Déclaration des pratiques de certification de l'Office européen des brevets

Version 1.10

Date d'entrée en vigueur : 1 janvier 2011

Office européen des brevets
Bayerstrasse 35
80335 Munich Allemagne
Tél. : +31 (0)70 340 4500
http://www.epo.org

Déclaration des pratiques de certification de l'Office européen des brevets

Date de révision : 16 mai 2011

Publié par
l'Office européen des brevets (OEB).

L'OEB est l'organe exécutif de l'Organisation européenne des brevets, dont le siège est Erhardtstrasse 27, 80469 Munich, Allemagne, et est représenté par le Président de l'OEB.

Contact
Les demandes concernant la présente Déclaration des pratiques de certification (DPC) sont à adresser à le service Soutien aux utilisateurs de l'OEB, Office européen des brevets, Bayerstrasse 35, 80335, Munich, Allemagne, courriel : support@epo.org

Droits d'auteur
Sauf indication contraire (usage limité ou soumis à une autorisation préalable), la reproduction, même partielle, des informations contenues dans le présent document est autorisée, moyennant l'indication des sources, pour autant qu'aucun changement ne soit apporté aux données.

Logo
Le logo officiel de l'OEB est protégé à l'échelle mondiale en tant qu'emblème officiel d'une organisation internationale en vertu de la Convention de Paris pour la protection de la propriété industrielle.

Clause de non-responsabilité
Le présent document décrit certains services dont la portée est limitée et qui sont mis à la disposition d'un groupe spécifique d'utilisateurs. Certaines limites de responsabilité s'appliquent comme indiqué en détail dans le présent document.

L'OEB ne garantit pas que les dispositions légales du présent document soient formulées de manière identique dans le texte officiel adopté. Seul fait foi le texte de la Convention sur le brevet européen (CBE) et des dispositions qui en découlent, tel qu'il est publié dans l'édition imprimée de la CBE publiée par l'OEB, ainsi que, le cas échéant, le texte des modifications qui y ont été apportées, telles qu'elles sont publiées dans les versions imprimées du Journal officiel de l'OEB.

La présente clause de non-responsabilité n'a pas pour but de limiter la responsabilité de manière contraire aux dispositions de la CBE ou aux dispositions juridiques nationales auxquelles renvoie la CBE.

Divers
Rien de ce qui précède ne doit être compris comme une renonciation de l'Organisation européenne des brevets aux privilèges et immunités qui lui sont conférés, en sa qualité d'organisation internationale, notamment par le Protocole sur les privilèges et immunités de l'Organisation européenne des brevets du 5 octobre 1973.

L'OEB se réserve le droit de modifier sans préavis, dans le cadre des dispositions juridiques en vigueur, tout ou partie des services et informations figurant dans le présent document.

Données internes

Historique des modifications

Version	Date	Description
1.00	1er mars 2008	Diffusion du document
1.10	16 mai 2011	Mise à jour du documents suite à la révision de certains instruments juridiques et changements organisationnels

TABLE DES MATIÈRES

TABLE DES MATIÈRES **5**

GLOSSAIRE **9**

REFERENCES **13**

1. INTRODUCTION À LA DÉCLARATION DES PRATIQUES DE CERTIFICATION DE L'OFFICE EUROPÉEN DES BREVETS **14**

1.1. Généralités 14
1.1.1. L'Office européen des brevets et ses services en ligne 14
1.1.2. Communications sécurisées avec l'OEB 14
1.1.3. Communications sécurisées entre les utilisateurs habilités et les autres institutions de propriété industrielle 14
1.1.4. L'ICP OEB dans les grandes lignes 15
1.1.5. Base juridique de l'ICP OEB 15
1.2. Identification 16
1.3. Communauté et champ d'application 16
1.3.1. Autorité de certification (AC) 16
1.3.2. Autorité d'enregistrement (AE) de l'OEB 16
1.3.3. Abonnés 16
1.3.4. Parties utilisatrices 16
1.4. Attributions et contacts 17
1.4.1. Administration de la Déclaration des pratiques de certification 17
1.4.2. Questions supplémentaires 18
1.4.3. Organe déterminant la conformité de la DPC par rapport à la PC 18
1.5. Entrée en vigueur et dispositions transitoires 18

2. DISPOSITIONS GÉNÉRALES **19**

2.1. Obligations 19
2.1.1. AC chargée des obligations incombant à l'OEB 19
2.1.2. AE chargée des obligations incombant à l'OEB 19
2.1.3. Obligations incombant à l'abonné(e) 19
2.1.4. Obligations incombant à la partie utilisatrice 20
2.1.5. Obligations concernant la banque d'archivage 20
2.2. Responsabilité 20
2.2.1. Étendue de la responsabilité de l'OEB 20
2.2.2. Limitation de la responsabilité 20
2.2.3. Lois régissant la responsabilité de l'OEB 21
2.2.4. Responsabilités de l'abonné(e) et de la partie utilisatrice 21
2.3. Responsabilité financière 21
2.3.1. Indemnisation par les parties utilisatrices 21
2.3.2. Relations fiduciaires 21
2.3.3. Procédures administratives 21
2.4. Interprétation et exécution 21
2.4.1. Droit applicable 21
2.4.2. Divers 22
2.4.3. Procédures de résolution des litiges 22
2.5. Taxes 23
2.5.1. Taxes d'émission ou de renouvellement de certificats 23
2.5.2. Taxes d'accès aux certificats 23
2.5.3. Taxes d'information sur la révocation et le statut 23
2.5.4. Taxes afférentes à d'autres services tels que l'information relative à la politique 23
2.5.5. Politique de remboursement 23

2.6. Publication et banque d'archivage 23
2.6.1. Publication d'informations relatives à l'AC de l'OEB 23
2.6.2. Fréquence de publication 23
2.6.3. Contrôles d'accès 23
2.6.4. Banques d'archivage 23
2.7. Audit de conformité 24
2.7.1. Fréquence des audits de conformité 24
2.7.2. Identité/qualifications de l'auditeur 24
2.7.3. Relations entre l'auditeur et la partie faisant l'objet de l'audit 24
2.7.4. Thèmes couverts par l'audit 24
2.7.5. Mesures à prendre en cas de carence 24
2.7.6. Communication des résultats 24
2.8. Confidentialité 24
2.8.1. Types d'informations soumises à confidentialité 24
2.8.2. Types d'informations considérées comme non confidentielles 24
2.8.3. Divulgation des informations relatives à la révocation/suspension des certificats 25
2.8.4. Divulgation d'informations aux agents chargés de faire appliquer la loi 25
2.8.5. Divulgation dans le cadre d'une instruction civile 25
2.8.6. Divulgation à la demande du titulaire 25
2.8.7. Autres circonstances justifiant la divulgation d'informations 25
2.9. Droits de propriété intellectuelle 25
3. IDENTIFICATION ET AUTHENTIFICATION 26
3.1. Enregistrement initial 26
3.1.1. Types de nom 26
3.1.2. Caractère significatif des noms 26
3.1.3. Règles d'interprétation des différents types de nom 26
3.1.4. Caractère unique des noms 26
3.1.5. Procédure de résolution en cas de litige portant sur le nom 26
3.1.6. Reconnaissance, authentification et rôle des marques 26
3.1.7. Preuve de la détention d'une clé privée 26
3.1.8. Authentification de l'identité de l'organisation 26
3.1.9. Authentification de l'identité individuelle 26
3.2. Renouvellement de clés 27
3.3. Renouvellement de clés après révocation 27
3.4. Demande de révocation 27
4. EXIGENCES OPERATIONNELLES 28
4.1. Demande de certificat 28
4.2. Émission des certificats 28
4.2.1. Génération des clés 28
4.2.2. Stockage sur porte-clés 28
4.2.3. Création de certificats 28
4.2.4. Génération des codes PIN 28
4.2.5. Distribution et livraison 29
4.3. Acceptation et activation du certificat 29
4.4. Révocation des certificats 29
4.4.1. Circonstances entourant la révocation 29
4.4.2. Qui peut demander la révocation ? 30
4.4.3. Procédure de demande de révocation 30
4.4.4. Délai de traitement des demandes de révocation 30
4.4.5. Circonstances entourant la suspension 30
4.4.6. Qui peut demander la suspension ? 30
4.4.7. Procédure de demande de suspension 30
4.4.8. Limites du délai de suspension 30
4.4.9. Fréquence de publication de la LCR (le cas échéant) 30
4.4.10. Exigences relatives aux vérifications de la LCR 30
4.4.11. Disponibilité de la vérification en ligne de la révocation ou du statut 31
4.4.12. Exigences relatives à la vérification en ligne des révocations 31
4.4.13. Autres formes d'annonces concernant la révocation 31
4.4.14. Exigences de vérification pour d'autres formes d'annonces concernant la révocation 31

4.4.15. Obligations particulières concernant la compromission relative aux clés....31
4.5. Procédures d'audit en matière de sécurité....31
4.5.1. Types d'événements enregistrés....31
4.5.2. Fréquence de traitement des fichiers-journaux....32
4.5.3. Période de conservation des fichiers-journaux d'audit....32
4.5.4. Protection des fichiers-journaux d'audit....32
4.5.5. Procédures de sauvegarde des fichiers-journaux d'audit....32
4.5.6. Système de collecte des données d'audit (interne/externe)....33
4.5.7. Notification sur l'origine de l'événement....33
4.5.8. Évaluations de vulnérabilité....33
4.6. Archivage....33
4.6.1. Types d'événements archivés....33
4.6.2. Période de conservation des archives....33
4.6.3. Protection des archives....33
4.6.4. Procédures de sauvegarde des archives....33
4.6.5. Système de collecte des archives (interne/externe)....33
4.6.6. Procédures visant à obtenir et vérifier les informations d'archive....33
4.7. Changement de clé....34
4.8. Récupération en cas de compromission et de sinistre....34
4.8.1. Compromission relative aux clés....34
4.8.2. Récupération en cas de sinistre....34
4.9. Cessation des activités de l'AC de l'OEB....34
5. CONTRÔLES DE SÉCURITÉ PHYSIQUES, PROCÉDURAUX ET RELATIFS AU PERSONNEL....35
5.1. Contrôles physiques....35
5.1.1. Emplacement et construction des sites....35
5.1.2. Accès physique....35
5.1.3. Électricité et climatisation....36
5.1.4. Dégâts des eaux....36
5.1.5. Prévention et protection contre les incendies....36
5.1.6. Stockage des supports de données....36
5.1.7. Élimination des déchets....37
5.1.8. Sauvegarde hors site....37
5.2. Contrôles procéduraux....37
5.2.1. Rôles de confiance....37
5.2.2. Nombre de personnes requis par tâche....38
5.3. Contrôles du personnel....38
5.3.1. Curriculum vitae, qualifications, expérience et habilitations....38
5.3.2. Procédures de vérification du curriculum vitae....38
5.3.3. Exigences en matière de formation....39
5.3.4. Besoins et fréquence des cours de recyclage....39
5.3.5. Rotation des postes....39
5.3.6. Sanctions pour actions abusives....39
5.3.7. Conditions relatives au personnel sous contrat....39
5.3.8. Documentation fournie au personnel....39
6. CONTRÔLES TECHNIQUES DE SÉCURITÉ....40
6.1. Génération et installation de paires de clés....40
6.1.1. Génération de paires de clés....40
6.1.2. Remise de la clé privée à l'entité....40
6.1.3. Remise de la clé publique à l'émetteur du certificat....40
6.1.4. Remise de la clé publique de l'AC de l'OEB et de la LCR aux utilisateurs habilités....40
6.1.5. Taille des clés....41
6.1.6. Génération de paramètres de clé publique....41
6.1.7. Contrôle de la qualité des paramètres....41
6.1.8. Génération matérielle/logicielle des clés....41
6.1.9. Finalités d'utilisation des clés (champ d'utilisation de la clé : X.509 v3)....41
6.2. Protection des clés privées....41
6.2.1. Normes du module de cryptage....41
6.2.2. Contrôle des clés privées par plusieurs personnes (n sur m)....41
6.2.3. Séquestre des clés privées....41

6.2.4. Sauvegarde des clés privées 42
6.2.5. Archivage des clés privées 42
6.2.6. Entrée de clés privées dans le module de cryptage de l'AC de l'OEB 42
6.2.7. Méthode d'activation des clés privées 42
6.2.8. Méthode de désactivation des clés privées 42
6.2.9. Méthode de destruction des clés privées 43
6.3. Autres aspects de la gestion des paires de clés 43
6.3.1. Archivage des clés publiques 43
6.3.2. Durée d'utilisation des clés publiques et des clés privées 43
6.4. Données d'activation 43
6.4.1. Génération et installation des données d'activation 43
6.4.2. Protection des données d'activation 43
6.4.3. Autres aspects des données d'activation 44
6.5. Contrôles de la sécurité informatique 44
6.5.1. Conditions techniques particulières en matière de sécurité informatique 44
6.5.2. Notation de la sécurité informatique 44
6.6. Contrôles techniques tout au long du cycle de vie des systèmes 44
6.6.1. Contrôle de développement des systèmes 44
6.6.2. Contrôle de la gestion de la sécurité 44
6.6.3. Notation en matière de sécurité tout au long du cycle de vie des systèmes 44
6.7. Contrôles de la sécurité des réseaux 44
6.8. Contrôles techniques du module de cryptage 45
7. PROFILS DES CERTIFICATS ET DES LCR 46
7.1. Profil des certificats 46
7.1.1. Numéro(s) de version 46
7.1.2. Extensions des certificats 46
7.1.3. Identificateurs d'objets algorithmiques 46
7.1.4. Formes des noms 46
7.1.5. Contraintes concernant les noms 46
7.1.6. Identificateur d'objets de la politique de certification 47
7.1.7. Extension concernant les contraintes afférentes à l'utilisation de la politique 47
7.1.8. Syntaxe et sémantique des qualificatifs de politique 47
7.1.9. Sémantique de traitement pour les extensions critiques de la politique de certification 47
7.2. Profil des LCR 47
7.2.1. Numéro(s) de version 47
7.2.2. Extensions des LCR et des entrées des LCR 47
8. GESTION DES SPÉCIFICATIONS 48
8.1. Procédures de modification des spécifications 48
8.2. Politiques de publication et de notification 48
8.3. Procédures d'approbation de la PC 48

GLOSSAIRE

Abonné(e)	[Annexe F] Entité qui est le sujet nommé ou identifié dans un certificat émis à son intention et qui détient une clé privée correspondant à la clé publique indiquée dans le certificat.
Autorité de certification (AC)	[Annexe F] L'AC est la partie de confiance qui émet et révoque les certificats de clé publique pour une communauté d'utilisateurs. L'AC doit vérifier les informations qui figurent sur les certificats de clé publique. L'AC a recours à ses propres serveurs ou systèmes informatiques et respecte les politiques et les procédures applicables à l'exploitation de ces serveurs. Le terme "serveur" désigne le matériel et les logiciels qui génèrent les certificats et les LCR.
Autorité d'enregistrement	[Annexe F] Autorité responsable de l'identification et de l'authentification des titulaires de certificats, mais pas de la signature ou de l'émission des certificats (en d'autres termes, l'autorité d'enregistrement (AE) se voit déléguer certaines tâches ayant trait à l'attestation d'identité pour le compte de l'AC). L'AE peut déléguer à son tour ses fonctions et les pouvoirs y afférents à des autorités locales d'enregistrement.
Banque d'archivage	[Annexe F] Système servant à stocker et à rechercher des certificats et d'autres informations relatives aux certificats.
Carte à puce	Support de stockage pour les clés privées et les certificats d'abonnés
Certificat	[Annexe F] Le certificat lie le nom de l'entité (et d'autres attributs) à la clé publique correspondante. Le certificat doit être conforme à la recommandation X.509 de l'UIT, version 3, et doit remplir au minimum les conditions suivantes : • contenir une clé publique correspondant à une clé privée sous le contrôle exclusif du sujet ; • nommer ou identifier d'une autre façon le sujet ; • identifier l'AC émettrice du certificat ; • identifier sa période de validité ; • contenir un numéro d'ordre de certificat ; • inclure les adresses électroniques des entités finales ; • être signé numériquement par l'AC émettrice.

Certificat simplifié	[Annexe F] Certificat numérique délivré au demandeur, par exemple dans le cadre de l'enregistrement du client de dépôt en ligne, ou obtenu auprès d'une AC, et qui identifie le demandeur sans vérification préalable de son identité.

Clé privée	[Annexe F] Dans la cryptographie à clé publique, la clé privée est celle parmi la paire de clés publique-privée d'un utilisateur qui n'est connue que de ce dernier. L'utilisateur utilise sa clé privée pour signer numériquement des données, et pour déchiffrer les données qui ont été chiffrées avec sa clé publique.
Clé publique	[Annexe F] Dans la cryptographie à clé publique, la clé publique est celle parmi la paire de clés publique-privée d'un utilisateur qui est portée à la connaissance des autres membres de la communauté d'utilisateurs via un certificat de clé publique. La clé publique de l'utilisateur est utilisée par les autres utilisateurs pour chiffrer des données destinées à l'utilisateur et pour vérifier la signature numérique de l'utilisateur.
Compromission	[Annexe F] Divulgation, modification, substitution ou utilisation sans autorisation de clés de cryptage de textes en clair sensibles et d'autres paramètres de sécurité fondamentaux.
Déclaration des pratiques de certification (DPC)	[RFC 2527] Déclaration relative aux pratiques suivies par l'AC pour émettre des certificats.
Demandeur de certificat	Personne faisant la demande d'une carte à puce contenant des certificats d'abonnés afin d'accéder aux services sécurisés de l'OEB. Une fois approuvée par l'OEB, cette personne reçoit l'appellation d'abonné(e).
Domaine d'infrastructure à clé publique	[Annexe F] Entité indépendante consistant en une ou plusieurs autorités de certification auprès desquelles les abonnés détiennent le même certificat d'ancrage ou certificat principal.
Identificateur d'objet	[Annexe F] Numéro spécialement formaté, enregistré auprès d'un organisme de normalisation internationalement reconnu. Il doit permettre d'identifier les documents d'une organisation relatifs à sa politique et à ses pratiques en matière d'ICP.
Listes de certificats révoqués (LCR)	[Annexe F] Liste horodatée de certificats révoqués, munie de la signature numérique de l'AC.

Module de cryptage	[Annexe F] Ensemble de matériels, logiciels et microprogrammes, ou combinaison de ces éléments, qui servent à mettre en application une logique ou des fonctions de cryptage, dont les algorithmes de chiffrement, et qui sont contenus dans le périmètre de cryptage du module.

Nom distinctif	[Annexe F] Nom particulier à chaque titulaire de certificat ou abonné(e). Chaque entité du domaine ICP doit avoir un nom distinctif (ND) qui soit facilement reconnaissable et qui lui soit spécifique dans le champ d'identification de l'objet du certificat.
OEB	Office européen des brevets
Partie utilisatrice	[RFC 2527] Destinataire d'un certificat qui agit sur la base du certificat et/ou des signatures numériques vérifiées au moyen du certificat.
Politique de certification	[RFC 2527] Ensemble de règles stipulant les conditions d'application d'un certificat à un groupe ou une classe d'application ayant des impératifs de sécurité communs. Ainsi, la politique de certification peut indiquer qu'un type de certificat est approprié pour authentifier l'échange électronique de données pour le commerce de marchandises dans une fourchette de prix donnée.
Révocation d'un certificat	[Annexe F] Expiration prématurée de la validité d'un certificat à compter d'une date déterminée.

Abréviations

AC	Autorité de certification
AC de l'OEB	Autorité de certification de l'Office européen des brevets
AE	Autorité d'enregistrement
AE de l'OEB	Autorité d'enregistrement de l'Office européen des brevets
Annexe F	Annexe F, Appendice II du PCT -Architecture ICP pour la norme e-PCT, en vigueur depuis le 1er octobre 2005
APT	Assistance procédurale et technique
CBE	Convention sur le brevet européen
DPC	Déclaration des pratiques de certification
ICP	Infrastructure à clé publique
ICP OEB	Infrastructure à clé publique de l'Office européen des brevets
LCR	Liste de certificats révoqués
NC	Nom commun du certificat
ND	Nom distinctif du certificat
OEB	Office européen des brevets
PC	Politique de certification
PCT	Traité de coopération en matière de brevets
REPD	Représentant de dépôt
SDC	Système de données clients
SGC	Système de gestion de cartes

Références

Cette Déclaration des pratiques de certification de l'OEB fait référence aux documents suivants :

[Annexe F] OMPI, Traité de coopération en matière de brevets, Instructions administratives du Traité de coopération en matière de brevets : Modifications relatives au dépôt et au traitement électronique des demandes internationales, Annexe F, Appendice II -Architecture ICP pour la norme e-PCT, en vigueur depuis le 1er octobre 2005

[RFC2527] Network Working Group, Internet X.509 Public Key Infrastructure, Request for comments : 2527, Certificate Policy and Certification Practices Framework, mars 1999 (en anglais).

[CBE] Convention sur la délivrance de brevets européens (Convention sur le brevet européen) du 5 octobre 1973 telle que modifiée par l'acte portant révision de l'article 63 de la Convention sur le brevet européen du 17 décembre 1991 et par l'acte portant révision de la Convention sur le brevet européen du 29 novembre 2000.

[PC] Politique de certification de l'Office européen des brevets

[APU] Accord passé avec les parties utilisatrices

[AA] Accord d'abonnement

1. INTRODUCTION À LA DÉCLARATION DES PRATIQUES DE CERTIFICATION DE L'OFFICE EUROPÉEN DES BREVETS

1.1. Généralités

La présente Déclaration des pratiques de certification (DPC) complète la Politique de certification (PC) de l'Office européen des brevets. Ces deux documents concernent l'infrastructure de clé publique de l'Office européen des brevets (ICP OEB) et suivent la présentation proposée dans le document RFC 2527. Tandis que la PC décrit les impératifs liés à l'ICP OEB, la DPC va au-delà et décrit les pratiques employées par l'OEB pour délivrer, utiliser et révoquer des certificats d'abonnés au sein de l'ICP OEB, afin de répondre aux impératifs stipulés dans la PC. Certains passages de la PC ont été repris tels quels dans la DPC, notamment ceux qui ne nécessitent pas d'explications plus approfondies. Ces passages sont indiqués en italique dans la DPC pour être plus facilement reconnus.

1.1.1. L'Office européen des brevets et ses services en ligne

L'Office européen des brevets (OEB) est l'organe exécutif de l'Organisation européenne des brevets. Il a été créé par la Convention sur le brevet européen (CBE) et est doté d'une autonomie administrative et financière. Il délivre les brevets européens via une procédure unitaire et centralisée (art. 4 CBE). L'OEB effectue également des tâches au titre du Traité de coopération en matière de brevets (PCT) sur la base de la dixième partie de la CBE.

L'OEB a créé une gamme de produits et services en ligne pour permettre aux déposants, aux conseils en brevets et aux autres utilisateurs d'effectuer leurs transactions avec l'OEB sous forme électronique.

1.1.2. Communications sécurisées avec l'OEB

Même si un grand nombre de ces produits et services sont accessibles au public sans enregistrement, ils constituent aussi un environnement sécurisé dans lequel les utilisateurs habilités peuvent communiquer électroniquement de façon sécurisée avec l'OEB.

Ces utilisateurs habilités sont généralement des déposants ou leurs mandataires (mandataires agréés, employés de cabinets de brevets, avocats) (cf. art. 133 et 134 CBE).

Dans le but de fournir ces services sécurisés, l'OEB met son infrastructure de clé publique (l'ICP OEB) à la disposition des utilisateurs habilités. Dans le cadre de cette infrastructure, l'autorité de certification de l'Office européen des brevets (l'AC de l'OEB) émet des certificats d'abonnés aux utilisateurs habilités.

La présente Déclaration des pratiques de certification (DPC) de l'OEB décrit les pratiques employées par l'OEB pour délivrer, utiliser et révoquer des certificats d'abonnés au sein de l'ICP OEB.

1.1.3. Communications sécurisées entre les utilisateurs habilités et les autres institutions de propriété industrielle

En plus de ce qui précède, l'OEB, moyennant des arrangements spécifiques sur les questions juridiques ou autres, met à disposition, aux mêmes fins, ses services en ligne pour une utilisation entre des utilisateurs habilités et certaines autres organisations et institutions nationales et internationales et les institutions qui ont pour mission de traiter des demandes de brevets.

Si certaines conditions et exigences sont satisfaites, l'ICP OEB peut donc aussi être mise à la disposition des déposants, de leurs mandataires et d'autres utilisateurs habilités en vue de permettre des communications sécurisées avec certaines autres organisations et institutions nationales et internationales et les institutions qui ont pour mission de traiter des demandes de brevets.

1.1.4. L'ICP OEB dans les grandes lignes

L'ICP OEB comprend :

- une autorité de certification (l'AC de l'OEB), qui comprend une banque d'archivage des certificats révoqués ;
- une autorité d'enregistrement (l'AE de l'OEB) ;
- des abonnés.

Les abonnés sont des utilisateurs habilités tels que décrits aux points 1.1.2 et 1.1.3. Les certificats d'abonnés sont des certificats distribués sur des cartes à puce aux déposants, à leurs mandataires (art. 134(1), (8) ; 133(3) CBE), et à tout autre utilisateur ayant à communiquer électroniquement avec l'OEB (cf. 1.1.1).

Les certificats d'abonnés sont émis à la discrétion de l'OEB et destinés uniquement à des personnes physiques. Ils constituent des "certificats simplifiés" au sens de l'Annexe F. On se référera également au point 3 (Identification et authentification) et au point 7 (Profils des certificats et des LRC).

Les parties utilisatrices peuvent se fier aux certificats d'abonnés, comme cela est précisé dans la PC.

Bien que l'OEB conserve la responsabilité de tout ce qui touche à l'ICP OEB telle que définie dans la PC, il sous-traite à des tiers certains services liés notamment au fonctionnement de l'ICP, par exemple la gestion et l'administration des services de l'AC de l'OEB et le traitement de l'émission des cartes à puce.

1.1.5. Base juridique de l'ICP OEB

La base juridique sur laquelle repose le dépôt électronique, auprès de l'OEB ou auprès des services nationaux compétents lorsque cela est permis, de demandes de brevets européens, de demandes internationales (PCT) et d'autres documents, figure à la règle 2 CBE ainsi qu'à la règle 89bis 1 et 2 PCT.

Sur la base des dispositions juridiques susmentionnées, la Décision du Président de l'Office européen des brevets, en date du 12 juillet 2007, relative aux signatures électroniques, aux supports de données et aux logiciels utilisés pour le dépôt électronique de demandes de brevet et d’autres documents (édition spéciale n° 3, JO OEB 2007, A5), précisent les conditions de ce dépôt électronique, notamment en ce qui concerne l'utilisation de signatures électroniques, et la Décision du Président de l'Office européen des brevets, en date du 26 février 2009, relative au dépôt électronique de documents (JO OEB 2009, 182), et la Décision du Président de l'Office européen des brevets, en date du 8 février 2010, relative au logiciel de dépôt en ligne de l'OEB à utiliser pour le dépôt électronique de documents (JO OEB 2010, 226), précisent les conditions de ce dépôt électronique, notamment en ce qui concerne l'utilisation de signatures électroniques.

L'ICP OEB satisfait aux conditions énoncées à la Partie 7 et à l'Annexe F des Instructions administratives du PCT concernant le dépôt électronique et le traitement des demandes internationales. Des passages et définitions issus de ces documents sont repris dans des documents liés à l'ICP OEB, lorsque cela est applicable.

La base juridique de la communication électronique de l'abonné(e) avec d'autres parties désignées dépend des règlements et conditions qui régissent les communications avec lesdites parties. Ces règlements et conditions sont à obtenir auprès desdites parties.

1.2. Identification

Le présent document est intitulé Déclaration des pratiques de certification de l'Office européen des brevets.

Un identificateur unique de document (identificateur d'objet) n'a pas été attribué au présent document.

1.3. Communauté et champ d'application

L'OEB fournit des services aux abonnés, en qualité d'AC. L'ICP OEB permet à l'OEB de fournir ces services. Elle est constituée de plusieurs éléments techniques.

On trouvera ci-dessous une description des éléments de l'ICP OEB et du champ d'application des certificats émis dans le cadre de l'ICP OEB.

1.3.1. Autorité de certification (AC)

L'AC agissant au sein de l'ICP OEB est l'AC de l'Office européen des brevets (AC de l'OEB). Cette AC de l'OEB émet la totalité des certificats d'abonnés.

Le certificat de l'AC de l'OEB a été certifié par l'AC de l'Organisation européenne des brevets. Cette AC principale peut, au besoin, émettre des certificats pour des AC subordonnées.

1.3.2. Autorité d'enregistrement (AE) de l'OEB

L'AE de l'OEB est chargée d'identifier et d'authentifier les demandes de certificats au sein de l'ICP OEB.

1.3.3. Abonnés

Les abonnés sont les personnes physiques qui utilisent les certificats et les clés privées générés au sein de l'ICP OEB et stockés sur une carte à puce.

L'AC de l'OEB distingue deux groupes d'abonnés différents :

- les abonnés qui, au moment de la demande de la carte à puce, sont connus à l'OEB comme parties enregistrées auxquelles est affecté un numéro de REPD, par exemple des mandataires agréés, employés de cabinets de brevets, avocats ; ces abonnés peuvent accéder à l'ensemble des services en ligne de l'OEB ;
- les abonnés qui, au moment de la demande de la carte à puce, ne sont pas connus à l'OEB, par exemple des premiers déposants ou mandataires ; ces abonnés ne peuvent accéder qu'à l'application de dépôt en ligne (Online Filing).

1.3.4. Parties utilisatrices

1.3.4.1. OEB

L'OEB est une partie utilisatrice en vertu de la PC.

1.3.4.2. Office récepteur

D'autres entités peuvent être parties utilisatrices pour autant qu'elles remplissent les conditions leur permettant d'être offices récepteurs au titre du PCT (cf. art. 10 PCT), et qu'en tant qu'offices récepteurs, elles aient notifié au bureau international (cf. Instructions administratives, 703) qu'elles sont disposées à recevoir des demandes internationales sous forme électronique et qu'elles indiquent notamment accepter l'AC de l'OEB eu égard à l'émission de certificats pour la signature électronique devant être utilisée dans le dépôt international (cf. Instructions administratives, 710 a)vi).

Le bureau international doit publier la notification visée ci-dessus (Instructions administratives, 710 c).

La partie utilisatrice est censée se fier aux certificats émis par l'AC de l'OEB selon les paramètres susdits uniquement pour les actions ayant trait au PCT pour lesquelles une signature électronique est requise. L'élargissement du champ de confiance de la partie utilisatrice en matière de certificats nécessite une base juridique en plus du présent paragraphe.

1.3.4.3. Service central de la propriété industrielle

D'autres entités peuvent être parties utilisatrices pour autant qu'elles agissent en tant que service central de la propriété industrielle d'un État contractant à la CBE ou d'un État qui n'est pas partie à la CBE mais qui a été désigné par l'OEB comme partie utilisatrice. À cette fin, l'OEB peut fixer, le cas échéant, des conditions que devra remplir le service central de la propriété industrielle concerné.

1.3.4.4. Organisations intergouvernementales

Certaines entités agissant comme organisations intergouvernementales chargées de délivrer des brevets peuvent être parties utilisatrices à condition que l'OEB les ait désignées en tant que telles. À cette fin, l'OEB peut fixer, le cas échéant, des conditions que devra remplir l'organisation intergouvernementale concernée.

1.3.4.5. Champ d'application

La carte à puce de l'OEB comprend deux types de certificats d'abonnés : les certificats d'authentification qui permettent aux abonnés de s'authentifier eux-mêmes vis-à-vis d'un environnement de réseau, et les certificats non répudiables qui permettent aux abonnés d'appliquer une signature électronique à un document.

Les certificats d'abonnés ne peuvent être utilisés qu'en rapport à des services fournis par l'OEB ou une partie utilisatrice.

1.4. Attributions et contacts

1.4.1. Administration de la Déclaration des pratiques de certification

La Direction Sécurité et Audit de l'OEB est chargée du suivi du document relatif à la Déclaration des pratiques de certification.

1.4.2. Questions supplémentaires

Des exemplaires du présent document peuvent être téléchargés sur http://www.epo.org/applying/online-services/security/smart-cards_fr.html Toute question supplémentaire peut être adressée à Soutien aux utilisateurs eBusiness, Office européen des brevets, Bayerstrasse 35, 80335, Munich, Allemagne,
courriel: support@epo.org

1.4.3. Organe déterminant la conformité de la DPC par rapport à la PC

L'organe qui détermine si la DPC de l'OEB est conforme à la PC est désigné au point 1.4.1, Administration de la Déclaration des pratiques de certification.

1.5. Entrée en vigueur et dispositions transitoires

La DPC entre en vigueur à la date indiquée sur la page de garde.

La date de diffusion mentionnée dans la DPC est la date à laquelle la version actuelle de la DPC est parue et a été mise à disposition pour publication conformément au point 2.6.

Au cas où la date d'entrée en vigueur est antérieure à la date de diffusion, il est confirmé ici que les dispositions de la DPC s'appliquent à l'ICP OEB à partir de la date d'entrée en vigueur.

Sauf indication contraire dans la DPC, la dernière version de la DPC constituera la Déclaration applicable et s'appliquera donc également à tous les certificats émis avant sa date d'entrée en vigueur.

Toute autre révision de la DPC prendra effet pour le fonctionnement de l'ICP OEB à partir de la date d'entrée en vigueur indiquée sur le document révisé.

2. DISPOSITIONS GÉNÉRALES

2.1. Obligations

2.1.1. AC chargée des obligations incombant à l'OEB

L'AC de l'OEB s'acquittera des obligations spécifiques requises en vertu de la PC et/ou par les documents connexes fondés sur la PC, dont la DPC. L'AC de l'OEB doit notamment :

- agir selon les dispositions de la PC et de la DPC en vigueur ;
- prendre des mesures raisonnables pour veiller à ce que sa propre clé privée reste confidentielle, et entourer l'accès à cette clé et son utilisation d'un environnement sécurisé ;
- permettre aux utilisateurs habilités de l'ICP OEB d'accéder à la PC ;
- émettre des certificats d'abonnés aux abonnés, sur réception d'une demande en cours de validité de l'AE de l'OEB, conformément aux dispositions de la DPC ;
- révoquer les certificats d'abonnés sur réception d'une demande de révocation valable, et informer l'abonné(e) de la révocation, conformément aux dispositions de la PC ;
- placer les certificats d'abonnés émis dans la banque d'archivage appropriée (N.B. : l'accès à cette banque est réservé aux parties habilitées) ;
- générer des paires de clés pour les abonnés sur carte à puce, faire suivre pour certification les demandes de certificats des abonnés, renvoyer le certificat d'abonné(e) sur la carte à puce et envoyer la carte à puce et le code PIN de la carte à puce à l'abonné(e) par courrier ;
- générer une liste de certificats révoqués (LCR) et publier la LCR dans la banque d'archivage appropriée.

2.1.2. AE chargée des obligations incombant à l'OEB

L'AC de l'OEB s'acquittera des obligations spécifiques requises en vertu de la PC et/ou par les documents connexes fondés sur la PC, dont la DPC. Les obligations suivantes incomberont notamment à l'AE de l'OEB :

- agir selon les dispositions de la PC et de la DPC en vigueur ;
- veiller à ce que les demandes de certificat soient en cours de validité ;
- recevoir et traiter les demandes de certificats d'abonnés ;
- recevoir des requêtes de révocation de la part de parties habilitées (point 4.4.2), effectuer des recherches raisonnables afin d'établir la validité de ces requêtes et envoyer les requêtes validées à l'AC de l'OEB ;
- informer l'abonné(e) et l'AC de l'OEB de la révocation du certificat d'abonné(e).

2.1.3. Obligations incombant à l'abonné(e)

L'abonné(e) s'acquittera des obligations spécifiques requises en vertu de la PC et/ou des documents connexes fondés sur la PC, dont la DPC et, le cas échéant, l'accord d'abonnement. L'abonné(e) doit notamment :

- s'assurer que les clés publique et privée ainsi que les certificats d'abonnés ne sont utilisés qu'en conformité avec les dispositions de la PC ;
- fournir des informations exactes et complètes lors de toute demande de certificat ;
- s'assurer en permanence que la clé privée et le code PIN protégeant la carte à puce servant de support à la clé privée sont à l'abri de toute perte, de toute divulgation à une partie non habilitée, de toute modification ou utilisation abusive au sens de la PC ;

- s'assurer que le code PIN de l'abonné(e) ne soit connu que de lui (d'elle) ;
- envoyer immédiatement une demande de révocation à l'AE de l'OEB en cas de compromission effective ou supposée des clés privées, du code PIN ou de la carte à puce, ou de tout changement dans les informations fournies dans la demande de certificat.

2.1.4. Obligations incombant à la partie utilisatrice

La partie utilisatrice s'acquittera des obligations spécifiques requises en vertu de la PC et/ou des documents connexes fondés sur la PC, dont la DPC et, le cas échéant, l'accord passé avec la partie utilisatrice. La partie utilisatrice doit notamment :
évaluer indépendamment si l'utilisation d'un certificat est appropriée pour un usage donné et s'assurer que le certificat sera effectivement utilisé pour un usage approprié ;
vérifier s'il n'y a pas eu révocation ou suspension d'un certificat avant d'accepter sa vérification.

2.1.5. Obligations concernant la banque d'archivage

L'OEB sera responsable des fonctions de la banque d'archivage de l'AC de l'OEB. Au moment de la révocation d'un certificat d'abonné(e), l'AC de l'OEB publiera une attestation de révocation dans la banque de révocation.

2.2. Responsabilité

2.2.1. Étendue de la responsabilité de l'OEB

2.2.1.1.

En mettant en œuvre l'ICP OEB, notamment en signant un certificat qui indique que la PC est utilisée, l'OEB garantira, vis-à-vis des parties (cf. 1.3.4) qui accordent leur confiance raisonnable aux informations véhiculées par les certificats, que seuls ses services de certification et d'archivage, ainsi que l'émission et la révocation des certificats et l'émission de LCR, sont conformes à la PC. L'OEB sera uniquement tenu de fournir des efforts raisonnables pour veiller à ce que les abonnés et les parties utilisatrices s'en tiennent à ce qui est stipulé dans la PC eu égard à tout certificat contenant une référence à la PC ou aux clés associées (cf. 2.2.4).

2.2.1.2.

L'OEB ne sera pas tenu responsable des conséquences qui pourraient découler d'une utilisation quelconque des certificats émis en vertu de la PC, à des fins autres que la communication entre l'OEB et les utilisateurs habilités (cf. 1.1.2 et 1.3.4.1). L'OEB ne sera pas tenu responsable de l'utilisation des certificats émis en vertu de la PC pour la communication entre les utilisateurs habilités et les autres services chargés de la propriété industrielle ou tout autre tiers (cf. 1.1.3, et 1.3.4.2 / 1.3.4.3 / 1.3.4.4). La responsabilité éventuelle des parties utilisatrices vis-à-vis des abonnés reste intacte.

2.2.2. Limitation de la responsabilité

2.2.2.1.

La disponibilité de l'ICP OEB peut être réduite pendant les périodes de maintenance ou de réparation du système ou suite à des facteurs indépendants de la volonté de l'OEB. L'OEB décline donc toute responsabilité en cas de non disponibilité de l'ICP OEB.

2.2.2.2.

L'indemnisation des dommages est exclue sauf si l'OEB les a causés intentionnellement ou par suite d'une négligence grave de sa part, s'ils portent atteinte à la vie, à la santé ou à l'intégrité physique des personnes, ou en cas de manquement à une obligation fondamentale. Dans ce dernier cas, si le plaignant n'est pas un consommateur (au sens de l'art. 13 du code civil allemand), la responsabilité de l'OEB se limite aux dommages caractéristiques et prévisibles.

2.2.3. Lois régissant la responsabilité de l'OEB

Sans préjudice des dispositions relatives au droit applicable (2.4.1), les réclamations formulées à l'encontre de l'OEB sont régies par l'art. 9 CBE. Aux fins de l'application des art. 9(1) et (2) CBE, le droit applicable sera le droit allemand.

2.2.4. Responsabilités de l'abonné(e) et de la partie utilisatrice

Les accords d'abonnement et les accords passés avec les parties utilisatrices reflèteront la responsabilité limitée de l'OEB telle qu'énoncée au point 2.2 de la PC, et ces accords, le cas échéant, exigeront des abonnés et des parties utilisatrices qu'ils s'engagent à respecter leurs obligations respectives stipulées aux points 2.1.3 et 2.1.4.

2.3. Responsabilité financière

2.3.1. Indemnisation par les parties utilisatrices

Dans la mesure où le droit applicable le permet, les accords d'abonnement et les accords passés avec les parties utilisatrices exigeront des abonnés et des parties utilisatrices qu'ils indemnisent l'OEB afin de réparer toutes conséquences découlant du non-respect des conditions stipulées dans ces accords ou ailleurs dans les documents relatifs à l'ICP OEB.

2.3.2. Relations fiduciaires

L'émission de certificats n'autorisera pas l'AC de l'OEB d'agir en qualité d'agent, de société fiduciaire, d'administrateur ou de représentant, sous quelque forme que ce soit, pour le compte des abonnés ou des parties utilisatrices.

2.3.3. Procédures administratives

Sans objet.

2.4. Interprétation et exécution

2.4.1. Droit applicable

2.4.1.1. Droit applicable

Le droit applicable sera la Convention sur le brevet européen (CBE) et les règles et règlements se fondant sur celle-ci. Le PCT, les règles et autres règlements qui se fondent sur le PCT seront applicables dans la mesure où la CBE ou la PC le prévoit. À titre subsidiaire, le droit allemand sera applicable, à l'exclusion du recours au droit allemand des litiges.

Cette disposition relative au droit applicable s'appliquera à la PC et aux autres documents relatifs à l'ICP OEB basés sur la PC, tels que la DPC, les accords d'abonnement et les accords passés avec les parties utilisatrices, sauf indication contraire dans lesdits documents.

Cette disposition relative au droit applicable n'exclura pas l'application d'autres dispositions légales nationales dans la relation entre les parties utilisatrices d'une part, et les abonnés d'autre part. Cette dernière phrase ne s'applique pas à l'OEB.

Cette disposition relative au droit applicable est fondée sur le principe selon lequel les procédures et l'interprétation doivent être uniformes pour toutes les parties impliquées dans l'ICP OEB, indépendamment de leur lieu d'établissement.

2.4.1.2. Privilèges et immunités accordés à l'OEB

La PC sera interprétée en sorte que les droits de l'Organisation européenne des brevets décrits dans la CBE, dont le Protocole sur les privilèges et immunités de l'Organisation européenne des brevets, signé à Munich, le 5 octobre 1973, soient préservés dans tous les cas.

2.4.2. Divers

Si l'une ou plusieurs dispositions de la PC s'avèrent non valides, illicites ou inexécutables en droit, quelle qu'en soit la raison, leur inexécutabilité n'affectera pas les autres dispositions ; la PC sera alors interprétée comme si la ou les dispositions non exécutables n'en avaient jamais fait partie et de façon à respecter, dans la mesure du possible, l'esprit d'origine de la PC.

Il ne peut être renoncé à aucune disposition ou stipulation de la PC, et celles-ci ne peuvent être modifiées, annulées, complétées ou résiliées, si ce n'est en conformité avec les procédures prévues dans la PC.

Les notifications, accords, requêtes ou autres communications de l'AC de l'OEB en vertu de la PC seront établies sous forme électronique ou sur papier.

2.4.3. Procédures de résolution des litiges

Si un litige survient en rapport avec la mise en oeuvre de l'ICP OEB, de la PC, de la DPC ou de tout autre document concernant l'ICP OEB, les parties s'engageront de bonne foi à fournir tous les efforts raisonnables afin de régler le litige par voie de négociation.

Tout litige découlant de la mise en oeuvre de l'ICP OEB sera soumis à un arbitrage rendu par un seul arbitre, qui sera définitif et aura force obligatoire pour les parties, conformément aux dispositions du code de procédure civile allemand (ZPO). La procédure d'arbitrage se déroulera à Munich.

Nonobstant ce qui précède, si l'OEB renonce à son immunité de juridiction nationale, les tribunaux de Munich seront compétents pour tout litige.

Lorsqu'en vertu du droit des brevets applicable, un événement découlant de la mise en oeuvre de l'ICP OEB permet à une partie de demander à ce qu'il soit statué, les moyens judiciaires y afférents primeront sur les procédures de résolution de litiges susmentionnées. Le point 2.4.1.2 s'applique.

Les accords d'abonnés et les accords passés avec les parties utilisatrices contiendront une clause de résolution des litiges incluant les principes susmentionnés, sauf si des circonstances particulières nécessitent que l'on s'en éloigne.

2.5. Taxes

Les taxes dont sont redevables les abonnés et les parties utilisatrices pour l'utilisation de l'ICP OEB, les actions afférentes à la gestion des certificats, l'utilisation de cartes à puce ou de tout autre composant ou service mentionné dans la PC ou la DPC, seront comprises dans les taxes pour les services rendus par l'OEB, ou mentionnées séparément.

2.5.1. Taxes d'émission ou de renouvellement de certificats

Les cartes à puce, certificats et logiciels correspondants seront généralement fournis gratuitement aux abonnés. L'OEB se réserve toutefois le droit de prélever une taxe dans certaines circonstances.

2.5.2. Taxes d'accès aux certificats

L'OEB ne prélèvera généralement pas de taxe pour la réalisation des certificats destinés aux parties utilisatrices.

2.5.3. Taxes d'information sur la révocation et le statut

Les informations relatives aux révocations seront données gratuitement.

2.5.4. Taxes afférentes à d'autres services tels que l'information relative à la politique

L'OEB ne prélèvera pas de taxe pour l'accès à l'information relative à la politique comme celle figurant dans la PC ou la DPC.

2.5.5. Politique de remboursement

Sans objet.

2.6. Publication et banque d'archivage

2.6.1. Publication d'informations relatives à l'AC de l'OEB

L'OEB publiera les informations suivantes (au minimum sur un site web accessible via l'internet) :

- Politique de certification de l'OEB
- Déclaration des pratiques de certification de l'OEB
- Certificat de l'AC pour l'Organisation européenne des brevets (certificat principal)
- Accord passé avec les parties utilisatrices
- Accord d'abonnement
- Certificat de l'AC de l'OEB
- Banque d'archivage des LCR

2.6.2. Fréquence de publication

L'AC de l'OEB publiera les informations répertoriées au point 2.6.1 ci-dessus dès qu'elles deviennent disponibles.

2.6.3. Contrôles d'accès

L'AC de l'OEB contrôlera l'accès à sa banque d'archivage afin d'éviter que les informations qu'elle contient ne soient mises à jour ou effacées par une autre partie.

2.6.4. Banques d'archivage

L'AC de l'OEB gèrera des banques d'archivage en vue de la publication des certificats d'abonnés, des LCR et de documents relatifs à l'IPC OEB.

2.7. Audit de conformité

2.7.1. Fréquence des audits de conformité

L'OEB procèdera, à titre périodique et ad hoc, à des vérifications et à des audits de son site et de ses opérations afin de s'assurer de leur fonctionnement conformément aux pratiques et aux procédures en matière de sécurité énoncées ou citées en référence dans sa DPC. L'OEB chargera également un auditeur externe d'effectuer chaque année un audit indépendant.

2.7.2. Identité/qualifications de l'auditeur

Un auditeur externe conduira un audit indépendant une fois par an. L'auditeur sera salarié d'une société professionnelle spécialisée qui respecte les normes et codes de conduite nationaux et internationaux en vigueur.

2.7.3. Relations entre l'auditeur et la partie faisant l'objet de l'audit

L'audit et le rapport d'audit seront régis par un contrat passé entre l'auditeur et la partie faisant l'objet de l'audit.

2.7.4. Thèmes couverts par l'audit

L'audit déterminera la conformité des systèmes et procédures de l'ICP OEB eu égard à la PC et à la DPC de l'OEB. Il déterminera le risque économique inhérent au non-respect de la PC et la DPC, conformément aux objectifs de contrôle identifiés.

2.7.5. Mesures à prendre en cas de carence

L'OEB prendra les mesures qu'il juge nécessaires et appropriées pour remédier aux carences décelées par l'audit.

2.7.6. Communication des résultats

L'OEB sera tenu de faire en sorte que l'ICP OEB fonctionne conformément aux exigences et contrôles en vigueur. Le rapport d'audit détaillé sera publié uniquement par l'OEB.

2.8. Confidentialité

2.8.1. Types d'informations soumises à confidentialité

- L'OEB traitera le contenu des demandes de certificats ou des requêtes de révocation, que celles-ci aboutissent ou non, comme confidentiel vis-à-vis de l'AC de l'OEB et de l'abonné(e)/demandeur, sauf dans les circonstances visées aux points 2.8.2 à 2.8.7.
- L'OEB traitera la documentation en matière de sécurité et de fonctionnement comme confidentielle vis-à-vis des abonnés et des parties utilisatrices. L'OEB divulguera toutefois ces documents à l'auditeur désigné, sur la demande de ce dernier.

2.8.2. Types d'informations considérées comme non confidentielles

L'OEB ne traitera pas comme confidentielles les informations contenues dans les certificats, les LCR ou la PC.

2.8.3. Divulgation des informations relatives à la révocation/suspension des certificats

Le contenu des LRC ainsi que le statut des différents certificats sera divulgué librement à toute partie utilisatrice.

2.8.4. Divulgation d'informations aux agents chargés de faire appliquer la loi

L'OEB pourra divulguer des informations qu'il détient en tant qu'AC, en tant qu'AE ou à d'autres titres en rapport avec la mise en oeuvre de l'ICP OEB, dans la mesure où une telle divulgation est autorisée par le droit qui régit la PC et fondée sur des instruments légaux vérifiables et appropriés (ex : ordonnances du tribunal). Ceci sera sans préjudice des privilèges et immunités de l'OEB.

2.8.5. Divulgation dans le cadre d'une instruction civile

L'OEB pourra divulguer des informations confidentielles relatives à un(e) abonné(e) en particulier si une instruction civile l'exige, dans la mesure où une telle divulgation est permise par le droit qui régit la PC et fondée sur une base juridique vérifiable et appropriée. Ceci sera sans préjudice des privilèges et immunités de l'OEB.

2.8.6. Divulgation à la demande du titulaire

L'OEB s'engagera à communiquer sur demande, à un(e) abonné(e), toute information le(la) concernant.

2.8.7. Autres circonstances justifiant la divulgation d'informations

Sans objet.

2.9. Droits de propriété intellectuelle

Tous les droits de propriété intellectuelle se rapportant aux certificats des abonnés et à la PC seront et demeureront la propriété de l'OEB.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Enregistrement initial

3.1.1. Types de nom

L'AC de l'OEB utilise les « Distinguished Names » X.501 dans les champs « Issuer » et « Object », comme indiqué dans le Tableau 1 :

	NL
Country (C)=	
Organisation (O)=	Office européen des brevets Non utilisé
Organisational Unit (OU)=	Non utilisé
State or Province (S)=	Non utilisé
Locality (L)=	
Common Name (CN)	European Patent Office CA

Tableau 1 – Attributs des « Distinguished Names » se trouvant dans le certificat de l'AC de l'OEB

Les certificats d'abonnés établis par l'AC de l'OEB contiennent un « Distinguished Name » (nom distinctif) X.501 conformément au point 7.1.

3.1.2. Caractère significatif des noms

L'AE de l'OEB s'assurera que la série d'attributs désigne chaque abonné(e) de manière unique et comporte des valeurs ayant un caractère significatif si l'on ajoute un numéro d'identification (ID) unique à quatre chiffres.

3.1.3. Règles d'interprétation des différents types de nom

Sans objet.

3.1.4. Caractère unique des noms

L'AC de l'OEB attribuera les noms conformément aux points 3.1.1 et 3.1.2, de sorte à éviter toute ambiguité. L'AC de l'OEB rejètera les demandes de certificat où le nom du demandeur n'est pas suffisamment distinct du ND d'un(e) abonné(e) existant(e).

3.1.5. Procédure de résolution en cas de litige portant sur le nom

L'AC de l'OEB devra résoudre tout litige pouvant découler de la désignation de noms, en affectant un numéro unique à chaque demandeur de certificat, puis en s'assurant que le NC et donc le ND est toujours unique.

3.1.6. Reconnaissance, authentification et rôle des marques

L'AC der l'OEB ne sera pas tenue d'obtenir des preuves concernant les marques.

3.1.7. Preuve de la détention d'une clé privée

Sans objet vu que les clés des abonnés sont générées par l'AC de l'OEB.

3.1.8. Authentification de l'identité de l'organisation

L'AC de l'OEB vérifiera si l'organisation dont relève le demandeur figure dans la système de données clients (Client Data System – CDS) de l'OEB.

3.1.9. Authentification de l'identité individuelle

Si l'OEB a déjà affecté un numéro REPD à un(e) nouvel(le) abonné(e), l'identité du demandeur sera authentifiée par l'AE de l'OEB, laquelle vérifiera les qualités de l'abonné dans le SDC.

Si le demandeur n'est pas référencé dans le SDC, son identité doit être authentifiée par l'AE de l'OEB, laquelle vérifiera les éléments suivants :

- prénom(s) ;
- nom de famille ;
- adresse postale ;
- adresse électronique ;
- passeport ou carte d'identité ;
- signature de l'abonné(e) sur le formulaire d'inscription envoyé par fax.

L'AE de l'OEB valide la demande de certificat en enregistrant le "nouveau dossier abonné(e)" dans le système de gestion des cartes.

3.2. Renouvellement de clés

Si les certificats de l'abonné(e) n'ont pas été révoqués 60 jours avant leur expiration, l'AE de l'OEB enverra un courriel à l'abonné(e), l'invitant à renouveler ses certificats. L'abonné(e) sera dirigé(e) vers la page web réservée aux inscriptions et, une fois son identité vérifiée, l'abonné(e) pourra demander de nouveaux certificats. L'identité de l'abonné(e) sera vérifiée au moyen de son certificat en cours de validité.

L'AC de l'OEB générera de nouvelles clés sur une nouvelle carte à puce. Cette carte, accompagnée des certificats, sera envoyée à l'abonné(e) avec une lettre d'acceptation. L'abonné(e) devra retourner la lettre d'acceptation à l'AE de l'OEB. Dès réception, l'AC et l'AE de l'OEB feront le nécessaire pour activer les certificats.

3.3. Renouvellement de clés après révocation

Pour le renouvellement de clés après révocation, la procédure d'identification et d'authentification sera la même que celle suivie pour l'enregistrement initial.
Le renouvellement de clés après révocation n'est pas autorisé dans les cas suivants :

- si le certificat révoqué avait été établi au nom d'une autre personne ;
- si l'AE de l'OEB a des raisons de penser que les pièces justificatives sont fausses.

3.4. Demande de révocation

Avant de révoquer un certificat, l'AE de l'OEB authentifiera l'identité du demandeur en vérifiant :

- les pièces justificatives fournies par le demandeur (qui peut être l'abonné(e) ou son employeur).

4. EXIGENCES OPERATIONNELLES

4.1. Demande de certificat

Pour chaque demande de certificat, les demandeurs sont tenus de :

- s'authentifier auprès de l'AE de l'OEB conformément aux conditions spécifiées au point **3** ;
- demander une (nouvelle) clé privée générée et protégée selon la politique de certification ou présenter une clé publique et prouver qu'ils sont en possession d'une clé privée en prouvant également que cette clé publique a été générée et protégée conformément à la politique de certification ;
- fournir les données personnelles devant être certifiées et/ou accompagner la demande de certificat.

L'AC et l'AE pour l'OEB apporteront tout le soin et la diligence voulus pour accepter et traiter les demandes de certificat. L'AC de l'OEB dressera des procédures détaillées de traitement des demandes de certificat.

4.2. Émission des certificats

L'émission d'un certificat par l'AC de l'OEB signifiera l'approbation complète et définitive de la demande de certificat par l'AC de l'OEB.

Le processus de production des certificats et les clés privées et porte-clés associés au certificat se compose de cinq parties (ou fonctions) distinctes ayant chacune leurs sous-systèmes.

Les cinq fonctions sont les suivantes :

- génération des clés,
- stockage sur porte-clés,
- création de certificats,
- génération des codes PIN,
- distribution et livraison.

4.2.1. Génération des clés

Les clés sont générées à l'intérieur d'une carte à puce, conformément au point 6.1 de la présente DPC.

4.2.2. Stockage sur porte-clés

Les clés sont stockées sur la carte à puce personnalisée de l'abonné(e).

4.2.3. Création de certificats

Une fois que le nouveau dossier d'abonné(e) a été chargé dans le système de gestion de cartes (SGC), une demande de certificat PKCS#10 est générée et soumise à l'AC de l'OEB. Après réception de la réponse de l'AC de l'OEB sur le certificat, PKCS#7, le système de gestion de cartes inscrira le certificat dans la carte à puce.

4.2.4. Génération des codes PIN

Une fois le certificat inscrit dans la carte à puce, une valeur aléatoire est définie pour le code PIN de l'utilisateur.

4.2.5. Distribution et livraison

L'AC de l'OEB enverra à l'abonné(e) un ensemble contenant une carte à puce personnalisée, un lecteur de cartes à puce, un CD de démarrage des services en ligne, la lettre d'acceptation et d'autres documents imprimés émanant de l'OEB, dans les 10 jours suivant l'approbation de la demande.

4.3. Acceptation et activation du certificat

Les abonnés doivent accuser réception de leur carte à puce en retournant leur lettre d'acceptation signée, par fax, à l'AC de l'OEB. Cet accusé de réception est réputé valoir acceptation du certificat.

Après réception de la lettre d'acceptation signée, on envoie le code PIN correspondant à l'abonné(e). Un fichier LDIF est envoyé également à l'AE de l'OEB via une connexion sécurisée. L'AE de l'OEB active le certificat en le chargeant dans la banque d'archivage via ce fichier LDIF. Une fois le certificat chargé dans la banque d'archivage, l'abonné(e) peut utiliser les services en ligne de l'OEB.

Si l'abonné(e) ne retourne pas la lettre d'acceptation dans les 8 semaines, l'administrateur du SGC annulera la demande de carte de cet(te) abonné(e).

4.4. Révocation des certificats

Les certificats seront révoqués lorsque leur période de validité est dépassée ou lorsqu'ils ne sont plus fiables.

4.4.1. Circonstances entourant la révocation

4.4.1.1. Certificats des abonnés

Les abonnés (ou d'autres, voir point 4.4.2) peuvent demander la révocation de leurs certificats. Les circonstances ci-dessous peuvent constituer des motifs de révocation d'un certificat (liste non limitative) :

- vol, perte, divulgation, modification ou toute autre compromission ou compromission supposée de la clé privée, du code PIN ou de la carte à puce de l'abonné(e) ;
- mauvais usage délibéré des clés et/ou des certificats de la part de l'abonné(e) ;
- manquement important aux exigences opérationnelles stipulées dans la PC ou dans d'autres documents pertinents (ex : accords d'abonnés) ;
- les informations relatives aux certificats deviennent ou s'avèrent incorrectes (ex : changement de nom suite à un mariage) ;
- émission incorrecte (ex : informations du certificat incorrectes) ou erronée du certificat ;
- refus par l'OEB de donner à l'abonné(e) les droits d'accès à un produit ou à un service quelconque ;
- départ de l'abonné(e) de l'entreprise ou de l'organisation.

4.4.1.2. Certificats de l'AC

L'OEB procèdera à la révocation d'un certificat de l'AC sous son contrôle :
s'il découvre ou a des raisons de penser que la clé privée de l'AC a été compromise ;
si des membres du personnel de l'OEB habilités à le faire demandent la révocation du certificat.

4.4.2. Qui peut demander la révocation ?

Les entités suivantes sont autorisées à demander la révocation d'un certificat d'abonné :

- le(la) titulaire du certificat (l'abonné(e)) ;
- l'employeur de l'abonné(e) ;
- l'AE de l'OEB ;
- l'AC de l'OEB ;
- d'autres parties autorisées par l'OEB.

Les demandes de révocation de certificats émis par l'AC ne seront acceptées que par les parties dûment habilitées par l'OEB pour ce faire.

4.4.3. Procédure de demande de révocation

Les demandes de révocation seront soumises à l'AE de l'OEB (par courriel, fax ou courrier) par l'abonné(e) ou son employeur. L'AE de l'OEB vérifiera si la demande de révocation a été soumise par une partie autorisée pour le certificat concerné et, en échange, déposera une demande de révocation auprès de l'AC de l'OEB.

L'AC de l'OEB traitera la demande pendant les heures de bureau et publiera le certificat révoqué dans la LCR. L'AE de l'OEB informera ensuite l'abonné(e) de la révocation par courriel.

4.4.4. Délai de traitement des demandes de révocation

L'AE de l'OEB fera tout son possible pour traiter les demandes de révocation dans un délai raisonnable.

4.4.5. Circonstances entourant la suspension

La suspension n'est pas prévue dans le cadre de l'ICP OEB.

4.4.6. Qui peut demander la suspension ?

La suspension n'est pas prévue dans le cadre de l'ICP OEB.

4.4.7. Procédure de demande de suspension

La suspension n'est pas prévue dans le cadre de l'ICP OEB.

4.4.8. Limites du délai de suspension

La suspension n'est pas prévue dans le cadre de l'ICP OEB.

4.4.9. Fréquence de publication de la LCR (le cas échéant)

- L'AC de l'OEB publiera sa LCR toutes les 24 heures, même si elle n'a subi aucun changement.
- Chaque LCR indiquera quand aura lieu sa prochaine publication, conformément à ITU-T X.509. Une nouvelle LCR peut être publiée avant la date indiquée.
- L' AC de l'Organisation européenne des brevets rééditera sa LCR tous les trois mois ou lorsque le certificat de l'une des sous-AC est révoqué.

4.4.10. Exigences relatives aux vérifications de la LCR

Avant d'accepter de vérifier un certificat, les parties utilisatrices s'assureront que le certificat ne soit pas en cours de révocation ni de suspension (sur l'ensemble de la chaîne de certification), conformément aux obligations des parties utilisatrices, qui sont stipulées dans l'accord passé par les parties utilisatrices.

4.4.11. Disponibilité de la vérification en ligne de la révocation ou du statut

Sans objet.

4.4.12. Exigences relatives à la vérification en ligne des révocations

Sans objet.

4.4.13. Autres formes d'annonces concernant la révocation

Sans objet.

4.4.14. Exigences de vérification pour d'autres formes d'annonces concernant la révocation

Sans objet.

4.4.15. Obligations particulières concernant la compromission relative aux clés

Sans objet.

4.5. Procédures d'audit en matière de sécurité

L'AC de l'OEB enregistrera manuellement ou automatiquement les événements suivants :

4.5.1. Types d'événements enregistrés

- Evénements de gestion du cycle de vie des clés de l'AC, notamment :
  - génération, sauvegarde, stockage, récupération, archivage et destruction des clés ;
  - événements de gestion du cycle de vie des dispositifs de cryptage ;
- Événements de gestion du cycle de vie des certificats de l'AC et des abonnés, notamment :
  - demande et renouvellement de certificats, renouvellement de clés et révocation de certificats ;
  - éussite ou échec du traitement des demandes ;
  - énération et émission de certificats et de LCR.

- Événements liés à la sécurité, notamment :
  - réussite et échec de tentatives d'accès au système ICP ;
  - actions menées par le personnel de Getronics PinkRoccade sur le système de
  - sécurité et ICP ;
  - lecture, écriture ou suppression de fichiers ou d'enregistrements sensibles au
  - niveau de la sécurité ;
    hangements de profils de sécurité ;
    accidents système, pannes de matériel et autres anomalies ;
    activités des pare-feu et des routeurs ;
    entrée/sortie de visiteurs sur le site de l'AC.

Les entrées des fichiers-journaux comprennent les éléments suivants :

- date et heure d'entrée ;
- numéro de série ou de séquence de l'entrée, pour les entrées de journal automatiques ;
- identité de l'entité créatrice de l'entrée de journal ;
- type d'entrée.

Les AE de l'OEB et les administrateurs enregistreront dans des fichiers-journaux les informations relatives à l'inscription, notamment les éléments suivants :

- type de document(s) d'identification présenté(s) par l'abonné(e) ;
- enregistrement de données ou de numéros d'identification uniques ou d'une combinaison de documents d'identification (ex : référence du permis de conduire d'un chauffeur), le cas échéant ;
- emplacement de stockage de copies de demandes et de documents d'identification ;
- identité de l'entité chargée d'accepter la demande ;
- méthode utilisée pour valider les documents d'identification, le cas échéant ;
- nom de l'AC réceptrice ou de l'AE présentant les documents, le cas échéant.

En outre, le SGC doit fournir des fichiers-journaux d'audit pleinement opérationnels, détaillant toutes les opérations réalisées et identifiant l'utilisateur qui a demandé l'opération en question. Des rapports peuvent être générés pour obtenir les informations suivantes :

- données générales : permet de naviguer dans la piste d'audit via des critères de recherche ;
- listes de matériel : affichent une liste imprimable du matériel et des personnes qui en disposent ;
- demandes de certificats : affiche les demandes de certificat envoyées à l'AC de l'OEB ;
- certificats émis : examen et révocation de certificats émis ;
- certificats révoqués : examen des demandes de révocation de certificats ;
- ajout/modification/suppression d'utilisateurs ;
- émission/changement/annulation de cartes ;
- modification de la configuration système.

4.5.2. Fréquence de traitement des fichiers-journaux

Les fichiers-journaux en ligne seront traités chaque jour ouvrable afin de détecter les problèmes qui se posent ou risquent de se poser en matière de sécurité.

4.5.3. Période de conservation des fichiers-journaux d'audit

Les fichiers-journaux seront conservés pendant sept ans au moins.

4.5.4. Protection des fichiers-journaux d'audit

Les fichiers-journaux en ligne seront protégés contre toute modification, par exemple par une protection en écriture des supports correspondants, et les rapports d'audit seront protégés de manière à ce que seul le personnel autorisé puisse y accéder.

Les données soumises à un audit ne quitteront pas les locaux, et l'examen de ces données ne sera autorisé que sous le contrôle de membres du personnel de l'OEB ou du personnel d'entreprises tierces, ayant un contrat avec l'OEB.

Les données archivées électroniquement sont protégées contre tout affichage abusif et toute modification, suppression ou autre altération abusive, par des contrôles d'accès physiques et logiques.

4.5.5. Procédures de sauvegarde des fichiers-journaux d'audit

- Une copie de chaque fichier-journal en ligne sera conservée dans un lieu sûr hors site.

- Il devra être possible d'examiner les fichiers-journaux pendant leur période de conservation.

4.5.6. Système de collecte des données d'audit (interne/externe)

Des fichiers-journaux seront créés sur tous les systèmes de l'ICP OEB.

4.5.7. Notification sur l'origine de l'événement

Sans objet.

4.5.8. Évaluations de vulnérabilité

L'OEB procédera régulièrement à des évaluations de la vulnérabilité des systèmes de son AC et de son AE. Les politiques, pratiques et configurations système seront mises à jour si nécessaire, en fonction des résultats des évaluations.

4.6. Archivage

4.6.1. Types d'événements archivés

Les archives renfermeront toutes traces pertinentes que possède l'AC de l'OEB, notamment:

- les demandes de certificat et les messages y afférents ;
- la correspondance échangée et les contrats conclus avec d'autres parties ;
- les informations relatives au renouvellement de clés par l'AC de l'OEB, y compris les identificateurs de clés et les certificats de l'AC de l'OEB ;
- les demandes de révocation et les messages échangés avec l'auteur de la requête et/ou l'abonné(e) ;
- les fichiers-journaux d'audit, y compris les rapports des audits annuels de l'AC de l'OEB ;
- tous types d'événement listés au point 4.5.1.

4.6.2. Période de conservation des archives

- Tous les rapports d'audit seront conservés pendant sept années au total après leur création.
- Si les supports d'origine sont incapables de conserver les données jusqu'au terme de la période requise, l'AC de l'OEB mettra en place des procédures pour assurer le transfert régulier des données sur de nouveaux supports.
- L'AC de l'OEB entretiendra les applications nécessaires au traitement des données archivées aussi longtemps qu'il le faut.

4.6.3. Protection des archives

L'AC de l'OEB veillera à ce qu'aucune entité ne modifie ou n'efface les archives.

4.6.4. Procédures de sauvegarde des archives

L'AC de l'OEB veille à ce que les données archivées soient stockées hors site, dans un endroit séparé et sûr.

4.6.5. Système de collecte des archives (interne/externe)

Les archives seront collectées en interne.

4.6.6. Procédures visant à obtenir et vérifier les informations d'archive

L'AC de l'OEB veillera à ce que seul le personnel autorisé puisse obtenir des informations d'archive.

4.7. Changement de clé

- L'AC de l'OEB génèrera une nouvelle paire de clés pour la signature et la vérification des certificats au moyen d'un système de scission/partage de clé, et génèrera un certificat pour elle-même en tant qu'AC de l'OEB, au moins trois mois avant l'expiration de l'ancienne clé privée d'AC de l'OEB.
- Le changement d'une paire de clés d'AC de l'OEB impliquera les mêmes mesures de sécurité que la création de la paire de clés d'origine.
- L'AC de l'OEB veillera à ce que le changement de clé n'occasionne qu'un minimum de dérangement aux entités subordonnées dans la chaîne de confiance de l'AC de l'OEB.

4.8. Récupération en cas de compromission et de sinistre

L'OEB a mis en œuvre des plans de continuité de services et de récupération en cas de sinistre, qui sont spécifiques aux applications et aux systèmes. Ces plans permettent d'assurer la poursuite des opérations sans compromission en cas de sinistre. Il convient de se référer au Plan de continuité de service pour la gestion de l'information dans les Directions principales (PD IM).

4.8.1. Compromission relative aux clés

En cas de compromission avérée ou supposée concernant la clé privée de l'AC de l'OEB, l'OEB avertira immédiatement toutes les entités subordonnées de la chaîne de confiance de l'AC de l'OEB. Si le certificat de l'AC de l'OEB est révoqué, tous les certificats subordonnés le seront aussi.

4.8.2. Récupération en cas de sinistre

L'AC de l'OEB a mis en place un site distant de récupération en cas de sinistre. Pour assurer la récupération, les mesures suivantes ont été prises :

- système entièrement documenté, comprenant la conception, les fichiers de configuration et les scripts détaillés d'installation des systèmes, le matériel et le logiciel ;
- procédures pour la sauvegarde et la restauration : les sauvegardes sont stockées dans deux endroits différents ;
- clones du matériel de cryptage : deux clones sont des sauvegardes en temps réel l'un de l'autre, sur des serveurs de signature différents.

4.9. Cessation des activités de l'AC de l'OEB

L'AC de l'OEB avertira ses abonnés de l'expiration du certificat de l'AC de l'OEB au moins six moins avant son expiration.

Par "cessation des activités de l'AC de l'OEB", il faut entendre que tous les services liés à l'AC de l'OEB sont définitivement suspendus. Cela ne s'applique pas lorsque les services sont transférés d'une organisation à une autre, ou lorsqu'une ancienne paire de clés d'AC de l'OEB est remplacée par une nouvelle.

5. CONTRÔLES DE SÉCURITÉ PHYSIQUES, PROCÉDURAUX ET RELATIFS AU PERSONNEL

5.1. Contrôles physiques

L'AC de l'OEB, comportant une unité de traitement de cartes à puce (avec le système de gestion de cartes – SGC), est installée sur un site sécurisé non-OEB, aux Pays-Bas.

L'AE de l'OEB est installée dans les locaux de l'OEB à Munich. La présente DPC traite des exigences de sécurité de la Politique de certification de l'OEB. Toutes les opérations de l'AC et de l'AE doivent être conduites dans un environnement protégé physiquement, destiné à dissuader, prévenir et détecter toute intrusion manifeste ou cachée.

5.1.1. Emplacement et construction des sites

Les informations relatives à l'emplacement et à la construction des sites seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

L'AC de l'OEB sera installée dans les locaux de Getronics PinkRoccade (GPR) à Apeldoorn. Toutes les opérations de l'AC de l'OEB et les opérations de traitement des cartes à puce pour l'OEB seront menées dans l'environnement protégé physiquement de GPR, conçu spécialement à cet effet.

L'AC de l'OEB met en place jusqu'à six niveaux de sécurité physique. Ces niveaux, décrits au point 5.1.2, sont les suivants :

- émission de cartes à puce (niveau 3) ;
- fonctions de l'AC (niveau 4) ;
- modules de cryptage en ligne pour l'AC de l'OEB (niveau 5) ;
- modules de cryptage hors ligne pour l'AC de l'Organisation européenne des brevets (niveau 7).

L'AC der l'OEB prendra les mesures raisonnables qui s'imposent pour héberger son site de façon sûre, de sorte que les murs ou les parois extérieurs ainsi que les plafonds et les toitures qui pourraient permettre des intrusions soient construits au moins en briques, en tuiles et en béton aggloméré. Les murs seront raccordés en haut et en bas à des plafonds/toitures et à des planchers, c'est-à-dire qu'ils doivent pénétrer dans les plafonds suspendus ou les planchers qui pourraient permettre l'accès par des espaces vides.

Les activités de l'AC de l'OEB, notamment les opérations de validation, seront réalisées dans les locaux du département de soutien aux utilisateurs eBusiness, qui se situent dans les bureaux de l'OEB à Munich.

5.1.2. Accès physique

Les informations relatives à l'accès physique seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

L'accès physique à l'AC de l'OEB se caractérise comme suit :

- l'accès au niveau 1 des locaux de GPR nécessite d'avoir un badge personnel de proximité ;
- au niveau 2, un contrôle d'accès individuel s'applique à toutes les personnes qui pénètrent dans les parties communes de l'AC de l'OEB, avec le badge personnel de proximité ;
- au niveau 3, un contrôle d'accès individuel est appliqué avec une authentification de deux facteurs, utilisant notamment la biométrie ;
- le centre de données situé au niveau 4 requiert un contrôle d'accès individuel, et la salle de remise des clés nécessite un double contrôle, avec chacun une authentification de deux facteurs, utilisant notamment la biométrie ;
- niveaux 5 à 7 : les unités de sécurité de cryptage (USC) en ligne sont protégées grâce à l'utilisation d'armoires fermées à clé ; les USC hors ligne sont protégées grâce à l'utilisation de coffres, d'armoires et de conteneurs fermés à clé ; l'accès aux USC et au matériel de codage est restreint conformément à la répartition des tâches chez GPR ;
- tous les accès physiques aux niveaux décrits ci-dessus sont automatiquement enregistrés dans des fichiers-journaux.

L'accès physique à l'AE de l'OEB se caractérise comme suit :

- le département de soutien aux utilisateurs eBusiness est gardée par du personnel de sécurité ;
- le département de soutien aux utilisateurs eBusiness est accessible aux employés de l'OEB pendant les heures d'ouverture ;
- l le département de soutien aux utilisateurs eBusiness est fermée à clé en dehors des heures d'ouverture ;
- toutes les informations que possède l'AE de l'OEB sont protégées grâce à l'utilisation d'armoires fermées à clé.

5.1.3. Électricité et climatisation

Les installations de l'AC et de l'AE de l'OEB sont équipés de systèmes d'alimentation principale et de secours :

- systèmes d'alimentation électrique assurant une alimentation continue et ininterrompue ;
- systèmes de chauffage, de ventilation et de climatisation permettant de contrôler la température et l'humidité relative.

5.1.4. Dégâts des eaux

L'AC de l'OEB prend toutes les mesures raisonnables qui s'imposent pour protéger son site contre les inondations -qu'il s'agisse d'eau venue de l'extérieur ou de fuite des installations de réfrigération et/ou de chauffage -susceptibles d'affecter les principales opérations de traitement (choix de l'emplacement géographique de l'AC au-dessus du niveau de la mer).

5.1.5. Prévention et protection contre les incendies

L'AC de l'OEB prend toutes les mesures raisonnables qui s'imposent pour protéger son site contre les incendies pouvant affecter les ordinateurs, les supports de données, les équipements ou les documents papier.

5.1.6. Stockage des supports de données

Les informations relatives au stockage des supports de données seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à

ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.
L'AC de l'OEB stockera ses supports de données mobiles en toute sécurité, dans les locaux OEB/GPR ou dans un emplacement sécurisé hors site.

5.1.7. Élimination des déchets

Les informations relatives à l'élimination des déchets seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

Les documents et le matériel sensibles seront déchiquetés avant d'être éliminés. Les dispositifs de cryptage seront physiquement détruits et remis à zéro conformément aux instructions du fabricant en matière d'élimination. Les autres déchets seront éliminés selon les exigences standard de l'OEB et de GPR dans ce domaine.

5.1.8. Sauvegarde hors site

L'AE de l'OEB procédera régulièrement à des sauvegardes hors site des données système indispensables, des données des fichiers-journaux et d'autres informations sensibles.

5.2. Contrôles procéduraux

5.2.1. Rôles de confiance

Les informations relatives aux rôles de confiance seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

Les personnes de confiance sont tous les employés, sous-traitants et consultants à la fois de GPR et de l'OEB, qui ont accès aux opérations de cryptage ou d'authentification pouvant affecter les activités suivantes ou qui contrôlent ces opérations :

- validation des informations figurant dans les demandes de certificats ;
- acceptation, refus et autre traitement des demandes de certificats, demandes de révocation ou de renouvellement, ou informations relatives aux inscriptions ;
- émission ou révocation de certificats, y compris pour le personnel ayant accès à des parties restreintes de la banque d'archivage ;
- traitement des informations ou des demandes des abonnés.

Les personnes de confiance sont entre autres :

- le personnel du service client ;
- le personnel chargé des opérations de cryptage ;
- le personnel de sécurité ;
- le personnel de l'administration des systèmes ;
- le personnel d'ingénierie désigné ;
- les cadres chargés de gérer la fiabilité des infrastructures.

Les personnes souhaitant faire partie du personnel de confiance et obtenir une fonction en tant que tel doivent satisfaire aux exigences de sélection décrites aux paragraphes suivants. L'ensemble du personnel signera une déclaration de sécurité.

5.2.2. Nombre de personnes requis par tâche

Les informations relatives au nombre de personnes requis par tâche seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

Les tâches les plus sensibles au sein de l'AC de l'OEB, par exemple l'accès aux modules de cryptage de l'AC de l'OEB et au matériel de codage associé ainsi que leur gestion, requièrent au moins deux personnes de confiance.

Pour jouer son rôle, l'AE de l'OEB nécessite un(e) employé(e) pour le traitement de la demande de certificat, des demandes de révocation et de renouvellement et des informations relatives aux inscriptions.

5.3. Contrôles du personnel

5.3.1. Curriculum vitae, qualifications, expérience et habilitations

Les informations relatives au curriculum vitae, aux qualifications, à l'expérience et aux habilitations dont dispose le personnel seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

Le personnel souhaitant devenir personnes de confiance doit fournir des justificatifs de son curriculum vitae, de ses qualifications et de son expérience telles qu'elles sont requises pour occuper le poste en question de manière responsable et satisfaisante.

5.3.2. Procédures de vérification du curriculum vitae

Les informations relatives aux procédures de vérification du curriculum vitae seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

Avant de recruter une personne de confiance, l'AC de l'OEB procédera à des vérifications de son curriculum vitae, notamment sur les points suivants :

- confirmation du poste occupé précédemment ;
- vérification des références professionnelles ;
- confirmation du plus haut diplôme obtenu ou du diplôme le plus représentatif ;
- vérification du curriculum vitae.

Un candidat pourra se voir refuser un poste de confiance suite à la vérification de son curriculum vitae, pour les raisons suivantes entre autres :

- fausse déclaration du candidat ;
- références personnelles très largement défavorables ou très peu fiables ;
- certaines condamnations pénales.

5.3.3. Exigences en matière de formation

Le personnel contribuant à l'ICP OEB bénéficiera d'une formation à l'embauche et en plus de la formation en cours d'emploi nécessaire pour s'acquitter correctement de ses responsabilités de manière compétente et satisfaisante.

Les programmes de formation portent notamment sur les aspects suivants :

- concepts de base de l'ICP ;
- responsabilités liées au poste de travail ;
- politiques et procédures opérationnelles et de sécurité ;
- utilisation et fonctionnement du matériel et du logiciel installés ;
- signalement et traitement des incidents et compromissions ;
- procédures de récupération en cas de sinistre et de continuité de l'activité.

5.3.4. Besoins et fréquence des cours de recyclage

Le personnel bénéficiera de cours de recyclage. Une formation périodique sur la sensibilisation à la sécurité sera organisée en continu.

5.3.5. Rotation des postes

Les informations relatives à la rotation des postes seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

5.3.6. Sanctions pour actions abusives

L'AC de l'OEB prendra des mesures disciplinaires à l'encontre de tout membre du personnel qui enfreindra les termes de la PC, de la DPC ou de toute autre politique ou procédure. Ces mesures disciplinaires peuvent aller jusqu'au licenciement, selon la fréquence et la gravité des actions abusives menées par l'employé(e).

5.3.7. Conditions relatives au personnel sous contrat

Les informations relatives aux exigences applicables au personnel sous contrat seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

Dans certains cas, on peut faire appel à des sous-traitants ou consultants indépendants pour assumer des rôles de confiance. Ces sous-traitants et consultants seront soumis aux mêmes exigences liées à la fonction et à la sécurité que celles qui s'appliquent au personnel de l'OEB et de GPR.

5.3.8. Documentation fournie au personnel

L'ensemble du personnel lié à l'AC et à l'AE de l'OEB sera invité à lire la présente DPC, la PC de l'OEB et les politiques de sécurité en vigueur.

6. CONTRÔLES TECHNIQUES DE SÉCURITÉ

L'AC de l'OEB est une sous-AC de l'AC de l'Organisation européenne des brevets (voir point 1.3.1). Ce chapitre décrit les contrôles de sécurité applicables à l'AC de l'OEB et aux clés d'abonnés émises par cette dernière.

6.1. Génération et installation de paires de clés

6.1.1. Génération de paires de clés

Les informations relatives à la génération de paires de clés seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

L'AC de l'OEB et l'AC de l'Organisation européenne des brevets utilisent des modules de cryptage matériels séparés ayant été certifiés comme répondant au niveau de sécurité 3 de la norme FIPS PUB 140-1 pour la génération de signatures de certificats et la vérification de paires de clés.

L'AE de l'OEB génère ses paires de clés en utilisant un module de cryptage certifié au niveau 1 de la norme FIPS 140-1, fourni avec leur logiciel de navigation.

Les paires de clés de l'abonné(e) sont générées dans sa carte à puce. Ainsi, les clés ne quitteront jamais la carte. La carte est elle-même protégée par un code PIN que seul(e) l'abonné(e) connaît.

6.1.2. Remise de la clé privée à l'entité

Les clés privées des abonnés sont stockées sur les cartes à puce des abonnés, puis remises aux abonnés par l'AC de l'OEB.

6.1.3. Remise de la clé publique à l'émetteur du certificat

Les informations relatives à la remise de la clé publique à l'émetteur du certificat seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

Les clés publiques d'abonnés sont générées par l'AC de l'OEB sur les cartes à puce des abonnés. Le système de gestion de cartes (SGC) génère une demande de certificat PKCS#10 pour chaque certificat et la soumet à l'AC de l'OEB pour traitement. Après réception de la réponse de l'AC de l'OEB sur le certificat, PKCS#7, le SGC inscrit le certificat dans la carte à puce de l'abonné(e). Une fois le certificat inscrit dans la carte à puce, une valeur aléatoire est définie pour le code PIN de l'abonné(e). Puis Getronics PinkRoccade (GPR) envoie ce code PIN dans un courrier spécifique à l'abonné(e), selon le point 4.3.

6.1.4. Remise de la clé publique de l'AC de l'OEB et de la LCR aux utilisateurs habilités

La clé publique de l'AC de l'OEB est fournie à des utilisateurs habilités et distribuée sous la forme d'un certificat auto-signé figurant sur le CD. La LCR est publiée par Getronics PinkRoccade sur http://www.megasign.nl/crl/EuropeanPatentOfficeepoline/LatestCRL.crl.

6.1.5. Taille des clés

- Les clés de l'AC de l'OEB ont une longueur de 2048 bits.
- Les clés d'abonnés ont une longueur de 1024 bits.

6.1.6. Génération de paramètres de clé publique

Sans objet.

6.1.7. Contrôle de la qualité des paramètres

Sans objet.

6.1.8. Génération matérielle/logicielle des clés

La génération des clés de l'AC de l'OEB s'effectue sur un module de cryptage répondant au moins à la norme FIPS PUB 140-1, niveau 3.

Les clés de l'abonné(e) sont générées dans sa carte à puce.

6.1.9. Finalités d'utilisation des clés (champ d'utilisation de la clé : X.509 v3)

Pour les certificats ITU-T X.509 Version 3, l'extension KeyUsage des certificats est utilisée conformément du document RFC 2459 : Profil des LCR et certificat d'infrastructure de clé publique Internet X.509.

6.2. Protection des clés privées

6.2.1. Normes du module de cryptage

L'AC de l'OEB utilise un module de cryptage matériel qui a été certifié comme répondant au niveau de sécurité 3 de la norme FIPS PUB 140-1 pour la protection des clés privées de l'AC de l'OEB.

La clé privée de l'abonné(e) est stockée sur une carte à puce qui répond aux exigences de la norme FIPS PUB 140-1.

6.2.2. Contrôle des clés privées par plusieurs personnes (n sur m)

Les informations relatives au contrôle des clés privées par plusieurs personnes (n sur m) seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

L'AC de l'OEB a mis en oeuvre des mécanismes techniques et procéduraux impliquant la participation de plusieurs personnes de confiance pour réaliser des opérations sensibles de cryptage pour l'AC. Au moins trois éléments secrets sur les neuf au total créés et distribués pour le module de cryptage de l'AC de l'OEB sont nécessaires pour activer la clé privée de l'AC de l'OEB, stockée sur ce module.

La clé de l'abonné(e) est stockée sur une carte à puce, laquelle est elle-même protégée par un code PIN dont seul(e) l'abonné(e) a connaissance.

6.2.3. Séquestre des clés privées

Les clés de l'ICP OEB ne sont pas déposées sur un séquestre.

6.2.4. Sauvegarde des clés privées

L'AC de l'OEB créé des copies de sauvegarde de clés privées de l'AC pour procéder à des récupérations de routine et des récupérations en cas de sinistre. Ces clés sont stockées sous forme cryptée dans des modules de cryptage et dispositifs associés de stockage de clés.

L'AC de l'OEB ne réalise pas de copies de sauvegarde de ses clés privées ou de celles des abonnés.

6.2.5. Archivage des clés privées

Les clés de signature privées inactives ou arrivées à expiration ne seront pas archivées. Elles seront détruites conformément au point 6.2.9.

L'AC de l'OEB n'archive pas de copies des clés privées de l'AE de l'OEB ou de celles des abonnés.

6.2.6. Entrée de clés privées dans le module de cryptage de l'AC de l'OEB

Les informations relatives à l'entrée de clés privées dans le module de cryptage de l'AC de l'OEB seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

L'AC de l'OEB génère des paires de clés sur le module matériel dans lequel les clés seront utilisées. En plus, l'AC de l'OEB réalise des copies de ces clés en vue de récupérations de routine et de récupérations en cas de sinistre. Lorsque l'AC de l'OEB est sauvegardée sur un autre module matériel de cryptage, les paires de clés sont transportées entre les modules sous forme cryptée.

6.2.7. Méthode d'activation des clés privées

Les informations relatives à la méthode d'activation des clés privées seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

La clé privée de l'AC de l'Organisation européenne des brevets est activée uniquement pour signer le certificat de l'AC de l'OEB. Ensuite, elle est désactivée et le module de sécurité revient à un stockage sécurisé.

Les clés privées des administrateurs de l'AE de l'OEB sont stockées sur une carte à puce et activées avec un code PIN dont seul l'administrateur a connaissance.

Les paires de clés de l'abonné(e) sont générées dans sa carte à puce. Par conséquent, les clés ne quittent jamais la carte. Les clés privées de l'abonné(e) sont activées par un code PIN dont seul l'abonné(e) a connaissance.

6.2.8. Méthode de désactivation des clés privées

Les clés privées des administrateurs de l'AE de l'OEB sont désactivées lorsqu'ils se déconnectent du système. L'AE de l'OEB doit se déconnecter de la station de travail avant de quitter le domaine de travail.

Les clés privées des abonnés sont désactivées lorsque les cartes à puce sont retirées du lecteur.

6.2.9. Méthode de destruction des clés privées

L'AC de l'OEB désactive sa clé privée en la détruisant irrévocablement.
Les clés d'abonnés ne peuvent pas être détruites, mais les certificats correspondants peuvent être révoqués en évitant un mauvais usage d'une clé privée (voir 4.4.1). La carte de remplacement a de nouvelles clés et de nouveaux certificats.

6.3. Autres aspects de la gestion des paires de clés

6.3.1. Archivage des clés publiques

Le certificat de l'AC de l'OEB, le certificat de l'AE de l'OEB et les certificats des abonnés sont sauvegardés et archivés dans le cadre de la procédure de sauvegarde de routine de l'AC de l'OEB.

6.3.2. Durée d'utilisation des clés publiques et des clés privées

Les clés de l'AC de l'Organisation européenne des brevets ont une durée d'utilisation de 20 ans. Les clés de l'AC de l'OEB ont une durée d'utilisation de 10 ans. Les clés d'abonnés ont une durée d'utilisation de 3 ans.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

Les informations relatives à la génération et à l'installation des données d'activation seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

L'AC de l'OEB utilise des mots de passe qui suivent des règles strictes, pour protéger les clés privées. D'après les instructions de sélection des mots de passe, ceux-ci doivent présenter les caractéristiques suivantes :

- être générés par l'utilisateur,
- être composés d'au moins huit caractères,
- comporter au moins un caractère alphabétique et un caractère numérique,
- avoir au moins un caractère en minuscule,
- ne pas contenir trop souvent le même caractère,
- être différents du nom de profil de l'opérateur,
- ne pas contenir une longue chaîne avec le nom de profil de l'utilisateur.

L'AE de l'OEB utilise une solide authentification pour activer les clés privées : carte à puce et code PIN.

Les abonnés utilisent également une solide authentification pour activer les clés privées : carte à puce et code PIN (voir aussi 6.1.3).

6.4.2. Protection des données d'activation

Il est demandé aux administrateurs de l'AC de l'OEB de sauvegarder leurs éléments secrets et de signer un accord de reconnaissance de leurs responsabilités.

Il est demandé également aux administrateurs de l'AC de l'OEB de stocker les clés privées des administrateurs sous une forme cryptée, sur une carte à puce.

6.4.3. Autres aspects des données d'activation

Sans objet.

6.5. Contrôles de la sécurité informatique

6.5.1. Conditions techniques particulières en matière de sécurité informatique

L'AE et l'AC de l'OEB procèderont à des contrôles de sécurité informatique pour identifier chaque membre du personnel. Une carte à puce et un code PIN sont demandés pour accéder aux installations de l'AE de l'OEB et du SGC. En plus, l'AC de l'OEB limitera l'accès aux données et aux fonctions conformément au rôle et aux droits de l'utilisateur, et enregistrera les accès au moyen d'un fichier-journal en ligne (piste d'audit) où figureront les événements relatifs à la sécurité.

6.5.2. Notation de la sécurité informatique

Sans objet. Cf. 6.1.1.

6.6. Contrôles techniques tout au long du cycle de vie des systèmes

6.6.1. Contrôle de développement des systèmes

L'AC de l'OEB procèdera à des contrôles de développement si nécessaire, afin de s'assurer que matériels et logiciels sont créés, intégrés, testés, configurés, installés, mis en service et maintenus conformément aux objectifs économiques de l'AC de l'OEB. Elle mettra en oeuvre des procédures appropriées de réception et de suivi des marchandises achetées.

6.6.2. Contrôle de la gestion de la sécurité

L'AC de l'OEB mettra en place une organisation pour la gestion de la sécurité. Elle gèrera et contrôlera toutes les activités de sécurité associées au développement et au fonctionnement des systèmes.

6.6.3. Notation en matière de sécurité tout au long du cycle de vie des systèmes

Sans objet.

6.7. Contrôles de la sécurité des réseaux

Les informations relatives aux contrôles de la sécurité des réseaux seront enregistrées à part. Pour des raisons de sécurité, ces informations ne seront pas divulguées au public. L'accès à ces informations peut être octroyé à des parties autorisées qui auront préalablement déposé une demande motivée à la Direction Sécurité et Audit de l'OEB.

L'AC de l'OEB protègera ses réseaux de communication internes de tout accès non autorisé, y compris de l'accès par le biais de connexions à des réseaux externes. Elle emploiera un pare-feu pour protéger chacune de ces connexions. Elle configurera chaque pare-feu selon une politique de sécurité appropriée qui limite la circulation de données entre les réseaux au minimum nécessaire pour réaliser ses objectifs économiques. Au besoin, elle analysera les données entrantes pour éviter les contaminations par virus. Elle effectuera des analyses de routine ainsi que des analyses ciblées du fonctionnement du pare-feu afin de détecter des atteintes à la sécurité avérées ou supposées.

Le lien qui relie l'AE de l'OEB au SGC (système de gestion de cartes) sera crypté et fera appel à l'authentification mutuelle.
Toutes les communications entre la composante d'enregistrement du SGC et l'AC de l'OEB seront signées numériquement. Pour ce faire, le serveur du SGC utilisera :

- un certificat unique d'AE de l'OEB et la clé privée correspondante ;
- le certificat public d'AC de l'OEB.

Toutes les opérations de demande seront signées numériquement à l'aide du certificat d'AE de l'OEB. Cela permettra à l'AC de l'OEB de les valider comme provenant d'une AE de l'OEB agréée uniquement.

Toutes les réponses venant de l'AC de l'OEB et adressées à l'AE de l'OEB seront signées à l'aide de la clé privée d'AC de l'OEB. Cela permettra au SGS de les valider en tant que réponses officielles en provenant de l'AC de l'OEB.

6.8. Contrôles techniques du module de cryptage

Voir point 6.2.1.

7. PROFILS DES CERTIFICATS ET DES LCR

Conformément à la définition figurant à l'Annexe F du PCT, les certificats octroyés aux abonnés sont des certificats simplifiés.

7.1. Profil des certificats

Les certificats d'abonnés doivent être conformes au document RFC 2459.
Le profil des certificats comprend les valeurs ou contraintes de valeurs suivantes :

Version	
Serial number	Voir DPC § 7.1.1.
	Valeur unique pour chaque ND d'utilisateur (clé publique de type MD5) SHA1 RSA
Signature algorithm Issuer DN	
Valid from	Voir point 7.1.4.
Valid to	Date d'émission (TUC, Temps Universel Coordonné). Codée selon RFC 2459.
	Date d'émission + 3 ans (TUC, codée selon RFC 2459).
Subject DN	P : pays de l'abonné(e)
	O : entreprise de l'abonné(e)
	NC : <première lettre du prénom> + <.>+ <-> +<première lettre du deuxième prénom> + <espace> + <nom de famille> + <espace> + <ID OEB>
Subject public key	Codée selon RFC 2459 en utilisant des algorithmes spécifiés au point 7.1.3 de la DPC et longueur de clé spécifiée au point 6.1.5 de la DPC. Générée et codée selon RFC 2459.
Signature	

Tableau 2 -Profil des certificats

7.1.1. Numéro(s) de version

Les certificats d'AC de l'OEB et d'abonnés sont des certificats X.509 version 3.

7.1.2. Extensions des certificats

L'AC de l'OEB met en oeuvre une extension de la politique de certificat unique et non critique, conformément à RFC 2459, avec des qualificatifs de politique sur chaque certificat .

7.1.3. Identificateurs d'objets algorithmiques

Les certificats d'abonnés sont signés par SHA-1 par le cryptage RSA (1 2 840 113549 1 1 5) conformément à RFC 2459.

7.1.4. Formes des noms

Cf. 3.1.1

7.1.5. Contraintes concernant les noms

Sans objet.

7.1.6. Identificateur d'objets de la politique de certification

Cf. 1.2

7.1.7. Extension concernant les contraintes afférentes à l'utilisation de la politique

Sans objet.

7.1.8. Syntaxe et sémantique des qualificatifs de politique

Sans objet.

7.1.9. Sémantique de traitement pour les extensions critiques de la politique de certification

Sans objet.

7.2. Profil des LCR

Le profil des LCR comprend les champs et contenus de base, spécifiés dans le tableau ciaprès :

Version	
	Voir DPC, paragraphe 7.2.1. Md5RSA ou md2RSA
Signature algorithm Issuer	
Effective date	Date d'émission de la LCR. Émetteur de la LCR. Le nom d'émetteur est conforme au point 7.1.4.
Next update Revoked	Date à laquelle la prochaine LCR sera émise. La prochaine mise à jour sera réalisée trois mois après la date d'entrée en vigueur de la LCR de l'AC de l'Organisation européenne des brevets. La fréquence d'émission des LCR pour les certificats d'abonnés est conforme au point 4.4.9 de la DPC.
certificates	Listage des certificats révoqués, comprenant le numéro de série du certificat révoqué et la date de révocation. Générée et codée selon RFC 2459.
Signature	

Tableau 3 – Champs de base de profil

7.2.1. Numéro(s) de version

L'AC de l'OEB émet la version 1 des LCT X.509.

7.2.2. Extensions des LCR et des entrées des LCR

Sans objet.

8. GESTION DES SPÉCIFICATIONS

8.1. Procédures de modification des spécifications

Les modifications se présenteront sous la forme d'une mise à jour ou d'un document contenant une version modifiée de la DPC.

8.2. Politiques de publication et de notification

Cf. détails au point 1.4.

8.3. Procédures d'approbation de la PC

La Direction Sécurité et Audit de l'OEB sera chargée du suivi du document relatif à la PC.