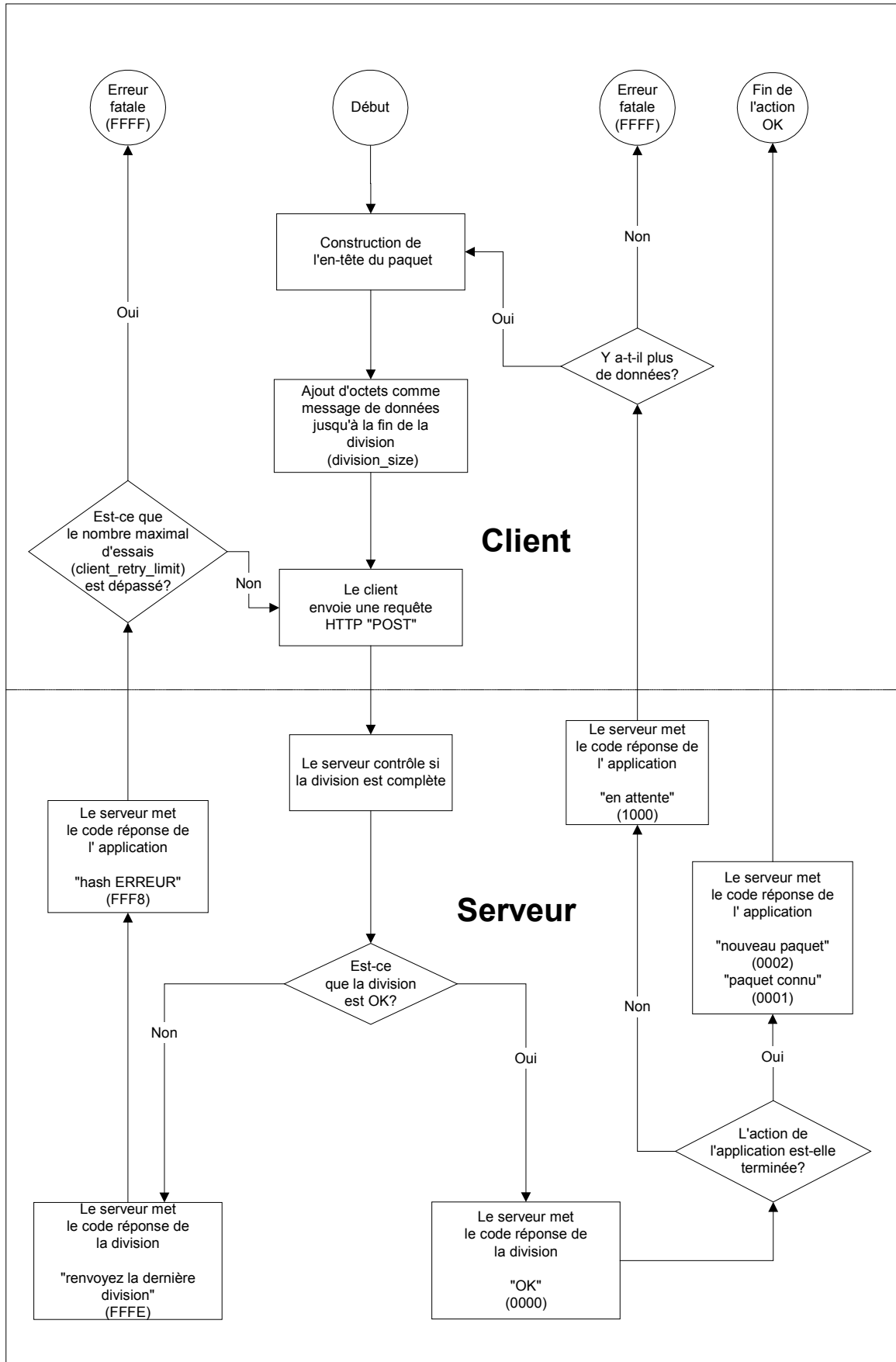


Figure 7 - Conduite à suivre pour l'envoi de l'en-tête du paquet

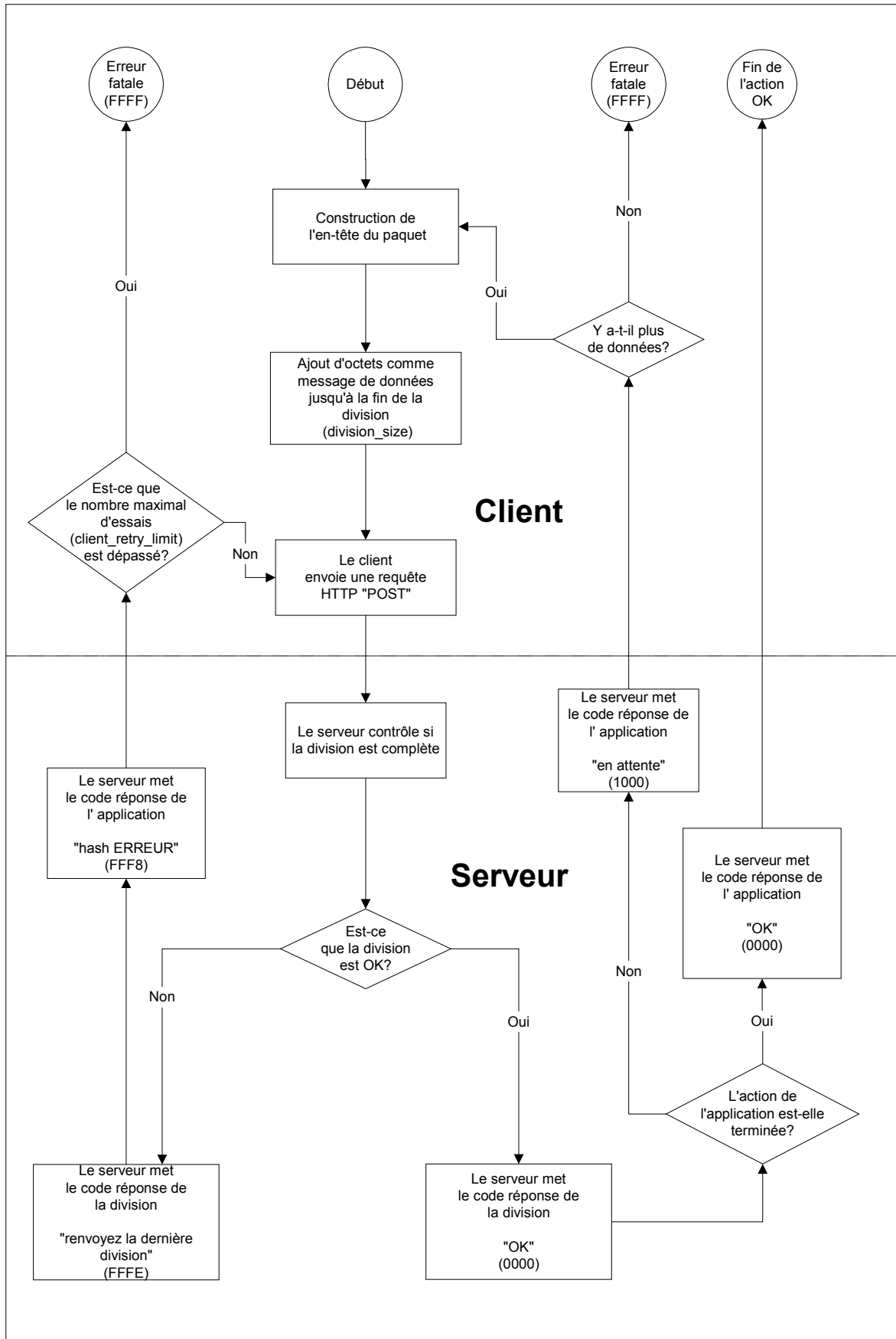


Figure 8 - Conduite à suivre pour l'envoi du paquet de données

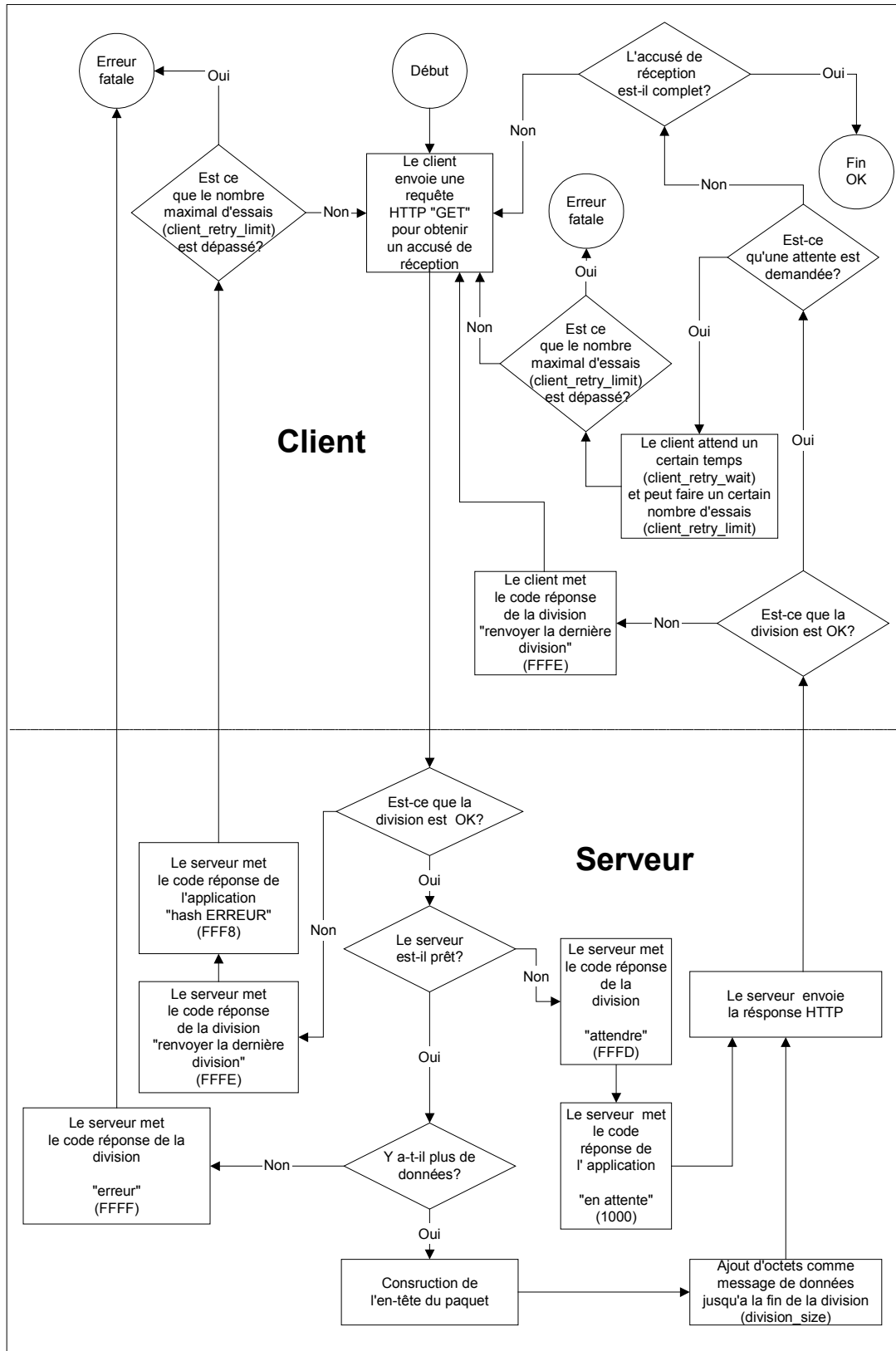


Figure 9 - Conduite à suivre pour l'obtention de l'accusé de réception

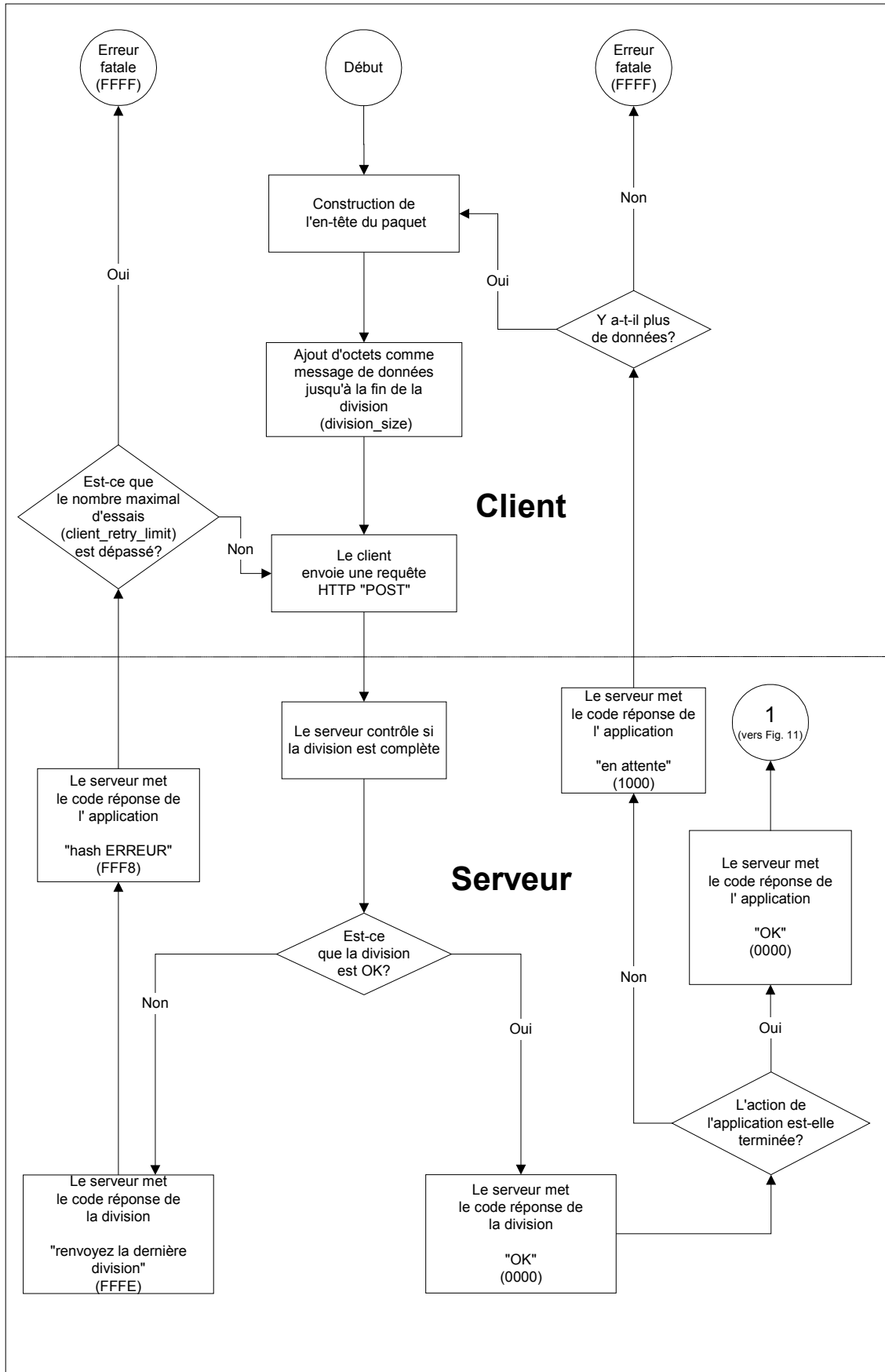


Figure 10 – Conduite à suivre pour l'obtention de l'en-tête du paquet (du déposant à l'office)

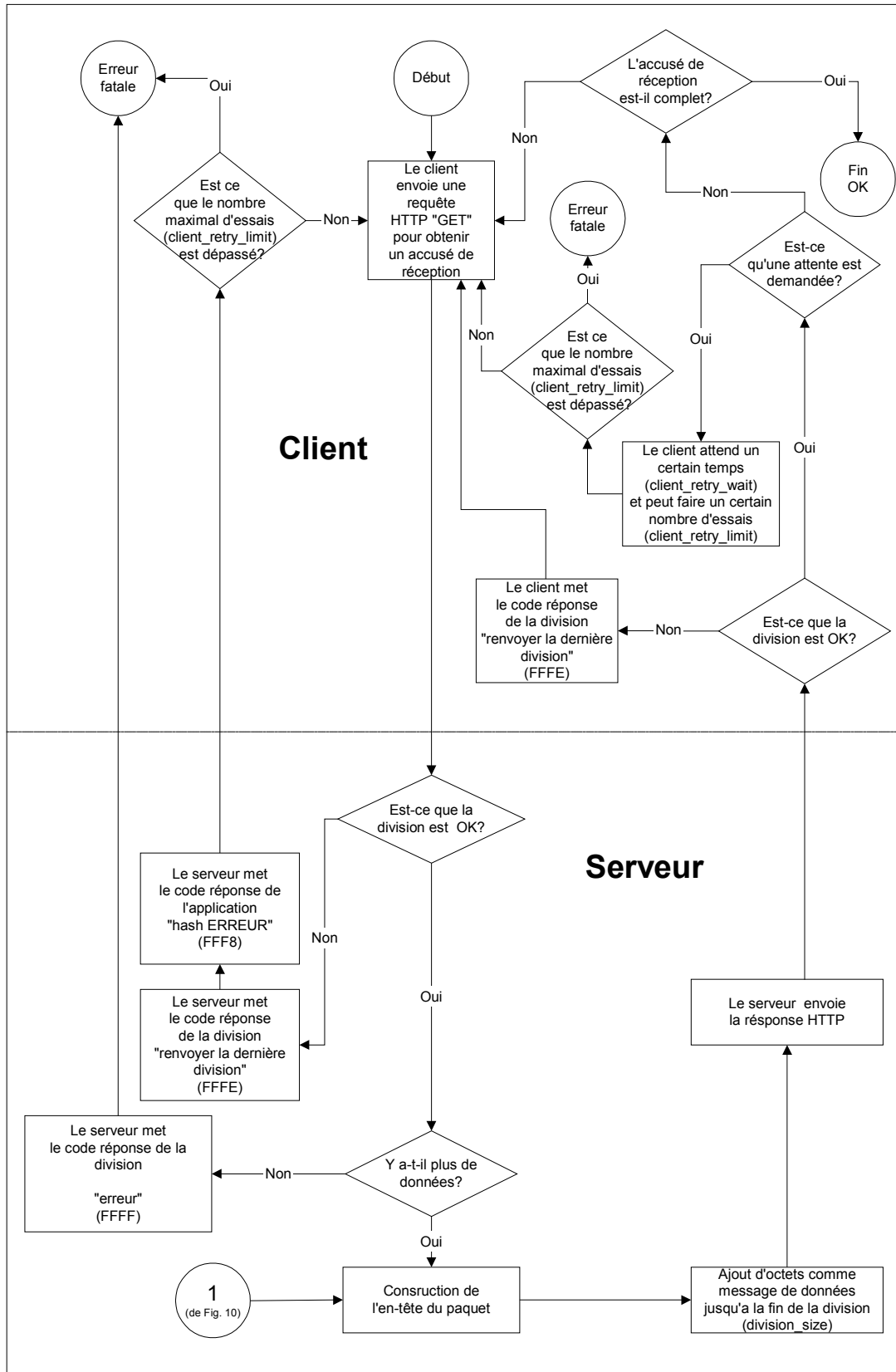


Figure 11 – Conduite à suivre pour l'obtention de l'en-tête du paquet (de l'office au déposant) [Nouvelle]

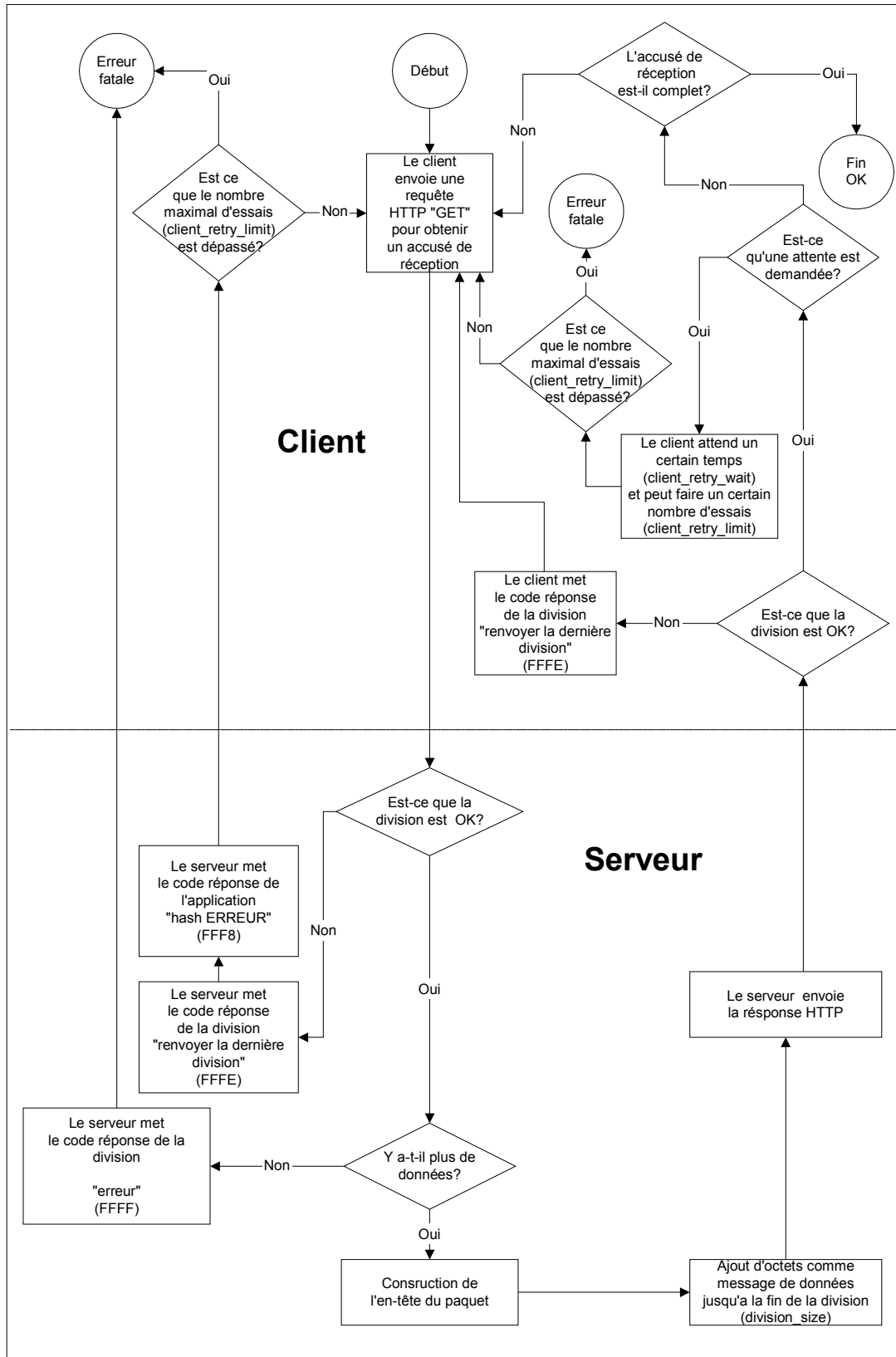


Figure 12 – Conduite à suivre pour l'obtention des données du paquet [Nouvelle]

5.2 Combinaisons paquet/transmission

[Sans changement au texte introductif]

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

Les documents constitutifs de la demande internationale peuvent être déposés en ligne (dans un environnement ICP) par l'intermédiaire de l'Internet ou d'un réseau privé, 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 basée ICP n'est pas autorisé à l'heure actuelle, sauf dans le cadre des réserves provisoires permises en vertu de l'instruction administrative 703.f) (voir la section 7.1.1 quant aux conséquences d'un dépôt non fondé sur une technologie ICP effectué en vertu d'une réserve provisoire de ce type).

La figure 13 présente une grille des différentes combinaisons mécanismes de transmission/paquet autorisées dans le secteur de communication entre le déposant et l'office (phase internationale) en vertu de la présente norme. En résumé, pour chaque mécanisme transmission :

- En ligne/Internet : il faut utiliser le paquet signé et chiffré (SEP), ainsi qu'un TCP/IP pour l'échange de données, en temps réel, à travers l'Internet.
- En ligne/environnement sécurisé: il convient d'utiliser un SEP, un WASP ou un C-WASP. Ceci est défini comme une connection de télécommunication établie pour échanger des données, à travers un réseau qui est a pour caractéristiques : 1) d'être un réseau privé, 2), d'utiliser l'Internet avec un niveau élevé de chiffrement (par ex. SSL), 3) d'avoir une connection Internet sur un réseau privé virtuel (VPN).
- Hors ligne/supports matériels: les types de paquets suivants doivent être employés: SEP, WASP, C-WASP ou WAD. Le support matériel (par ex. disquette, CD-ROM, DVD, etc.) est employé pour conserver les données des demandes internationales sans échange de données en temps réel.

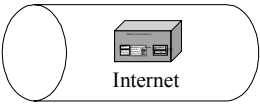





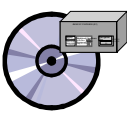


	Paquet signé et chiffré	Paquet compacté et signé WASP combiné	Documents constitutifs de la demande, compactés
En ligne / Internet	 Internet	 Non autorisé	 Non autorisé
En ligne environnement sécurisé	 Environnement sécurisé	 Environnement sécurisé	 Non autorisé
Hors ligne Supports matériels			

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)*

Tous les échanges de données dans le secteur office à office doivent s'inscrire dans un environnement ICP. Les documents constitutifs des demandes internationales peuvent être échangés en ligne sur l'Internet ou un réseau privé (tels que Tri-Net ou le WIPONET), ou envoyés sur support matériel.

La figure 14 présente une grille des différentes combinaisons transmission/paquet autorisées en vertu de la présente norme. En résumé, pour chaque mécanisme d'échange de données :

- a) En ligne/Internet : il convient d'utiliser le paquet signé et chiffré, ainsi qu'un TCP/IP pour l'échange de données, en temps réel, à travers l'Internet.
- b) En ligne/réseau sécurisé : il convient d'utiliser un SEP ou un WASP. Ceci est défini comme une connection de télécommunication établie pour échanger des données, à travers un réseau qui est a pour caractéristiques : 1) d'être un réseau privé (par ex. WIPONET, Tri-Net), 2) d'utiliser l'Internet avec un niveau élevé de chiffrement (par ex. SSL), 3) d'avoir une connection Internet sur un réseau privé virtuel (VPN).
- c) Hors ligne/support matériel : un SEP ou un WASP doit être utilisé. Le support matériel (par ex. disquette, CD-ROM, DVD etc.) est employé pour conserver les données des demandes internationales sans échange de données en temps réel.

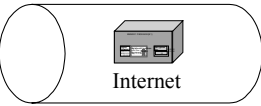








	Paquet signé et chiffré	Paquet compacté et signé	Documents constitutifs de la demande, compactés
En ligne / Internet	 Internet	 Non autorisé	 Non autorisé
En ligne environnement sécurisé	 Environnement sécurisé	 Environnement sécurisé	 Non autorisé
Hors ligne Supports matériels	 Supports matériels	 Supports matériels	 Non autorisé

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

5.2.3 Secteur de communication des offices désignés

Un SEP, WASP ou WAD peut être utilisé dans l'échange de documents dans le secteur de communication des offices désignés. La figure 15 présente une grille des différentes combinaisons mécanismes de transmission/paquet autorisées. En résumé, pour chaque mécanisme d'échange de données :

- a) En ligne/Internet : il faut utiliser un SEP, ainsi qu'un TCP/IP pour l'échange de données, en temps réel, à travers l'Internet.
- b) En ligne/réseau sécurisé : il convient d'utiliser un SEP, un WASP ou un WAD. Ceci est défini comme une connection de télécommunication établie pour échanger des données, à travers un réseau qui est a pour caractéristiques : 1) d'être un réseau privé (par ex. Tri-Net, WIPONET), 2) d'utiliser l'Internet avec un niveau élevé de chiffrement (par ex. SSL), 3) d'avoir une connection Internet sur un réseau privé virtuel (VPN).
- c) Hors ligne/support matériel : un SEP, un WASP ou un WAD. Le support matériel (par ex. disquette, CD-ROM, DVD etc.) est employé pour conserver les données des demandes internationales sans échange de données en temps réel.

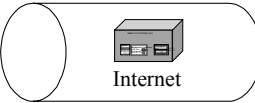








	Paquet signé et chiffré	Paquet compacté et signé	Documents constitutifs de la demande, compactés
En ligne / Internet	 Internet	 Non autorisé	 Non autorisé
En ligne environnement sécurisé	 Environnement sécurisé	 Environnement sécurisé	 Environnement sécurisé
Hors ligne Supports matériels			

Figure 15 - Combinaisons paquet/transmission autorisées dans le secteur de communication des offices désignés

6. à 9. [Sans changement]

[Fin du document]