F

OMPI

PCT/AI/1 Add.4 Prov.
ORIGINAL : anglais
DATE : 9 juin 2000

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

PROPOSITIONS DE MODIFICATION RELATIVES AU DÉPÔT, AU TRAITEMENT ET À L'ARCHIVAGE ÉLECTRONIQUES DES DEMANDES INTERNATIONALES ET À LA GESTION DES DOSSIERS ÉLECTRONIQUES RELATIFS À CES DEMANDES

(ANNEXE F, APPENDICE I : PROJET DE NORME TECHNIQUE POUR L'ÉCHANGE EN LIGNE DE DOCUMENTS DE PROPRIÉTÉ INDUSTRIELLE DANS UN ENVIRONNEMENT ICP)

établies par le Bureau international pour examen lors d'une réunion consultative informelle du PCT relative au dépôt électronique, Genève, 11 - 14 juillet 2000

INTRODUCTION

1. Lors de sa vingt-huitième session (16ème session extraordinaire), qui s'est tenue à Genève en mars 2000, l'Assemblée de l'Union du PCT a étudié la mise en œuvre du dépôt et du traitement électroniques des demandes internationales. Les délibérations de l'Assemblée ont eu lieu sur la base du document PCT/A/28/3, qui comportait des propositions de modification des instructions administratives du PCT[1] ainsi que les commentaires formulés sur ce document par des délégations et des représentants des utilisateurs et figurant dans les documents PCT/A/28/3 Add.2 à Add.5. Les délibérations ont aussi porté sur les documents reproduits dans le document PCT/A/28/3 Add.1 relatif à l'élaboration de la norme technique nécessaire pour permettre la mise en œuvre du dépôt et du traitement électroniques des demandes internationales. L'Assemblée a convenu que la proposition de nouvelle septième partie des instructions administratives du PCT (instructions relatives au dépôt, au traitement et au stockage électroniques des demandes internationales et à la gestion des dossiers électroniques relatifs à ces demandes) et le projet d'annexe F desdites instructions (Norme concernant le dépôt, le traitement et le stockage électroniques des demandes internationales et la gestion des dossiers électroniques relatifs à ces demandes) devaient être considérablement révisés, et que des consultations supplémentaires devaient être menées sur les versions révisées (voir le rapport de l'Assemblée, document PCT/A/28/5, paragraphe 24)[2].

2. En vue de la poursuite des consultations prévues à la règle 89.2.b), qui ont commencé lors de la vingt-huitième session de l'Assemblée, le présent document et les documents connexes[3] contiennent une version révisée des dispositions d'application des instructions administratives qu'il convenait de modifier. Ces documents sont les suivants :

PCT/AI/1 Add.2 Prov., qui contient un projet révisé de septième partie;

PCT/AI/1 Add.3 Prov., qui contient un projet révisé d'introduction de l'annexe F;

PCT/AI/1 Add.4 Prov, qui contient un projet révisé d'appendice I de l'annexe F (Norme technique pour l'échange en ligne de documents de propriété intellectuelle dans un environnement ICP);

---

[1] Dans le présent document, les termes "articles", "règles" ou "instructions" désignent, respectivement, les articles du Traité de coopération en matière de brevets (PCT), les règles du règlement d'exécution du PCT (le "règlement d'exécution") et les instructions administratives du PCT (les "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/fre/pct/texts/index.htm Les termes "législation nationale", "demandes nationales", "offices nationaux" etc. doivent être interprétés comme englobant la législation régionale, les demandes régionales, les offices régionaux, etc.

[2] Le rapport et les autres documents présentés lors de la session de l'Assemblée sont disponibles sur le site Internet de l'OMPI à l'adresse suivante: http://www.wipo.int/fre/document/govbody/wo_pct/index_28.htm

[3] Le présent document et tout autre document destiné à être soumis pour examen à la réunion consultative informelle du PCT relative au dépôt électronique sont disponibles sur le site Internet de l'OMPI à l'adresse suivante: http://www.wipo.int/fre/meetings/2000/pct_ef/index.htm

PCT/AI/1 Add.5 Prov., qui contient un projet révisé d’appendice II de l’annexe F (DTD selon le XML pour l’échange de documents de propriété intellectuelle);

PCT/AI/1 Add.6 Prov., qui contient un projet révisé d’appendice III de l’annexe F (Dépôt électronique sur support matériel).

[L’appendice I de l’annexe F suit]

PROPOSITIONS DE MODIFICATION
DES INSTRUCTIONS ADMINISTRATIVES DU PCT

ANNEXE F
NORME CONCERNANT LE DÉPÔT, LE TRAITEMENT
ET LE STOCKAGE ÉLECTRONIQUES
DES DEMANDES INTERNATIONALES ET LA GESTION
DES DOSSIERS ÉLECTRONIQUES RELATIFS À CES DEMANDES

Appendice I
Projet de norme technique pour l'échange en ligne de documents de propriété industrielle dans un environnement ICP

1 Généralités

Ce document expose les exigences techniques de l'échange en ligne de documents de propriété industrielle dans un environnement d'infrastructures à clé publique (environnement ICP), y compris le dépôt en ligne.

La présente norme énonce des exigences obligatoires pour tous les déposants et offices prenant part à de tels échanges, ainsi que des exigences facultatives. Tous les éléments facultatifs sont indiqués en *italique*.

2 Portée

La présente norme technique couvre les exigences dans les domaines suivants :

a) sécurité et ICP
b) signatures électroniques
c) prescriptions relatives au format des documents
d) envoi

3 Sécurité et ICP

3.1 Infrastructure à clé publique

Dans la version actuelle de la norme, l'assemblage et la transmission sont exécutés en utilisant la technique ICP. Les mises à jour de la norme pourront inclure d'autres techniques de sécurité dès qu'elles seront disponibles et réalisables. La spécification technique de la présente norme exige donc aujourd'hui l'utilisation d'une ICP.

La mise en œuvre des ICP s'effectuera conformément aux recommandations établies par le groupe de travail sur l'inter opérabilité des infrastructures à clé publique (PKIX) de l'*Internet Engineering Task Force* (IETF), exposées dans l'appel à commentaires RFC 2459 de l'IETF.

Dans la pratique, on utilisera des paires de clés et des certificats numériques distincts aux fins d'authentification et de confidentialité. *Facultatif : un office de propriété industrielle ou une autorité de certification reconnue peut décider d'offrir un service de récupération de clés pour la paire de clés garantissant la confidentialité, lorsque la législation nationale le permet (ou l'exige).*

3.2 Certificats

La norme prévoit deux catégories de certificats numériques :

Certificat reconnu : le déposant est déjà en possession d'un certificat numérique émis par un tiers de confiance qui établit son identité. Ce certificat est ensuite utilisé à la fois pour la création des paquets et la transmission des données.

Certificat ad-hoc : le déposant n'est pas en possession d'un certificat reconnu, auquel cas la transmission technique des données est exécutée en utilisant un certificat numérique *"ad-hoc"* 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 non reconnue). Le déposant doit fournir son nom et son adresse de courrier électronique pour obtenir ce certificat.

Dans les deux cas, le certificat numérique doit suivre la recommandation X.509 de l'Union internationale des télécommunications (UIT), version 3, en ce qui concerne le format des certificats.

Facultatif : les certificats peuvent être stockés sur une carte à microprocesseur, une disquette ou un disque dur.

3.3 Autorités de certification

Chaque office récepteur doit préciser quelles sont les autorités de certification qu'il accepte. Le Bureau international publiera cette liste d'autorités de certification "reconnues" avec un lien vers l'énoncé de politique ICP publié par ces autorités de certification.

Dans le même temps, les États membres œuvreront avec le Bureau international à la définition d'un ensemble coordonné de principes directeurs permettant d'évaluer ces énoncés de politiques ICP. À plus long terme, ces principes directeurs devraient permettre d'établir une liste des autorités de certification acceptables pour tous les offices récepteurs. Le Bureau international publiera alors cette liste.

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 doit stocker 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 comprendront, pour la publication et l'extraction de certificats numériques d'utilisateurs, une interface externe conforme au protocole simplifié d'accès à l'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 doit publier une liste d'annulation (CRL) établie selon la version 2 de la recommandation X.509.

Chaque office de propriété industrielle s'abonnera aux listes d'annulation (CRL) correspondant à toutes les autorités de certification qu'il accepte. Chaque fois qu'un certificat sera utilisé aux fins d'identification, l'office de propriété industrielle consultera ces listes d'annulation (CRL) pour s'assurer que le certificat n'a pas été annulé.

3.4 Signatures numériques

Les signatures numériques utilisées pour signer des documents électroniques aux fins de l'échange de documents de propriété industrielle devront respecter le format et la pratique spécifiés dans la norme PKCS#7 de *RSA Laboratories* relative à la syntaxe du message cryptographique, intitulée *Cryptographic Message Syntax Standard*, version 1.5, en ce qui concerne la définition du contenu du type *Signed-data* (données signées).

La construction de ces signatures nécessite un certificat répondant aux exigences énoncées à la section 3.2 ci-dessus.
Toutes les signatures numériques doivent être codées selon les règles DER.

3.5 Algorithmes de chiffrement

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 pourra pas être utilisé pour l'échange de documents de propriété industrielle 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.

Facultatif : il est recommandé d'utiliser rsaEncryption comme algorithme de chiffrement asymétrique et dES-EDE3-CBC comme algorithme de chiffrement symétrique. Le même algorithme de chiffrement asymétrique devrait être utilisé pour les certificats, signatures et enveloppes numériques.

3.6 Chiffrement 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 propriété industrielle devront 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.

3.7 Algorithmes de compression

À la chaîne de caractères du message est appliqué l'algorithme de hachage à sens unique SHA-1, algorithme de compression à haut niveau de sécurité qui crée une empreinte du message.

4 Mécanismes de signature

Un certain nombre de types de signature ont été reconnus possibles aux fins de l'échange de documents de propriété industrielle. Chaque office récepteur et chaque office désigné peut choisir dans la liste suivant les types de signature qu'il accepte :

a) signatures électroniques simples
   i) image en fac-similé de la signature de l'utilisateur
   ii) chaîne de caractères
   iii) signature enveloppée électroniquement selon la méthode dite du "click-wrap"
b) signature électronique sécurisée
   i) signature PKCS#7

La signature électronique simple est encodée dans la structure “correspondant” du document XML comme indiqué ci-après :

```
…
<!ELEMENT electronic-signature
              (date-signed,
              place-signed,
              signature-type,
              (signature-file, signature-mark)) >
…
```

Une signature électronique simple dans un document XML peut être complétée par l’adjonction d’une signature numérique aux documents enveloppés.

4.1 Signature en fac-similé

Pour créer ce type de signature, le déposant doit insérer l’élément signature-type=“facsimile” et un renvoi à une entité externe (par exemple signature-file=“signature.tif”) dans le document XML désignant le fichier contenant la représentation en mode point (bitmap) de la signature. Le fichier de la représentation en mode point doit être une image monobande de 300dpi, à codage Intel et au format TIFF Groupe 4.

4.2 Signature composée d’une chaîne de caractères

Pour créer ce type de signature, le déposant doit insérer l’élément signature-type=“mark” et une chaîne de caractères dans un document XML, sous le format suivant :

signature-mark=“/text-string/”

où la chaîne de caractères est une chaîne de caractères codés UTF-8, ne comprenant pas le caractère “/”, choisie par le déposant comme signature électronique. Voici quelques exemples valables :

signature-mark=“/Jean Dupont/”
signature-mark=“/etreounepasetre/”
signature-mark=“/1345728625235/”
signature-mark=“/Günter François/”

4.3 Signature enveloppée électroniquement selon la méthode dite du “click-wrap”

Pour créer ce type de signature, le déposant doit cliquer sur un bouton dans l’interface utilisateur indiquant “I accept”. Ceci est codé dans le document XML sous la forme signature-type=“click-wrap”, signature-mark= “click-wrap-signature-accepted”.

4.4 Signature PKCS#7

Il s’agit d’un type “données signées” PKCS#7, produit à partir du message électronique par l’action du signataire qui utilise sa clé d’authentification privée pour chiffrer l’empreinte du

message (signature numérique). Le type “données signées” PKCS#7 comporte une copie du certificat numérique délivré au signataire par une autorité de certification reconnue.

L’utilisation d’une signature PKCS#7 doit être indiquée dans le fichier XML par l’utilisation des éléments signature-type=“PKCS#7” et signature-mark=“use-digital-signature”.

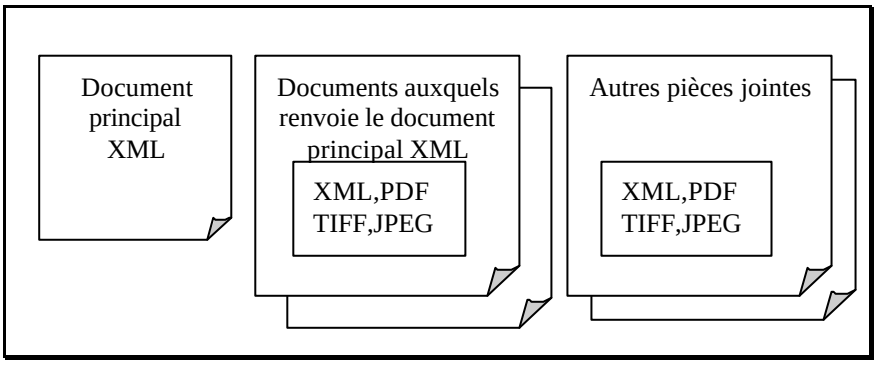
5 Prescriptions relatives au format des données

On utilise le mécanisme d’assemblage de documents pour combiner en un seul et même objet binaire à la fois les renseignements sur ce qui est transmis et le contenu de la transmission; on applique ensuite les signatures numériques et le chiffrement appropriés.

5.1 Préparation des documents

Dans chaque échange de documents de propriété industrielle, il y a un document principal XML, qui peut renvoyer expressément à d’autres documents, le cas échéant par des liens hyper-texte. Ces documents forment un tout logique avec le document principal auquel ils sont incorporés par renvoi (nouvelle demande de brevet par exemple). En outre, un échange de documents peut inclure d’autres pièces jointes (désignation de l’inventeur, paiement de taxes, etc.).

Le document principal XML doit se conformer à l’une des DTD spécifiées dans l’appendice II. Les documents auxquels ils renvoient (entités externes) sont généralement des images incrustées, des tableaux, des dessins ou d’autres documents composés; ils peuvent être codés en XML, PDF, TIFF ou JFIF(JPEG). Les pièces jointes sont des documents distincts, mais en rapport, qui peuvent être codés en XML, PDF ou format image.



Les offices de la coopération trilatérale et l’OMPI sont attachés au principe de la mise en place d’un environnement fondé sur des standards ouverts pour l’échange électronique de documents de propriété intellectuelle. Ceci a une conséquence notable: la norme applicable à l’envoi de documents électroniques recommandera de préférence des standards ouverts et ne préconisera pas l’utilisation de formats exclusifs de fournisseurs pour l’échange de documents électroniques. Il s’agit notamment, en adoptant cette ligne de conduite, d’éviter aux offices d’avoir à conserver les exemplaires authentiques de dépôts électroniques dans des versions particulières de formats exclusifs sur lesquels ils n’ont aucun contrôle.

Les systèmes exclusifs de traitement de texte communément employés présentent l’avantage d’assembler les documents en un fichier unique tel que .doc ou .wps. Les formats de

traitement de texte exclusifs .doc, .wps, etc. combinent texte, instructions de traitement, informations de mise en page, infographie par quadrillage, dessin en mode vectoriel, tableaux et autres types de données en un fichier unique de traitement de texte.

Les offices de la coopération trilatérale ont opté pour des systèmes ouverts de préférence aux fichiers de traitement de texte: on y utilisera pour les documents électroniques le langage XML (eXtensible Markup Language) en cours de développement pour permettre la communication de données structurées sur le Web. Un document XML, comme une page Web HTML, comprend un fichier texte codé caractère par caractère et, le cas échéant, un ou plusieurs fichiers supplémentaires pouvant contenir soit encore du texte, soit des données binaires telles qu'images et dessins. En XML, un document électronique de demande de brevet consistera normalement en une collection de fichiers. Il pourra, par exemple, comprendre un fichier textuel pour chaque pièce de procédure envoyée au titre de la demande, plus un fichier textuel pour le mémoire descriptif de l'invention, accompagné de multiples fichiers graphiques (un pour chaque dessin figurant dans le mémoire descriptif). L'approche XML libère les offices de l'obligation d'investir dans des formats de traitement de texte exclusifs, mais la simplicité du fichier unique qu'offrait le traitement de texte est perdue.

5.1.1 Images

Les images en fac-similé à utiliser dans l'échange de documents de propriété industrielle doivent répondre aux prescriptions suivantes :

a) format
   i) TIFF V6.0 avec compression de groupe 4, monobande, codage Intel ou
   ii) JFIF(JPEG)
b) 200, 300 ou 400 dpi
c) taille maximum : A4 ou format commercial

5.1.2 PDF

Les documents PDF à utiliser dans l'échange de documents de propriété industrielle doivent répondre aux prescriptions suivantes :

a) compatibilité Acrobat V3
b) texte non comprimé pour faciliter la recherche
c) texte non crypté
d) pas de signatures numériques
e) pas d'objets incorporés en OLE
f) toutes polices de caractères incorporées, standard PS17 ou construites à partir des polices Adobe MM.

5.1.3 XML

Tous les documents XML doivent se conformer à l'une des DTD spécifiées dans l'appendice II.

Le jeu de caractères utilisé pour tous les documents XML doit être soit Unicode UCS-2 (ISO/IEC 10646 : 193) codé UTF-8, soit JIS-X0208 codé ISO-2022-JP. (Pour les demandes PCT, sont aussi acceptables les caractères chinois GB2312 et les caractères coréens KSC 5601).

Outre ce qui précède, chaque office récepteur doit indiquer un schéma de codage de caractères tel que décrit dans les appels à commentaires [RFC 2277 de l'IETF] et [RFC 2130 de l'IETF] et informer le Bureau international de la spécification. Dans ce cas, il convient de définir ce qui suit :

a) un jeu de caractères codés (mappage d'un jeu de lettres en un jeu de nombres entiers) tel que décrit dans [RFC 2277 de l'IETF] et [RFC 2130 de l'IETF]

b) un jeu de glyphes pour relier un jeu de nombres entiers à un jeu de lettres

c) des règles de conversion entre les jeux de caractères codés, si plusieurs jeux sont utilisés dans le système.

5.1.4 ST.25

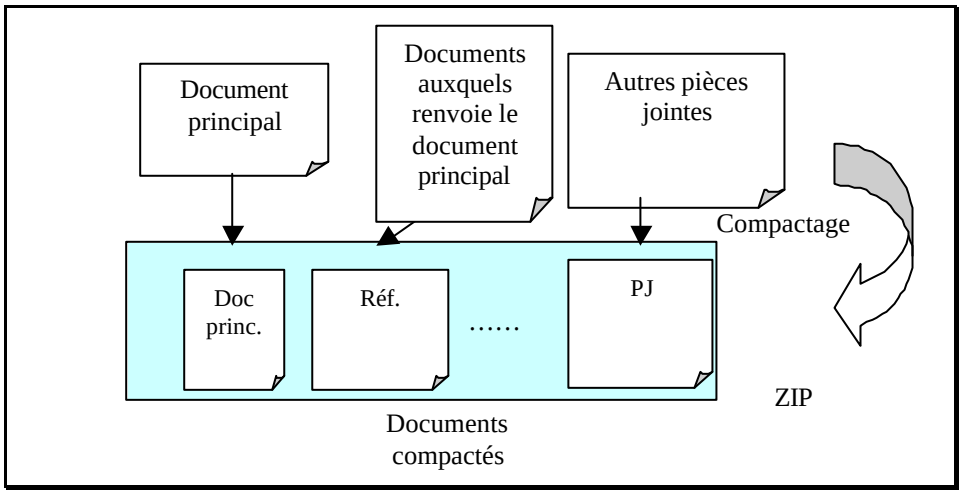
Un document créé en utilisant les balises SGML de la norme ST.25 de l'OMPI pour les listages de séquences peut être introduit comme document externe dans le bloc des documents constitutifs de la demande compactés (WAD, Wrapped Application Documents).

5.1.5 ASCII

Un document créé en plein texte ASCII peut être inséré comme document externe dans un WAD. Dans ce cas, le document principal XML doit comporter la page de code du texte ASCII.

5.1.6 Compactage des documents

Le document principal, les documents auxquels il renvoie expressément et les autres pièces jointes, le cas échéant, sont compactés en un seul bloc de données. Ce bloc de données, dit "documents constitutifs de la demande compactés" est créé par application du standard de compression ZIP. Le déposant doit utiliser un logiciel d'archivage et de compression en format ZIP pour grouper les fichiers des documents qui constituent la demande électronique.



Le logiciel employé pour créer le fichier ZIP doit être conforme aux spécifications du format ZIP, publiées dans le descriptif du logiciel PKZIP® de PKWARE® (révisé le 08/01/1998), sur la page web de PKWARE® : *http://www.pkware.com/appnote.html*.

Devront être comprimés les fichiers correspondant à toutes les parties du document identifiées par ailleurs dans la présente spécification. Tous les fichiers externes auxquels renvoie le mémoire descriptif de l'invention doivent être inclus dans l'envoi en fichier ZIP. Les noms de fichiers figurant dans le répertoire central du fichier ZIP doivent respecter les spécifications du système d'opération applicable, précisées dans une autre partie de la présente spécification.

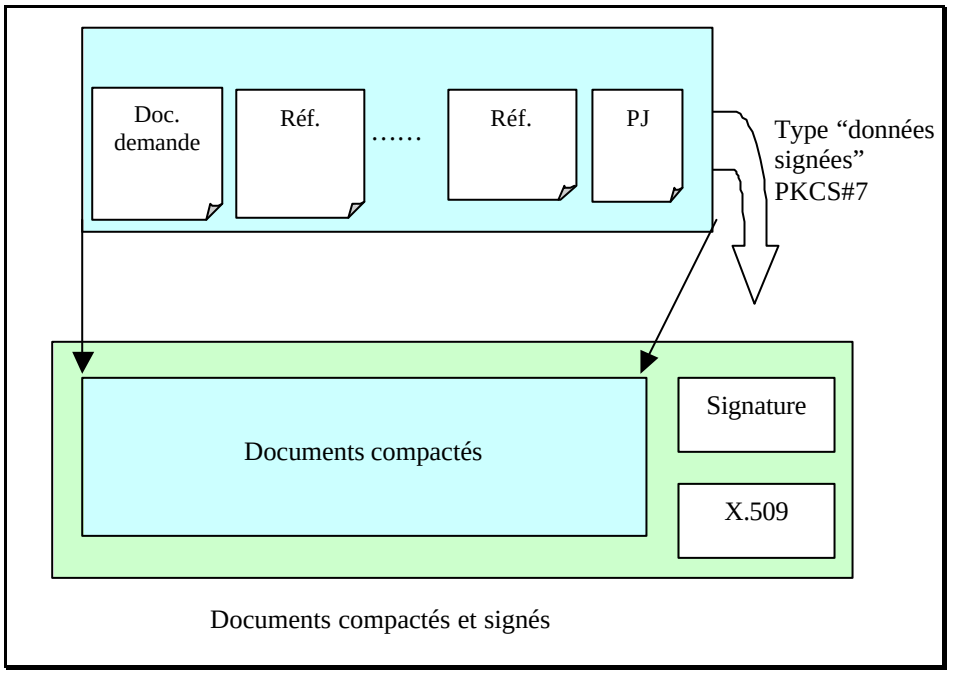
Tous les fichiers ZIP doivent avoir une structure de répertoire plate. Lorsqu'une collection de fichiers doit être intégrée dans un fichier ZIP, il faut la compacter en un fichier ZIP unique qui sera incorporé à plat.

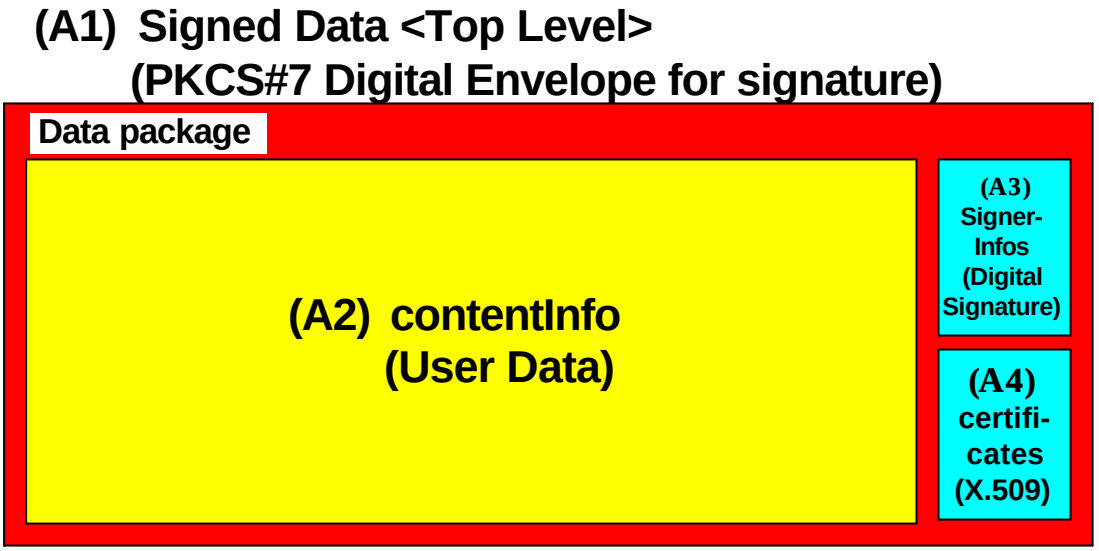
Le standard ZIP donne au logiciel de compression le choix parmi un certain nombre d'algorithmes de compression. La méthode de compression par défaut sera la "déflation" avec l'option compression normale. Les logiciels de décompression traitent ce format sans la moindre difficulté. La méthode de compression par "rétrécissement" ne sera pas employée parce qu'elle fait appel à un algorithme de compression LZW (Lempel-Ziv-Welch) qui est protégé par un brevet détenu par la société UNISYS.

5.2 Signature des documents constitutifs de la demande compactés

Afin de lier la personne qui crée le paquet aux documents électroniques de la demande compactés, une signature numérique est ajoutée pour créer l'élément "documents constitutifs de la demande compactés et signés". L'adjonction de cette signature a pour objet d'identifier le déposant et de permettre au destinataire de détecter toute altération non autorisée en cours de transmission.

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





Règles de production de l'enveloppe numérique PKCS#7 aux fins de certification

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 le standard *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 SignedData (données signées), premier niveau

N°.	Nom d'article	Article PKCS#7	Contenu
1	Version	Version	Mettre la valeur entière "1"
2	Jeu d'identificateurs d'algorithme	DigestAlgorithms	
2.1	Identificateur d'algorithme	AlgorithmIdentifier	Mettre UN SEUL **jeu** d'identificateurs d'algorithme {sha-1}
3	Information relative au contenu	ContentInfo	Mettre une information relative au contenu (voir le tableau A2)
4	Certificats	Certificates	Mettre un élément Certificates (voir le tableau A4)
5	Listes d'annulation	Crls	Vide (ne rien mettre)
6	Information relative au signataire	SignerInfos	Mettre un élément signerInfos (voir le tableau A3)

Tableau A2 contentInfo (information relative au contenu), premier niveau

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

Tableau A3 signerInfos (informations relatives au signataire), premier niveau

N°	Nom d'article	Article PKCS#7	Contenu
1	Version	Version	Mettre la valeur entière "1"
2	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)
3	Jeu d'algorithmes de compression	DigestAlgorithm	
3.1	Identificateur d'algorithme	AlgorithmIdentifier	Mettre UN SEUL **jeu** d'identificateurs d'algorithme {sha-1} pour la production d'une empreinte de signature numérique
4	Attributs authentifiés	AuthenticatedAttributes	Vide (ne rien mettre)
5	Algorithme de chiffrement de l'empreinte	DigestEncryptionAlgoritm	Identificateur d'OBJET de l'algorithme de chiffrement de l'empreinte (algorithme recommandé: rsaEncryption)
6	Empreinte chiffrée	EncryptedDigest	Empreinte des données du message; le contenu est chiffré au moyen de la clé privée du signataire
7	Attributs non authentifiés	UnauthenticatedAttributes	Vide (ne rien mettre)

Tableau A4 certificates (certificats), premier niveau

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

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

6 Envoi

Un office récepteur peut décider de ne pas utiliser le mécanisme d'enveloppement décrit dans cette section comme mécanisme de chiffrement pour la transmission, s'il utilise un chiffrement au niveau de la voie d'accès du type SSL. En cas de transmission entre offices, il n'est pas nécessaire d'utiliser ces mécanismes de chiffrement si l'on utilise un réseau privé tel que TriNet.

6.1 Paquet de transmission

Le lot de données qui est effectivement transmis dans l'échange entre le déposant et l'office récepteur est appelé paquet.

Le paquet contient plusieurs articles, variables selon le type de paquet. On y trouve :

a) un objet "en-tête"
b) un élément "documents" constitué des documents compactés et signés
c) des données de transmission telles que l'heure de la transmission.

Dans l'en-tête sont indiqués le type de paquet, le nom de fichier de l'élément "documents", etc. L'objet en-tête est toujours présent dans le paquet. Il est écrit en XML, conformément à la DTD exposée à l'appendice II.

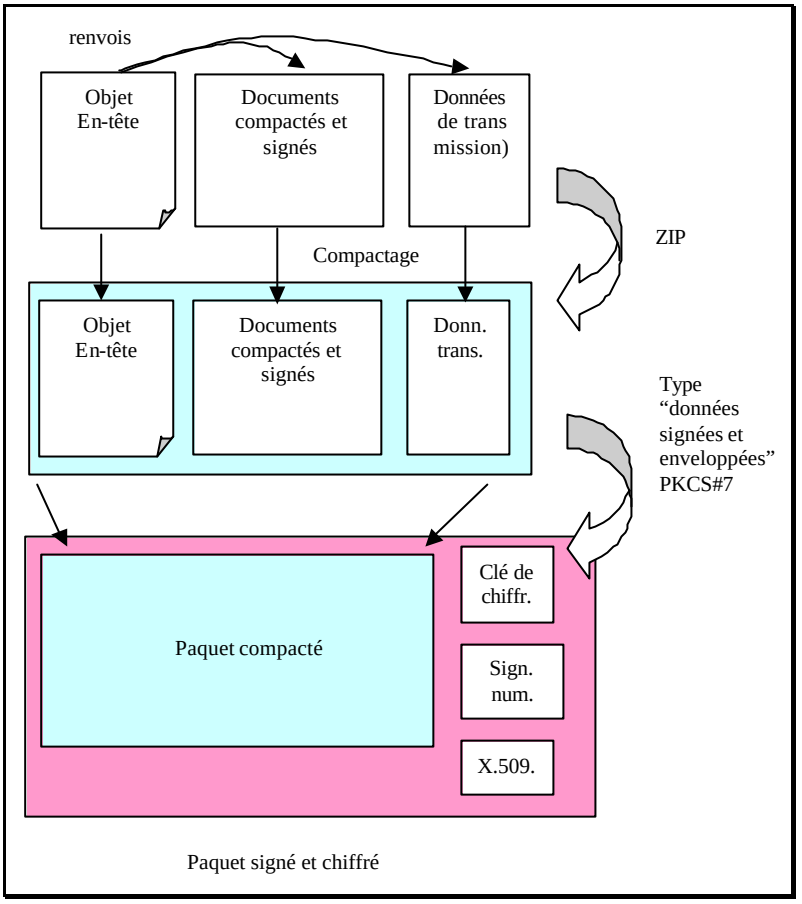
La marche à suivre pour créer le paquet est la suivante :

a) création d'un paquet compacté par compression ZIP des documents constitutifs de la demande, compactés et signés, avec les éléments utilisés pour la transmission

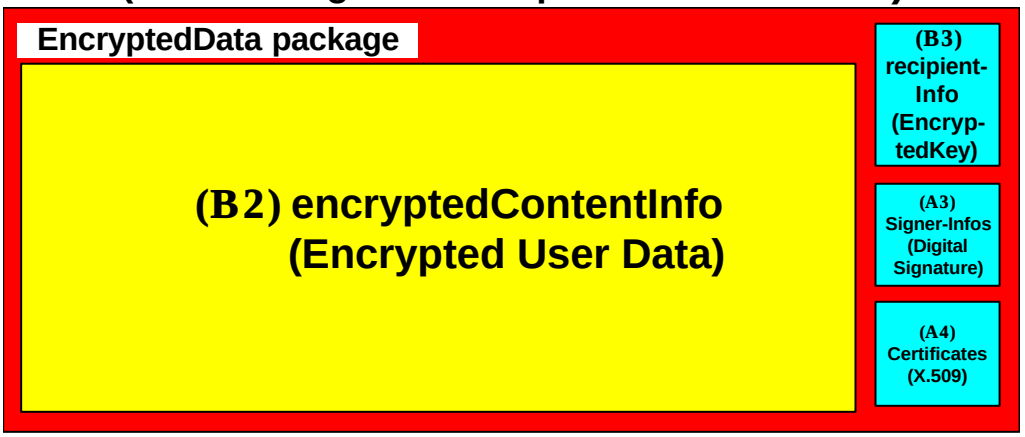
b) création d'un paquet signé et chiffré pour la transmission sur le réseau, avec chiffrement selon le type "données signées et enveloppées" PKCS#7.

La signature a pour objet d'assurer la combinaison et le contenu de chaque élément, et de permettre au destinataire de pouvoir détecter toute altération non autorisée intervenue en cours de transmission. Le chiffrement vise à éviter l'interception illicite des données en cours de communication.

La signature numérique pour les documents de la demande compactés peut être produite soit par le déposant, soit par son mandataire. La personne qui engage la transmission produit la signature numérique pour aboutir au type "données signées et enveloppées".



(B1) SignedAndEnvelopedData <Top Level>
(PKCS#7 Digital Envelope for Transmission)



Règles de production de l’enveloppe numérique de transmission PKCS#7

Tableau B1 SignedAndEnvelopedData (données signées et enveloppées), premier niveau

N°	Nom d'article	Article PKCS#7	Contenu
1	Version	Version	Mettre la valeur entière "1"
2	Informations relatives au destinataire	RecipientInfos	Mettre UN SEUL **jeu** d'éléments recipientInfo (voir le tableau B3)
2	Jeu d'identificateurs d'algorithme	DigestAlgorithms	
2.1	Identificateur d'algorithme	AlgorithmIdentifier	Mettre UN SEUL **jeu** d'identificateurs d'algorithme {sha-1}
3	Informations relatives au contenu chiffré	EncryptedContentInfo	Mettre un élément contenu chiffré (voir le tableau B2)
4	Certificats	Certificates	Mettre un élément Certificates (voir le tableau A4)
5	Listes d'annulation	Crls	Vide (ne rien mettre)
6	Informations relatives au signataire	SignerInfos	Mettre un élément signerInfos (voir le tableau A3)

Tableau B2 EncryptedContentInfo (information relative au contenu chiffré), premier niveau

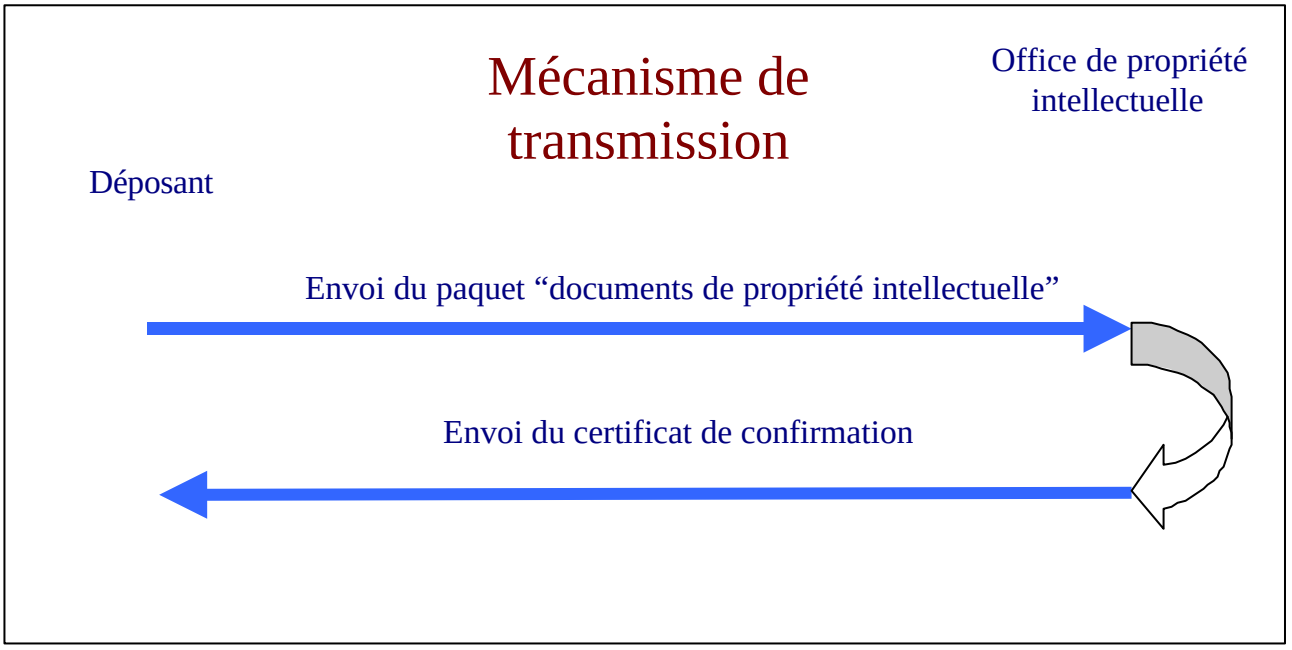
N°	Nom d'article	Article PKCS#7	Contenu
1	Type de contenu	ContentType	Mettre l'identificateur d'objet {pkcs-7 1}
2	Algorithme de chiffrement du contenu	ContentEncryptionAlgorithm	Identificateur d'OBJET de l'algorithme de chiffrement du contenu (algorithme recommandé = dES-EDE3-CBC
3	Contenu chiffré	EncryptedContent	Données utilisateur chiffrées

Tableau B3 recipientInfo (information relative au destinataire), premier niveau

N°	Nom d'article	Article PKCS#7	Contenu
1	Version	Version	Mettre la valeur entière "1"
2	Émetteur et numéro d'ordre	IssuerAndSerialNumber	Émetteur et numéro d'ordre du certificat comportant la clé publique pour le cryptage de la clé de chiffrement des données utilisateur
3	Algorithme de surchiffrement	KeyEncryptionAlgorithm	Identificateur d'OBJET de l'algorithme de cryptage de la clé de chiffrement des données utilisateur (algorithme recommandé = rsaEncryption)
4	Clé cryptée	EncryptedKey	Clé cryptée pour le déchiffrement des données utilisateur

6.2 Mécanisme de transmission

Le mécanisme de transmission fonctionne comme suit :



a) une session électronique est ouverte entre le déposant et l'office de propriété industrielle;

b) le déposant transmet le jeu complet des fichiers qui constituent le paquet "documents de propriété industrielle";

c) à réception du jeu complet de fichiers, les documents font l'objet d'un contrôle anti-virus et sont traités de manière à restituer leur empreinte univoque;

d) cette empreinte est comparée à l'empreinte initiale du message figurant dans les documents de la demande signés et compactés. Si les deux empreintes correspondent, un accusé de réception est envoyé au déposant. Si elles ne correspondent pas, le déposant en est dûment informé. La session prend alors fin.

6.2.1 Balayage anti-virus

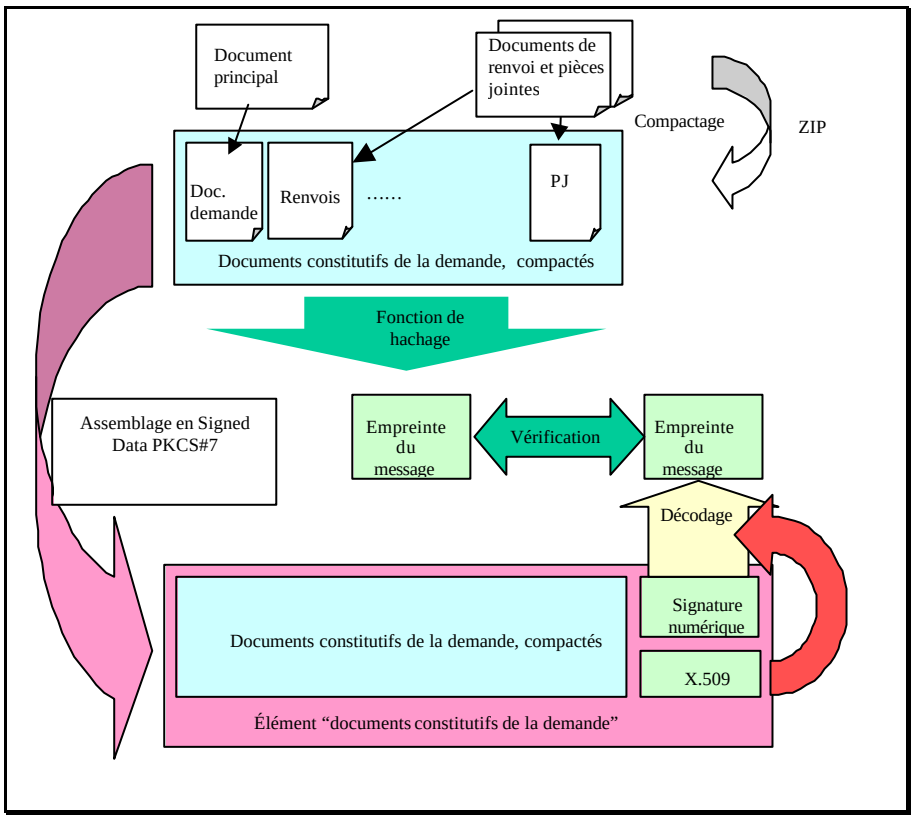
L'office récepteur doit balayer les envois électroniques pour détecter la présence éventuelle de virus.

Le Bureau international mettra un logiciel de balayage anti-virus à la disposition de tous les offices récepteurs participant au projet WIPONET.

Les responsables du projet WIPONET distribueront des manuels contenant des directives de sécurité à tous les offices participants. Ces manuels contiendront également des recommandations sur la méthode de balayage anti-virus des envois électroniques.

Les instructions administratives indiquent les mesures à prendre en cas de détection d'une éventuelle contamination par virus.

6.2.2 Vérification de l'empreinte du message



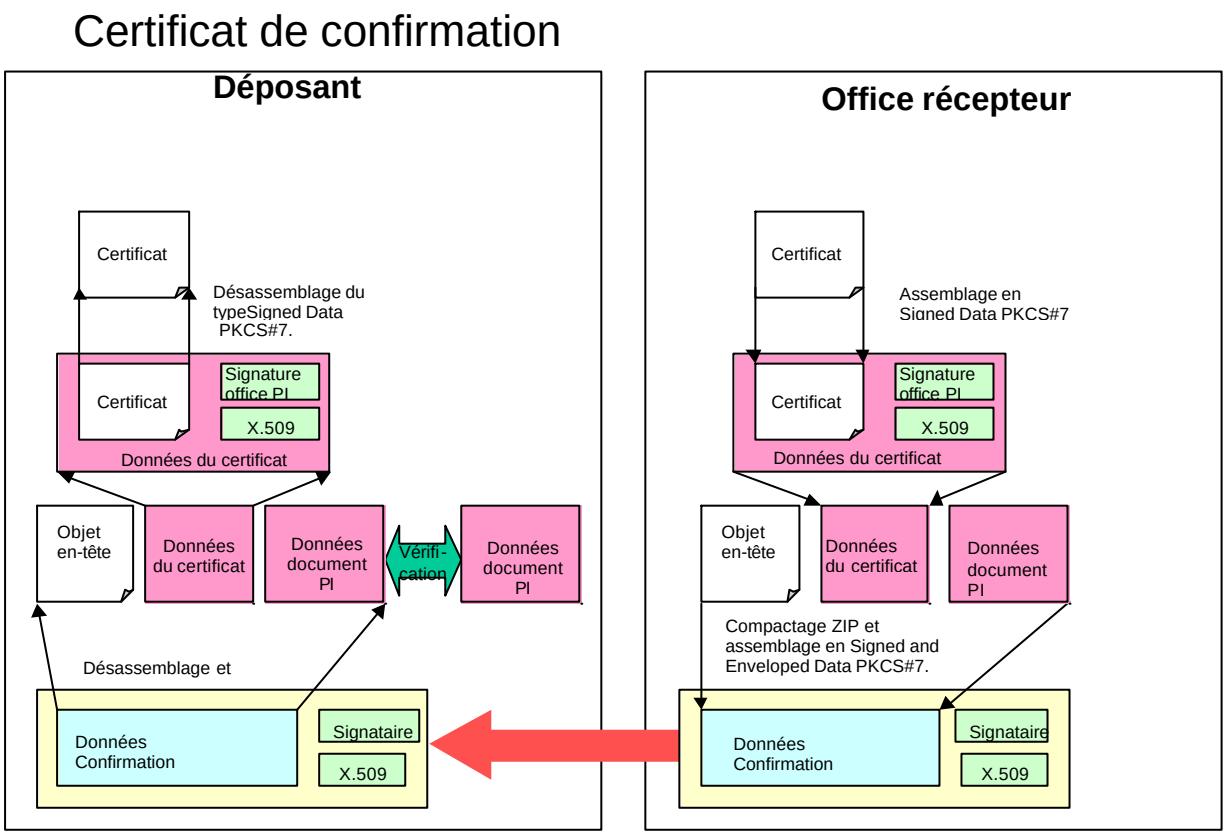
Lorsque l'office de propriété industrielle reçoit le paquet, il en ouvre les différents éléments et détermine le rôle de chacun d'après les indications qui figurent dans l'en-tête.

6.2.3 Certificat de confirmation

Le certificat de confirmation comporte un élément “données du certificat”, un objet d’en-tête indiquant que le paquet correspondant est un certificat de confirmation et, à titre facultatif, l’élément “documents constitutifs de la demande” reçu avec la nouvelle demande.

En cas de problème dans les communications ou dans la comparaison des empreintes de message, le certificat de confirmation renseigne sur le problème détecté.

Le certificat de confirmation est créé par compactage et assemblage des éléments en un type *Signed And Enveloped Data* (données signées et enveloppées) PKCS#7.



Le certificat de confirmation sert à informer le déposant de la réception de sa demande et doit contenir une version XML de cette information. Il peut contenir une version des données formatée en PDF, TIFF et JFIF(JPEG). Ces fichiers sont combinés en un fichier ZIP unique et signés au moyen du certificat numérique de l’office de propriété industrielle.

6.3 Protocole de trans mission

Afin d’accroître la probabilité de validation, une couche “protocole de transport” fiable doit être utilisée pour tous les transferts entre offices. Ce protocole sert à garantir que toutes les données à transmettre ont été correctement transférées entre les applications logicielles d’expédition et de réception et correctement réassemblées.

Chaque office récepteur doit préciser le protocole de transfert acceptable entre lui-même et le déposant. On recommandera les protocoles FTP ou protocole HTTP pour la transmission.

Facultatif : la sécurité de transmission assurée par le chiffrement du type "données signées et enveloppées" PKCS#7 sera normalement suffisant mais, si un office de propriété industrielle l'estime nécessaire, il peut opter pour un chiffrement au niveau de la voie d'accès du type SSL ou IP Sec, qui rendra la transmission encore plus sûre.

6.4 Supports matériels

Tout office récepteur peut choisir des supports matériels à la place ou en plus du dépôt en ligne. Les règles relatives aux exigences d'étiquetage ou d'emballage matériel sont définies dans l'appendice III.

7 Types d'échange de documents

La norme relative à l'échange de documents de propriété industrielle vise à couvrir tous les types d'échange entre déposants, représentants et offices de propriété industrielle. Les types d'échange suivants sont définis en détail :

7.1 Nouvelles demandes PCT

La procédure de création du format de données requis est la suivante :

a) création d'un document XML comme spécifié dans la section de l'appendice II consacrée à la DTD pour les nouvelles demandes PCT;

b) création d'un paquet compacté par compression ZIP du document XML et du document de la demande signé et compacté;

c) adjonction de la signature numérique du déposant en type "données signées" PKCS#7.

7.2 De l'office récepteur au Bureau international

La procédure de création du format des données est la suivante :

d) création d'un document XML contenant la date de dépôt, le numéro de la demande et un renvoi externe au WAD signé envoyé par le déposant;

e) création d'un paquet compacté par compression ZIP du document XML et du WAD signé;

f) adjonction de la signature numérique de l'office récepteur en type "données signées" PKCS#7.

7.3 De l'office récepteur à l'administration chargée de la recherche internationale

On utilise la même procédure que pour les communications de l'office récepteur au Bureau international.

7.4 Du Bureau international à l'office désigné (office élu)

Les données échangées entre le Bureau international et l'office désigné ne se limitent pas au document constitutif de la demande. Le format des données sera déterminé après discussion entre le Bureau international et l'office désigné. Si un office désigné ne peut pas recevoir le format des documents (par exemple PDF), le Bureau international enverra le document après l'avoir converti dans un format que l'office désigné accepte.

8 Mise en œuvre des renvois

Dans le cadre de l'élaboration de la présente norme, les offices de la coopération trilatérale préparent deux modalités de renvoi (toutes deux en JAVA et C++ sous Windows NT), qui permettent à d'autres concepteurs de réutiliser et d'étendre le code source initial fourni pour concevoir des implémentations spécifiques pour tel client ou telle procédure.
Les implémentations de renvoi couvrent les domaines suivants :

a) ZIP
b) PKCS#7
c) compactage
d) mécanisme de transmission comprenant l'envoi d'un certificat de confirmation.

Elle sont disponibles en code source et en code objet.

En outre, des jeux de données – tests standard sont à disposition pour vérifier les implémentations de tiers.

9 Accès à la forme électronique des documents

Un office récepteur peut, à titre facultatif, offrir aux déposants ou aux particuliers des moyens d'accès aux documents stockés sous forme électronique par cet office.

Un office récepteur peut autoriser l'accès à des données confidentielles. Pour s'assurer que seules les personnes autorisées ont accès aux données confidentielles, l'office utilisera des certificats reconnus avec des techniques ICP pour déterminer l'identité des personnes qui demandent l'accès.

Il est envisagé que le déposant puisse accéder par l'Internet aux services de base de données de l'office récepteur en utilisant un logiciel de navigation disponible sur le marché. Les versions actuelles des navigateurs Internet supportent des sessions SSL 128-bits, qui peuvent être utilisées pour assurer une communication chiffrée sécurisée entre le déposant et l'office récepteur.

L'office récepteur peut fournir au déposant, à sa demande, des documents électroniques dans des formats de documents standard supportés par cet office, envoyés par messagerie électronique ou messagerie électronique sécurisée, ou sur des supports matériels standard précisés à l'appendice III et supportés par cet office (disquette, disque compact enregistrable, etc.).

Supplément 1 - Sigles

DTD	*Document Type Definition* Définition de type de document
EPCT	*Electronic PCT Application* Demande électronique PCT
FTP	*File Transfer Protocol* Protocole de transfert de fichier
HTTP	*Hyper Text Transfer Protocol* Protocole de transmission
IETF	*Internet Engineering Task Force*
IP Sec	*IP Security* Protocole de sécurité Internet
PCT	*Patent Cooperation Treaty* Traité de coopération en matière de brevet
PKCS	*Public Key Cryptographic Standard* Standard de cryptographie à clé publique
ICP	Infrastructure à clé publique
RFC	*Request For Comments* Appel à commentaires
SGML	*Standardized Generic Mark-up Language* Langage normalisé de balisage généralisé
SSL	*Secure Sockets Layer* Couche de sockets sécurisés
WAD	*Wrapped Application Documents* Documents de la demande compactés
OMPI	Organisation Mondiale de la Propriété Intellectuelle
XML	*Extensible Mark-up Language* Langage de balisage extensible

[Fin du document]