Politique de certification de l'Office européen des brevets

Version 2.1

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

Politique de certification de l'Office européen des brevets

Date de révision : 1er janvier 2011

Publiée 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 politique de certification (PC) sont à adresser au département de soutien aux utilisateurs eBusiness de l'OEB, Office européen des brevets, Bayerstrasse 35, 80335, Munich, Allemagne, courriel: support@epo.org

Droits d'auteur

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.

Dénégation de responsabilité
Le présent document décrit certains services à portée limitée et mis à la disposition d'un groupe spécifique d'utilisateurs. Il existe certaines limitations de responsabilité, lesquelles sont décrites dans le présent document.

L'OEB ne garantit pas que les dispositions légales du présent document soient identiques mot pour mot au texte officiel adopté. Seul fait foi le texte de la Convention sur le brevet européen (CBE) et des dispositions en découlant 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 que publiées dans la version imprimée 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 à tout moment et sans notification préalable, 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
1.0	15 avril 2005	Parution du document
1.1	14 juillet 2005	Changements au point 4.4.4
2.0	1er mars 2008	Mise à jour du documents suite à la révision de certains instruments juridiques en liaison avec l'entrée en vigueur de la CBE 2000
2.1	16 mai 2011	Mise à jour du documents suite à la révision de certains instruments juridiques et changements organisationnels

TABLE DES MATIÈRES

GLOSSAIRE

Abonné	[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 recourt à des serveurs ou à des systèmes informatiques propres, 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 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 qui correspond à une clé privée sous le contrôle exclusif du sujet ; • nommer ou identifier d'une autre façon le sujet ; • identifier l'AC qui l'émet ; • indiquer sa période de validité ; • contenir un numéro d'ordre du certificat ; • inclure l'adresse de courrier électronique des entités finales ; • être signé numériquement par l'AC qui l'émet.

Certificat simplifié	[Annexe F] Certificat numérique décerné au demandeur, par exemple dans le cadre de l'enregistrement du client de dépôt en ligne, ou obtenu auprès d'une autorité de certification, 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 de 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 de la paire de clés publiqueprivée 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 cryptographiques, textes en clair sensibles et 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 peut et 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 cryptographique	[Annexe F] Ensemble de matériels, logiciels et microprogrammes, ou combinaison de ces éléments servant à mettre en application une logique ou des fonctions cryptographiques, dont les algorithmes de chiffrement, et contenu dans le périmètre cryptographique du module.
Nom distinctif	[Annexe F] Nom particulier à chaque titulaire de certificat ou abonné. Chaque entité du domaine ICP doit avoir un nom distinctif ou ND qui soit facilement reconnaissable et qui lui soit spécifique dans le champ d'identification du sujet 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 l'applicabilité d'un certificat à un groupe ou classe d'application ayant des impératifs de sécurité communs. Ainsi, la politique de certification peut indiquer qu'un type de certificat est applicable à l'authentification de 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 1 octobre 2005
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 P
CT	Traité de coopération en matière de brevets

Références

Ce document relatif à la politique de certification de l'OEB fait référence aux sources suivantes :

[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 1 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 l’acte portant révision de la Convention sur le brevet européen du 29 novembre 2000.

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

1.1. Généralités

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

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.

Ce document sur la politique de certification de l'OEB (PC) décrit les conditions relatives à l'émission, à l'utilisation et à la révocation de certificats d'abonnés dans l'ICP OEB.
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.

S'il est satisfait à certaines conditions et exigences, 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 les communications sécurisées avec certaines autres organisations et institutions nationales et internationales et les institutions qui ont pour mission de traiter des demandes de brevets.

L'ICP OEB dans les grandes lignes
L'ICP OEB comprend :

- une autorité de certification (l'AC de l'OEB), y compris une banque d'archivage de révocation de certificats ;
- une autorité d'enregistrement (l'AE de l'OEB) ;
- les abonnés.

Les abonnés sont des utilisateurs habilités tels que décrits aux point 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. point 1.1.1ci-dessus).

Les certificats d'abonnés sont émis à la discrétion de l'OEB, uniquement à l'intention de 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, tel qu'il est précisé dans la PC.
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 brevet 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 sources sont repris dans les 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 appelé "Politique 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. Autorités de certification

L'AC agissant au sein de l'ICP OEB est l'AC de l'Office européen des brevets. 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 OEB subordonnées.

1.3.2. 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.

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 office récepteur au titre du PCT (cf. art. 10 PCT), et qu'en tant qu'office récepteur, elle 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 publie 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 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 parties utilisatrices. À cette fin, l'OEB peut fixer des conditions que devra remplir l'organisation intergouvernementale concernée.

1.3.5. Champ d'application

La carte à puce de l'OEB comprend deux types de certificats d'abonnés : les certificats d'authentification, avec lesquels les abonnés peuvent s'authentifier eux-mêmes vis-à-vis d'un environnement de réseau et les certificats non répudiables, avec lesquels les abonnés peuvent 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 politique de certification

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

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 est à adresser au département de soutien aux utilisateurs eBusiness de l’OEB.
l'OEB, Office européen des brevets, Bayerstrasse 35, 80335, Munich, Allemagne,

courriel : support@epo.org

1.4.3. Organe qui détermine la conformité de la Déclaration des pratiques de certification par rapport à la politique

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

1.5. Entrée en vigueur et dispositions transitoires

La PC entre en vigueur à la date indiquée sur la page de garde. La date de diffusion mentionnée dans la PC est la date à laquelle la version actuelle de la PC 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 à ce point 1.5 que les dispositions de la PC s'appliquent à l'ICP OEB rétroactivement à partir de la date d'entrée en vigueur.

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

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

Les conditions stipulées ci-dessus s’appliqueront également à tout autre document lié à la PC (et à ses versions ultérieures), notamment mais pas uniquement à la DPC, aux accords d’abonnement et aux accords passés avec les parties utilisatrices.

2. DISPOSITIONS GÉNÉRALES

2.1. Obligations

2.1.1. Obligations incombant à l'AC de l'OEB

L'AC de l'OEB s'acquitte 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 ;
- donner accès à la PC aux utilisateurs habilités de l'ICP OEB ;
- émettre des certificats d'abonnés à l'intention des abonnés, sur réception d'une demande valable 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 ;
- poster les certificats d'abonnés émis dans la banque d'archivage (N.B. : l'accès à cette banque est limité aux parties habilitées) ;
- générer des paires de clés pour les abonnés sur la carte à puce, faire suivre pour certification les demandes de certificats des abonnés à l'AC de l'OEB, retourner le certificat d'abonné sur la carte à puce et envoyer 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.

2.1.2. Obligations incombant à l'AE de l'OEB

L'AE de l'OEB s'acquitte 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 incombent notamment à l'AE de l'OEB :

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

2.1.3. Obligations incombant à l'abonné(e)

L'abonné(e) s'acquitte 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 d'abonné(e) ne soit connu que de l'abonné(e) ;
- envoyer immédiatement une demande de révocation à l'AE de l'OEB en cas de compromission avérée ou de compromission possible des clés privées, du PIN ou de la carte à puce, ou de tout changement des informations fournies dans la demande de certificat.

2.1.4. Obligations incombant à la partie utilisatrice

La partie utilisatrice s'acquitte 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.

2.2. Responsabilité

Etendue de la responsabilité de l'OEB

2.2.1.1.

Par sa mise en oeuvre de l'ICP OEB, notamment en signant un certificat indiquant l'utilisation de la PC, l'OEB, vis-à-vis des parties (cf. 1.3.4) qui accordent leur confiance raisonnable aux informations véhiculées par les certificats, garantit seulement que ses services de certification et d'archivage dans la banque des certificats ainsi que l'émission et la révocation des certificats et l'émission de LCR, sont conformes à la PC. L'OEB est uniquement tenu de fournir des efforts raisonnables pour veiller à ce que les abonnés et les parties utilisatrices s'en tiennent aux stipulations de 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 n'est pas responsable des conséquences qui pourraient découler d'un usage 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 n'est pas responsable de l'utilisation des certificats émis en vertu de la PC pour la communication entre les utilisateurs habilités et les autres services de la propriété industrielle ou tout autre tiers (cf. 1.1.3 et / 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 affectée en période de maintenance du système, en raison de réparations ou de 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 ou 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 la responsabilité 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 est le droit allemand.

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

Les accords d'abonnement et les accords passés avec les parties utilisatrices reflètent 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 figurant aux points 2.1.3 et 2.1.4.

2.3. Responsabilité financière

2.3.1. Exonération 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 exigent des abonnés et des parties utilisatrices qu'ils exonèrent l'OEB de toute conséquence découlant du non respect des conditions stipulées dans ces accords ou autre part dans les documents relatifs à l'ICP OEB.

2.3.2. Relations fiduciaires

En aucun cas l'émission de certificats n'implique que l'AC de l'OEB agit 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 est 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 sont applicables dans la mesure où la CBE ou la PC le prévoit. À titre subsidiaire, le droit allemand s’applique, à l'exclusion du recours au droit allemand des litiges.

Cette disposition relative au droit applicable s'applique 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'exclut 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 doit être 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

Au cas où une ou plusieurs dispositions de la PC, pour quelque raison que ce soit, se révèleraient être non valables, illicites ou inexécutables en droit, leur inexécutabilité n'affecte pas les autres dispositions ; la PC est 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, 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 devront avoir lieu sous forme électronique ou sur papier.

2.4.3. Procédures de résolution des litiges

Si un litige surgit 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'engagent 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 est 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 déroule à Munich.

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

Lorsque, 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 priment sur les procédures de résolution susmentionnées. Le point 2.4.1.2 s'applique.

Les accords d'abonnement et les accords passés avec les parties utilisatrices doivent contenir 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, sont 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 de révocation ou d'information relative au 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 publie les informations suivantes dans la banque d'archivage (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 de 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 publie les informations répertoriées au point 2.6.1 ci-dessus aussitôt qu'elles deviennent disponibles.

2.6.3. Contrôles d'accès

L'AC de l'OEB contrôle 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 doit avoir une banque d'archivage destinée à la publication des certificats d'abonnés et des LCR.

2.7. Audit de conformité

2.7.1. Fréquence des audits de conformité

L'OEB procède, 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 référencées 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

L'auditeur externe effectue un audit indépendant chaque année. L'auditeur doit être au service d'une société spécialisée compétente qui respecte les normes et codes de conduite nationaux et internationaux pertinents.

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

L'audit et le rapport d'audit sont 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 détermine la conformité des systèmes et procédures de l'ICP OEB eu égard à la PC et à la DPC de l'OEB. Il détermine 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 prend les mesures qu'il juge nécessaires et appropriées pour remédier aux carences décelées par l'audit.

2.7.6. Communication des résultats

L'OEB est tenu de gérer l'ICP OEB en conformité avec les conditions et contrôles applicables. 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 traite le contenu des demandes de certificat ou des demandes de révocation, que celles-ci aboutissent ou non, comme confidentiel vis-à-vis de l'AC de l'OEB et l'abonné/demandeur, sauf dans les circonstances visées aux points 2.8.2 à 2.8.7.
- L'OEB traite 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, sur demande, à l'auditeur désigné.

2.8.2. Types d'informations non soumises à confidentialité

L'OEB ne traite 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 certificats est divulgué librement aux parties utilisatrices.

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

L'OEB peut 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 est sans préjudice des privilèges et immunités de l'OEB.

2.8.5. Divulgation dans le cadre d'une instruction civile

L'OEB peut divulguer des informations confidentielles relatives à un(e) abonné(e) 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 est sans préjudice des privilèges et immunités de l'OEB.

2.8.6. Divulgation à la demande du titulaire

L'OEB s'engage 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 d'abonnés et à la PC appartiennent et demeurent la propriété de l'OEB.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Enregistrement initial

3.1.1. Types de noms

L'AC de l'OEB s'identifie et identifie les abonnés au moyen de noms distinctifs (ND) utilisant les attributs définis dans la norme ITU-T X.501 relative aux noms distinctifs.

3.1.2. Caractère significatif des noms

L'AC de l'OEB veille à ce que les attributs identifient de façon unique chaque abonné et aient des valeurs significatives.

3.1.3. Règles d'interprétation des différents types de noms

Sans objet.

3.1.4. Unicité des noms

L'AC de l'OEB attribue les noms conformément aux points 3.1.1 et 3.1.2, de sorte à éviter toute ambiguïté. L'AC de l'OEB rejette 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 résout les litiges pouvant découler de l'attribution des noms en faisant des efforts raisonnables pour contacter le demandeur du certificat et convenir, par exemple, d'une modification du NC afin de lever l'ambiguïté dont est entaché le ND.

3.1.6. Reconnaissance, authentification et rôle des marques

L'AC de l'OEB n'est 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 spécifie dans sa DPC des méthodes d’authentification de l’identité d’une organisation.

3.1.9. Authentification de l'identité individuelle

Avant l'émission d'un certificat à l'intention d'un demandeur de certificat, l'AE de l'OEB authentifie l'identité du demandeur conformément aux procédures d'enregistrement. L'AE de l'OEB prend toutes les mesures raisonnables pour vérifier l'identité du demandeur de certificat.

3.2. Renouvellement de clé

Si leur certificat est toujours valable, les abonnés s'identifient au moyen de leur carte à puce. Si le certificat est périmé, la marche à suivre pour le renouveler est la même que pour l'enregistrement initial.

3.3. Renouvellement de clé après révocation

La procédure d'identification et d'authentification pour le renouvellement de clé après révocation est la même que celle pour l'enregistrement initial.

3.4. Demande de révocation

L'AC de l'OEB, dans sa DPC, spécifie de façon précise les procédures et mesures d'identification et d'authentification requises pour authentifier les demandes de révocation.

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 présente politique de certification, ou présenter une clé publique et prouver qu'ils possèdent la clé privée correspondante ainsi que la preuve que cette dernière a été générée et protégée conformément à la présente Politique ;
- fournir les données personnelles devant être certifiées et/ou accompagner la demande de certificat.

L'AC de l'OEB et l'AE de l'OEB font preuve de diligence raisonnable dans l'acceptation et le traitement des demandes de certificat. L'AC de l'OEB dresse 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 signifie 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 soussystèmes.

Les cinq fonctions sont :
1 génération des clés ;
2 stockage sur un porte-clés ;
3 création de certificats ;
4 génération des codes PIN ;
5 distribution et livraison.

4.3. Acceptation du certificat

Les abonnés accusent réception de leur carte à puce. Cet accusé de réception est réputé valoir acceptation du certificat.

4.4. Révocation du certificat

Un certificat est révoqué lorsqu'il perd sa validité ou sa fiabilité.

4.4.1. Circonstances entourant la révocation

Les abonnés peuvent solliciter la révocation de leur certificat. Les circonstances cidessous peuvent constituer des motifs de révocation d'un certificat (liste non limitative) :

- vol, perte, divulgation, modification ou tout autre compromission ou compromission supposée de la clé privée, du code PIN ou de la carte à puce de l'abonné(e) ;
- abus délibéré des clés et/ou des certificats de la part de l'abonné(e) ,
- manquement important aux conditions relatives au fonctionnement stipulées dans la PC ou dans d'autres documents pertinents (p.ex. accords d'abonnement) ;
- si les informations du certificat se révèlent inexactes ou le deviennent ;

- émission impropre (p.ex. informations du certificat incorrectes) ou erronée du certificat ;
- si l'OEB refuse de donner à l'abonné(e) les droits d'accès à un produit ou à un service.

4.4.2. Qui peut demander la révocation ?

Les entités suivantes peuvent demander la révocation d'un certificat d'abonné(e) :

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

4.4.3. Procédure de demande de révocation

Dans sa DPC, l'OEB spécifie ou fait référence à la procédure à suivre pour demander la révocation.

4.4.4. Délai de traitement des demandes de révocation

L'OEB spécifie, dans sa DPC, le délai de traitement des demandes de révocation.

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 publie sa LCR toutes les 24 heures, même si la LCR n'a subi aucun changement.
- Chaque LCR indique quand aura lieu la prochaine publication de la LCR, conformément à ITU-T X.509. Une nouvelle LCR peut être publiée avant la date indiquée.

4.4.10. Exigences relatives aux vérifications de la LCR

Cf. obligations incombant à la partie utilisatrice.

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. Devoir de vérification pour d'autres formes de publicité concernant la révocation

Sans objet.

4.4.15. Obligations particulières concernant la compromission des clés

Sans objet.

4.5. Procédures d'audit en matière de sécurité

Dans sa DPC, l'AC de l'OEB spécifie la manière dont les événements habituels ou exceptionnels seront enregistrés, dont les fichiers-journaux -tant sur papier que sous forme électronique -seront tenus, et dont les enquêtes périodiques et ad hoc auront lieu afin de vérifier de manière continue la sécurité du site, de ses utilisateurs (personnel de gestion ou d'exécution employé ou utilisé par l'AC de l'OEB) et de son fonctionnement. Les conditions stipulées ci-dessous représentent le minimum requis.

4.5.1. T**ypes d'événements enregistrés**

Le répertoire des événements inclut les détails pertinents, les utilisateurs/employés de l'AC de l'OEB impliqués, la date et l'heure des événements et, le cas échéant, le statut de l'événement (réussite ou échec). La DPC spécifie de façon complète les types d'événement enregistrés.

4.5.2. Fréquence de traitement des fichiers-journaux

Les fichiers-journaux en ligne sont 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 sont conservés pendant sept ans au moins.

4.5.4. Protection des fichiers-journaux d'audit

Les fichiers-journaux en ligne sont protégés contre les modifications, p.ex. en faisant en sorte que les supports soient protégés en écriture.

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.
- Les fichiers-journaux pourront être examinés pendant leur période de conservation.

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

Des fichiers-journaux sont 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 la vulnérabilité

Cf. 2.7

4.6. Archivage

Dans sa DPC, l'AC de l'OEB spécifie ou référence les mesures prises pour générer et assurer la maintenance de ses archives. Les conditions stipulées ci-dessous représentent le minimum requis.

4.6.1. Types d'événements archivés

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

- les demandes de certificat et les messages y afférents ;
- la correspondance et les contrats avec les autres parties ;
- les informations relatives au renouvellement de clés par l'AC de l'OEB, y compris les identifiants de clés et les certificats de l'AC ;
- les demandes de révocation et les messages échangés avec l'auteur de la demande et/ou l'abonné(e) ;
- les fichiers-journaux d'audit, y compris les rapports des audits annuels de l'AC de l'OEB.

4.6.2. Période de conservation des archives

- L'AC de l'OEB veille à ce que les archives soient conservées pendant sept ans au moins.
- Si les supports d'origine sont incapables de conserver les données jusqu'au terme de la période requise, l'AC de l'OEB met en place des procédures en vue du transfert régulier des données sur de nouveaux supports.
- L'AC de l'OEB entretient 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 veille 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 sont regroupées au niveau interne.

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

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

4.7. Changement de clé

- L'AC de l'OEB génère une nouvelle paire de clés pour la signature et la vérification des certificats au moyen d'un système de scission/partage de clé, et génère un certificat d'AC de l'OEB au moins trois mois avant l'expiration de l'ancienne clé d'AC de l'OEB.
- Le changement d'une paire de clés d'AC de l'OEB est entouré des mêmes mesures de sécurité que la création de la paire de clés d’origine.
- L'AC de l'OEB veille à ce que le changement de clé n'occasionne qu'un minimum de dérangement aux entités subordonnées de la chaîne de confiance de l'AC de l’OEB.

4.8. Récupération en cas de compromission et de sinistre

L’OEB dresse un plan de continuité de services afin de garantir que les activités puissent se poursuivre sans compromission en cas de sinistre. Dans sa DPC, l’OEB inclut le plan de continuité de service ou y fait référence.

En cas de compromission avérée ou supposée de la clé privée de l'AC de l'OEB, l'OEB avertit 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 sont aussi.

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

L'AC de l'OEB avertit 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 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

Dans sa DPC, l'AC de l'OEB spécifie les contrôles physiques nécessaires pour satisfaire aux exigences de la PC, les contrôles physiques nécessaires pour remplir les autres exigences éventuelles, et les répartitions de responsabilités auxquelles il est procédé en vue de faciliter les contrôles physiques.

5.1.1. Emplacement et construction des sites

L'AC de l'OEB prend 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 les intrusions soient construits au moins en briques, en tuiles ou en béton aggloméré. Les murs doivent se raccorder 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.

5.1.2. Accès physique

L'AC de l'OEB limite l'accès physique à son site au moyen des serrures et des dispositifs appropriés de contrôle d'entrée et de détection des intrus.

5.1.3. Électricité et climatisation

- L'AC de l'OEB prend les mesures raisonnables qui s'imposent pour protéger le site de manière adéquate contre les problèmes électriques afin de réduire les risques de dysfonctionnement des équipements essentiels causés par des coupures de courant, des pointes ou des surtensions.
- L'AC de l'OEB prend les mesures raisonnables qui s'imposent pour climatiser suffisamment son site afin de réduire les risques de dysfonctionnement des équipements essentiels suite à une surchauffe.

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 activités essentielles.

5.1.5. Prévention et protection contre l'incendie

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

L'AC de l'OEB stocke les supports mobiles en lieu sûr.

5.1.7. Élimination des déchets

L'AC de l'OEB veille à ce que les documents papier ou les supports contenant des informations confidentielles soient éliminés de façon sûre.

5.1.8. Sauvegarde hors site

Il est procédé régulièrement à des sauvegardes des données systèmes essentielles, des données contenues dans les fichiers-journaux d'audit ainsi que des autres informations sensibles.

5.2. Contrôles procéduraux

Dans sa DPC, l'AC de l'OEB spécifie les contrôles procéduraux nécessaires pour satisfaire aux exigences de la PC, les contrôles procéduraux nécessaires pour remplir les autres exigences éventuelles, et les répartitions de responsabilités auxquelles il est procédé en vue de faciliter les contrôles procéduraux.

5.2.1. Rôles de confiance

Dans sa DPC, l'AC de l'OEB spécifie les rôles de confiance au sein de l'environnement sécurisé.

5.2.2. Nombre de personnes requis par tâche

Dans sa DPC, l'AC de l'OEB spécifie le nombre de personnes requis par tâche.

5.3. Contrôles du personnel

Dans sa DPC, l'AC de l'OEB spécifie les contrôles du personnel nécessaires pour satisfaire aux exigences de la PC, les contrôles du personnel nécessaires pour remplir les autres exigences éventuelles, et les répartitions de responsabilités auxquelles il est procédé en vue de faciliter les contrôles du personnel.

5.3.1. Curriculum vitae, qualifications, expérience et habilitations

L'AC de l'OEB emploie ou continue d'employer du personnel conformément au curriculum vitae, aux qualifications, à l'expérience et aux habilitations qui sont spécifiés ou référencés dans sa DPC.

5.3.2. Procédures de vérification du curriculum vitae

L'AC de l'OEB exige que tout le personnel apporte la preuve de son identité et de ses qualifications en produisant les justificatifs appropriés.

5.3.3. Exigences en matière de formation

L'AC de l'OEB veille à ce que tout le personnel en activité ait la formation adéquate.

5.3.4. Besoins et fréquence des cours de recyclage

L'AC de l'OEB veille à ce que tout le personnel en activité puisse se recycler de façon adéquate.

5.3.5. Rotation des postes

L’AC de l’OEB spécifie ou fait référence à la rotation des postes dans sa DPC.

5.3.6. Sanctions pour actions abusives

L'AC de l'OEB applique des sanctions pour toute action abusive, les sanctions pouvant aller jusqu'au licenciement immédiat en cas d'atteinte aux dispositions de la PC, de sa DPC ou d'autres politiques et procédures.

5.3.7. Conditions relatives au personnel sous contrat

L'AC de l'OEB prend des mesures appropriées pour que les contractants ou consultants indépendants impliqués dans le fonctionnement de l'ICP OEB fournissent leurs services avec le soin et la diligence voulus et qu'ils utilisent pour ce faire du personnel suffisamment qualifié.

5.3.8. Documentation fournie au personnel

L'AC de l'OEB veille à ce que tout le personnel effectuant des opérations relatives à l'AC de l’OEB reçoive les guides, les modes d'emploi et/ou les spécifications techniques nécessaires.

6. CONTRÔLES TECHNIQUES DE SÉCURITÉ

6.1. Génération et installation de paires de clés

6.1.1. Génération de paires de clés

- L'AC de l'OEB utilise un ou plusieurs modules de cryptage matériels séparés ayant été certifiés comme répondant à la norme FIPS PUB 140-1 jusqu'au niveau de sécurité 3 au moins pour la génération de signatures de certificats et la vérification de paires de clés.
- Les paires de clés d'abonnés sont générées sur les cartes par l'AC de l'OEB.

6.1.2. Remise de la clé privée à l'entité

Les clés privées sont générées, stockées sur des cartes à puce puis remises à l'abonné(e) par l'AC de l'OEB.

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

Les clés publiques sont fournies à l'AC de l'OEB conformément à une demande de certificat PKCS#10.

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 mise à la disposition des utilisateurs habilités sur demande, via un moyen de communication durable tel que l'internet. Le point de distribution de la LCR est spécifié dans la DPC.

6.1.5. Taille des clés

Les clés de l'AC de l'OEB auront une longueur minimale de 2048 bits. Les clés d'abonnés auront une longueur minimale de 1024 bits.

6.1.6. Génération de paramètres de clé publique

Sans objet.

6.1.7. Contrôle de qualité des paramètres

Sans objet.

6.1.8. Génération matérielle/logicielle des clés

La génération de la clé 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.

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

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

6.2. Protection de la clé privée

6.2.1.1. Normes du module de cryptage

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

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

L'accès à la clé privée de l'AC de l’OEB est partagé entre plusieurs personnes. Au moins N de M personnes doivent être réunies pour donner l'accès aux clés. Dans sa DPC, l'AC de l’OEB spécifie ou référence précisément les contrôles mis en oeuvre.

6.2.3. Séquestre des clés privées

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

6.2.4. Sauvegarde de la clé privée

L'AC de l’OEB veille à ce que le système de scission/partage des clés permette de recréer la clé privée en cas de sinistre.

6.2.5. Archivage de la clé privée

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

6.2.6. Entrée de la clé privée dans le module de cryptage

L'AC de l’OEB veille à ce que le système de scission/partage des clés permette d'entrer en toute sûreté la clé privée dans le module de cryptage.

6.2.7. Méthode d'activation des clés privées

L'AC de l’OEB veille à ce que le système de scission/partage des clés permette d'activer en toute sûreté et efficacement la clé privée.

6.2.8. Méthode d'inactivation des clés privées

L’AC de l’OEB s’assure que les clés de l’AC, de l’AE et des abonnés sont correctement inactivées.

6.2.9. Méthode de destruction des clés privées

L'AC de l’OEB veille à ce que les clés privées désactivées de l'AC de l’OEB soient irrévocablement détruites.

6.3. Autres aspects de la gestion des paires de clés

6.3.1. Archivage de la clé publique

L'AC de l’OEB garde des copies des clés publiques de tous les abonnés, à des fins d'archivage.

6.3.2. Durée d'utilisation des clés publiques et 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

Selon les besoins, l'AC de l’OEB utilise des données d'activation telles que des mots de passe ou des codes PIN afin de contrôler l'accès aux ordinateurs, aux équipement et aux zones physiques de son site.

6.4.2. Protection des données d'activation

L'AC de l’OEB définit et applique une politique appropriée à son personnel (managers et opérateurs employés ou utilisés par l'AC de l’OEB) afin de protéger les mots de passe ou PIN attribués à ce personnel.

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'AC de l’OEB a recours à des contrôles de sécurité informatique lorsque cela est approprié, afin d'identifier les utilisateurs, de les authentifier au moyen d'un mot de passe ou d'un code PIN, de limiter l'accès aux données et aux fonctionnalités en fonction du rôle et des privilèges des utilisateurs. Elle enregistre également, via un journal en ligne (piste d'audit), les événements significatifs du point de vue de 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 du développement des systèmes

L'AC de l’OEB contrôle le développement lorsque cela est approprié, afin de s'assurer que matériels et logiciels sont créés, intégrés, testés, configurés, installés, commandés et maintenus conformément aux objectifs économiques de l'AC de l’OEB. Elle met en oeuvre 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 met en place un dispositif de sécurité. Elle gère et contrôle 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. Contrôle de la sécurité des réseaux

L'AC de l’OEB protège ses réseaux de communication internes de tout accès non autorisé, y compris l'accès par le biais de connexions à des réseaux externes. Elle emploie un pare-feu lors de telles connexions. Elle configure chaque pare-feu au moyen d'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 analyse les données entrantes pour éviter les contamination par virus. Elle effectue des analyses de routine ainsi que des analyses ciblées du fonctionnement du pare-feu afin de détecter les atteintes à la sécurité qui se sont produites ou qui ont été susceptibles de se produire.

6.8. Contrôle technique du module de cryptage

Sans objet.

7. PROFILS DES CERTIFICATS ET DES LCR

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

7.1. Profil des certificats

Les certificats d'abonnés doivent être conforme à RFC 2459.

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 certificat unique et non critique, dans le cadre de la politique de certification, conformément à RFC 2459 avec des qualificatifs de politique sur chaque certificat.

7.1.3. Identificateurs d'objets algorithmiques

Identificateurs tels que définis par 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'objet 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

7.2.1. Numéro(s) de version

Les LCR publiées dans le cadre de cette politique seront établies conformément à ITU-T x.509 et RFC 2459.

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 doivent se présenter sous la forme d'une mise à jour ou d'un document contenant une version modifiée de la PC.

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 est chargée du suivi du document relatif à la PC.