



Autorité de Certification AC @vocats Classe 3Plus

POLITIQUE DE CERTIFICATION

Date : 10/06/2005

Version : 0.1

OID : 1.2.250.1.148.1.1

Version	Date	Rédigée par	Validée par
0.1	10/06/2005	François Renou	

AC @vocats Classe 3Plus

Politique de Certification

Sommaire :

1	PREAMBULE	6
2	PRESENTATION GENERALE DE LA PC	8
2.1	Liste des acronymes utilisés	8
2.2	Définitions des termes utilisés dans la PC	9
2.3	Type d'applications concernées par la PC	11
2.4	Type de certificats délivrés par l'AC AC @vocats Classe 3Plus	11
2.5	Modification de la PC	12
2.6	Identification de la PC - OID	12
2.7	Coordonnées des entités responsables de la présente PC	12
2.7.1	Organisme responsable	12
2.7.2	Personne physique responsable	12
2.7.3	Personne déterminant la conformité de la DPC à la PC	12
3	DISPOSITIONS DE PORTEE GENERALE	13
3.1	Contrôle de conformité à la PC	13
3.1.1	Objet des contrôles de conformité	13
3.1.2	Indépendance et qualifications du contrôleur	13
3.1.3	Fréquence du contrôle de conformité	13
3.1.4	Périmètre du contrôle de conformité	13
3.1.5	Communication des résultats	13
3.1.6	Actions entreprises en cas de non-conformité	13
3.2	Respect et interprétation des dispositions juridiques	14
3.2.1	Droit applicable	14
3.2.2	Séquestre	14
3.2.3	Arbitrage des litiges	14
3.3	Obligations	14
3.3.1	Obligations de l'AC	14
3.3.2	Obligations de l'AE	14
3.3.3	Obligations communes à toutes les composantes de l'ICP	15
3.3.4	Obligations relatives à la gestion des Certificats	15
3.3.5	Obligations relatives à la gestion des supports, des codes PIN et des codes de révocation	16
3.3.6	Obligations relatives à l'identification	16
3.3.7	Obligations relatives à la publication	16
3.3.8	Obligations relatives à la journalisation	17
3.3.9	Obligations relatives à l'archivage	17
3.3.10	Obligations relatives au séquestre	17
3.3.11	Obligations du Mandataire de Certification.	17
3.4	Obligations du Porteur	18
3.5	Obligations des applications utilisatrices et des utilisateurs de Certificats	18
3.6	Responsabilités	18
3.6.1	Responsabilité de l'AC	18
3.6.2	Responsabilité de l'AE	19
3.7	Politique de confidentialité de l'AC	19
3.7.1	Types d'informations considérées comme confidentielles	19
3.7.2	Divulgaration des causes de révocation	19
3.7.3	Remise sur demande du propriétaire	20
3.7.4	Délivrance aux autorités habilitées	20
3.7.5	Droits de propriété intellectuelle	20
4	IDENTIFICATION ET AUTHENTIFICATION	21

AC @vocats Classe 3Plus

Politique de Certification

4.1	Enregistrement initial d'un Porteur	21
4.1.1	Conventions de noms	21
4.1.2	Nécessité d'utilisation de noms explicites	21
4.1.3	Règles d'interprétation des différentes formes de noms	21
4.1.4	Unicité des noms	21
4.1.5	Procédure de résolution de litige sur déclaration de nom	21
4.1.6	Reconnaissance, authentification et rôle des noms de marques	21
4.1.7	Authentification du MC	22
4.1.8	Authentification du demandeur	22
4.2	Authentification d'une demande de révocation	23
4.3	Renouvellement de clés (hors révocation)	23
4.4	Régénération de clés après révocation	23
5	BESOINS OPERATIONNELS	24
5.1	Demande de Certificat	24
5.1.1	Origine de la demande	24
5.1.2	Informations à fournir	24
5.1.3	Procédure de demande	24
5.1.4	Preuve de possession de la clé privée.	24
5.1.5	Acceptation du Certificat	24
5.1.6	Dossier de Souscription (DDS)	24
5.1.7	Archivage des dossiers	25
5.1.8	Opérations à effectuer	25
5.1.9	Emission et distribution d'un Certificat	25
5.1.10	Acceptation d'un Certificat	26
5.2	Révocation de Certificat	26
5.2.1	Origine d'une demande de révocation d'un Certificat Porteur	26
5.2.2	Informations à fournir	27
5.2.3	Procédure de demande de révocation d'un Certificat Porteur	27
5.2.4	Délai de traitement d'une révocation	27
5.2.5	Publication des motifs de révocation d'un Certificat.	27
5.2.6	Besoins spécifiques en cas de révocation pour compromission de clé	27
5.2.7	Suspension de Certificats	27
5.3	Renouvellement d'un Certificat	28
5.4	Emission des nouveaux certificats après révocation	28
5.5	Suspension de certificats	28
5.6	Vérification de la validité des certificats	28
5.6.1	Contrôle en ligne du statut de révocation de Certificat	28
5.6.2	Formes de publication des LCR	28
5.7	Renouvellement de clé d'une composante de l'ICP	28
5.7.1	Clé de signature de l'AC	28
5.7.2	Clé de signature des autres composantes de l'ICP	28
5.8	Révocation d'un certificat d'une composante de l'ICP	28
5.8.1	Causes de révocation d'un certificat d'une composante de l'ICP	29
5.8.2	Révocation d'un certificat d'une composante de l'ICP	29
5.8.3	Révocation du certificat de signature de l'AC	29
5.8.4	Délai de traitement	29
5.9	Journalisation des événements	29
5.9.1	Information enregistrées	30
5.9.2	Imputabilité	30
5.9.3	Evènements enregistrés par l'AE	30
5.9.4	Evènements enregistrés par l'AC	30
5.9.5	Evènements divers	31
5.9.6	Processus de journalisation	31
5.9.7	Protection d'un journal d'évènements	31
5.9.8	Copies de sauvegarde des journaux d'évènements	31

AC @vocats Classe 3Plus

Politique de Certification

5.9.9	Système de collecte des journaux (interne ou externe)	31
5.9.10	Anomalies et audit	32
5.10	Archives	32
5.10.1	Types de données à archiver	32
5.10.2	Protection des archives	32
5.10.3	Période de rétention des archives	33
5.10.4	Duplication des archives	33
5.10.5	Horodatage des enregistrements	33
5.10.6	Procédure de collecte des archives	33
5.10.7	Procédure de récupération des archives	33
5.11	Cessation d'activité de l'AC	33
5.11.1	Transfert d'activité	33
5.11.2	Cessation définitive	34
6	CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES, CONTROLE DU PERSONNEL	35
6.1.1	Situation géographique	35
6.1.2	Accès physique	35
6.1.3	Energie et air conditionné	35
6.1.4	Exposition aux liquides	35
6.1.5	Sécurité incendie	35
6.1.6	Site de secours	35
6.1.7	Conservation des médias	35
6.1.8	Destruction des supports	35
6.1.9	Sauvegarde hors site	36
6.2	Contrôles des procédures	36
6.2.1	Rôles de confiance	36
6.2.2	Nombre de personnes nécessaires à l'exécution de tâches sensibles	36
6.2.3	Identification et authentification des rôles	36
6.3	Contrôle du personnel	36
6.3.1	Passé professionnel, qualifications, expérience, et exigences d'habilitations	36
6.3.2	Procédures de contrôle du passé professionnel	37
6.3.3	Exigences de formation	37
6.3.4	Fréquence des formations	37
6.3.5	Gestion des métiers	37
6.3.6	Sanctions pour des actions non-autorisées	37
6.3.7	Contrôle des personnels contractants	37
6.3.8	Documentation fournie au personnel.	37
7	CONTROLES TECHNIQUES DE SECURITE	38
7.1	Génération et installation de bi-clés	38
7.1.1	Génération des bi-clés de Porteur	38
7.1.2	Transmission de la clé publique de signature (du Porteur) à l'AC	38
7.1.3	Fourniture d'un Certificat d'AC	38
7.1.4	Tailles des clés	38
7.1.5	Paramètres de génération des clés	38
7.1.6	Contrôle de la qualité des paramètres des clés	38
7.1.7	Mode de génération du biclé de l'AC	38
7.1.8	Usage de la clé publique des Porteurs	39
7.2	Protection de la clé privée	39
7.2.1	Dispositifs de gestion des éléments secrets du Porteur	39
7.2.2	Contrôle de la clé privée de signature de l'AC par plusieurs personnes	39
7.2.3	Récupération de clé privée de confidentialité* du Porteur.	39
7.3	Autres aspects de la gestion des bi-clés	39
7.3.1	Archivage des clés publiques des Porteurs	39
7.3.2	Durée de vie des Certificats	39
7.4	Code PIN des Porteurs	39

AC @vocats Classe 3Plus

Politique de Certification

7.4.1	Génération et utilisation des codes PIN	39
7.4.2	Protection des codes PIN	39
7.5	Sécurité des postes de travail des composants de l'ICP	39
7.6	Contrôles techniques du système durant son cycle de vie	40
7.6.1	Contrôles des développements des systèmes	40
7.6.2	Contrôles de la gestion de la sécurité.	40
7.7	Contrôles de la sécurité réseau	40
7.8	Contrôles des modules cryptographiques	40
8	PROFILS DE CERTIFICATS ET DE LCR	41
8.1	Profil des Certificats	41
8.2	Profil de LCR	42
8.2.1	Champs des LCR	42
8.2.2	Extensions des LCR	42
9	ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC	43
9.1	Procédures de modification de la PC	43
9.1.1	Causes de modification	43
9.1.2	Délai de préavis	43
9.2	Procédures de publication et de notification	43
9.3	Procédures d'approbation de la PC	43
10	ANEXE 1 – TEXTES LEGISLATIVES ET REGLEMENTAIRES	44

AC @vocats Classe 3Plus

Politique de Certification

1 PREAMBULE

Ce document constitue la Politique de Certification de l'Autorité de Certification AC @vocats Classe 3Plus, c'est-à-dire l'ensemble des obligations et engagements des différents acteurs et plus particulièrement de l'AC AC @vocats Classe 3Plus, concernant la délivrance de certificats numériques.

L'une des ambitions de l'AC AC @vocats Classe 3Plus est de satisfaire aux exigences relatives aux certificats qualifiés tels que définis dans le décret 2001-271 du 30 Mars 2001. Les certificats sont délivrés suite à un face-à-face. Ils sont générés et protégés par un support matériel (module cryptographique).

L'infrastructure à Clés Publiques repose sur les acteurs suivants :

- L'Autorité de Certification (AC), dont la fonction est de définir la Politique de Certification (PC) et de la faire appliquer ;
- L'Autorité d'Enregistrement (AE) : Ce service vérifie les informations d'identification du futur Porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante au service de génération des certificats et/ou au service de fourniture du dispositif du Porteur
- L'Opérateur de Services de Certification, dont la fonction est d'assurer la fourniture et la gestion du cycle de vie des Certificats. Son rôle consiste à mettre en œuvre une plate-forme logicielle et matérielle, dans le respect des exigences énoncées dans la Politique de Certification (PC) et dont les modalités sont détaillées dans la Déclaration des Pratiques de Certification (DPC).
- Le Porteur de Certificat est la personne physique détentrice d'un Certificat ;
- Le Tiers Utilisateur ou l'application utilisatrice des Certificats, dont la fonction est d'authentifier un Porteur de Certificat, ou de vérifier une signature numérique émise par Porteur de Certificat ;
- Le cas échéant le Mandataire de Certification personne en charge d'effectuer le face-à-face avec le futur Porteur et de fournir lors d'un face-à-face à l'AE les informations nécessaires à la délivrance du certificat du Porteur.

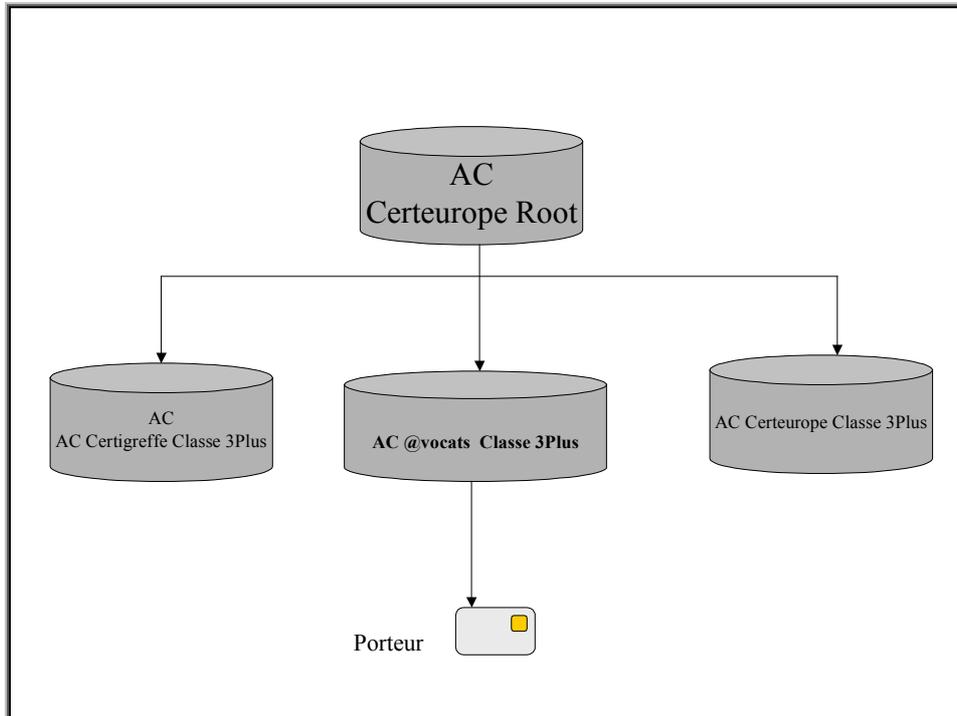
Dans le cadre présent, les différents acteurs sont les suivants :

- Le **Conseil** National des Barreaux est l'Autorité de Certification;
- Les fonctions de l'Autorité d'Enregistrement sont assurées par des entités responsables de la tenue des tableaux des Ordres, les Ordres sont donc au premier titre les AE. ;
- La société **CERTEUROPE** est l'Opérateur de Services de Certification de l'Autorité de Certification AC @vocats Classe 3Plus;
- Le Porteur est un Avocat dûment inscrit au tableau de son Ordre;

L'Autorité de Certification AC @vocats Classe 3Plus s'inscrit dans une hiérarchie d'Autorités de Certification. Le modèle de confiance est le suivant :

AC @vocats Classe 3Plus

Politique de Certification



2 PRESENTATION GENERALE DE LA PC

Une Politique de Certification (PC) est identifiée par un nom unique (OID*). Elle est composée d'un ensemble de règles décrivant les conditions de recevabilité d'un Certificat pour des applications ayant des besoins de sécurité communs.

Une PC est définie indépendamment des modalités de mise en œuvre de l'Infrastructure à Clés Publiques (ICP) à laquelle elle s'applique. Elle décrit les exigences auxquelles l'ICP doit se conformer pour l'enregistrement et la validation des demandes de Certificats, et pour la gestion des Certificats. Les procédures de certification sont rassemblées dans un document appelé Déclaration des Pratiques de Certification (DPC), distinct de la PC, qui décrit comment ces exigences sont atteintes en pratique.

La gestion des Certificats couvre toutes les opérations relatives à la vie d'un Certificat, depuis son émission jusqu'à la fin de vie de ce Certificat (expiration ou révocation).

L'Autorité de Certification AC @vocats Classe 3Plus vise le statut d'AC qualifiée au sens du décret 2001-271.

Cette PC est conforme au document "Procédures et Politiques de Certification de Clés (PC²)", niveau fort, émis par la Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI), à la PRIS *** de l'ADAE (Certificats Entreprise) ainsi qu'au document RFC 3647 de l'IETF.

2.1 Liste des acronymes utilisés

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AP	Autorité de Politique
C	Country (Pays)
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
DDS	Dossier de Souscription
DGI	Direction Générale des Impôts
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
DSA	Digital Signature Algorithm
EPC	Enoncé des Pratiques de Certification, ou DPC
ICP	Infrastructure à Clés Publiques
LDAP	Light Directory Access Protocol
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
MD5	Message Digest n°5
O	Organisation
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification

AC @vocats Classe 3Plus

Politique de Certification

PC ²	Procédures et Politiques de Certification de Clés
RSA	Rivest Shamir Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Algorithm One
SSL	Secure Sockets Layer
TLS	Transport Layer Security

2.2 Définitions des termes utilisés dans la PC

Le symbole (*) signifie que le terme est défini dans le présent paragraphe. Il est utilisé dans le reste du document lorsqu'il est important de renvoyer à la définition du terme employé.

Applications utilisatrices (de Certificats) : applications nécessitant la mise en œuvre des Certificats délivrés par l'AC*.

Autorité de Certification (AC) : autorité responsable de l'émission et de la gestion des Certificats et des LCR* signés en son nom. L'AC est le maître d'ouvrage de l'ICP*. Elle assume en particulier les fonctions suivantes :

- mise en application de la PC* ;
- gestion des Certificats* ;
- gestion des supports et de leur code PIN* ;
- publication des Listes de Certificats Révoqués (LCR*) ;
- journalisation et archivage des événements et informations relatives au fonctionnement de l'ICP*.

Autorité d'Enregistrement (AE) : entité qui vérifie que les demandeurs ou les Porteurs de Certificat sont identifiés, que l'identité présentée est valide et cohérente, que les contraintes liées à l'usage d'un certificat sont remplies, tout cela conformément à la Politique de Certification. L'AE a également pour tâche :

- de réceptionner les demandes de révocation de certificats et de les traiter ;
- d'archiver les dossiers de demande de certificats ou de révocation ;
- l'AE peut être constituée d'une seule unité ou d'unités distinctes, fixes ou mobiles. Elles se sont toutes engagées à répondre aux exigences de la PC* AC @vocats Classe 3Plus en matière d'enregistrement des Porteurs.

Bi-clé : couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptographie basée sur des algorithmes asymétriques. Le bi-clé peut être utilisé à des fins de signature, ou d'échange de clé ou de transport de clé.

Certificat : Fichier électronique attestant qu'une clé publique appartient à l'entité qu'il identifie (personne physique ou morale ou entité matérielle). Il est délivré par une autorité de confiance : l'Autorité de Certification. En signant le certificat, l'AC valide le lien entre une entité identifiée et un bi-clé cryptographique. Dans ce document le Certificat désigne le certificat délivré par l'Autorité

AC @vocats Classe 3Plus

Politique de Certification

de Certification AC @vocats Classe 3Plus à un Porteur. Par exception il peut désigner sous les vocables "Certificat AC", "Certificat AE" les certificats de l'AC, ou d'une AE.

Chaîne de confiance : ensemble des Certificats nécessaires pour valider la filiation d'un Certificat Porteur. Dans le cadre de cette PC, l'AC AC @vocats Classe 3Plus, dispose d'un certificat d'AC émis par l'AC Racine appelée CertEurope Root CA.

Clé privée de confidentialité : clé privée du bi-clé d'échange de clé*.

Code PIN (Personal Identification Number): code confidentiel adressé par courrier postal au Porteur* après avoir été généré automatiquement et aléatoirement par l'AC*. Il permet de mettre en œuvre le Certificat du Porteur. Le Porteur* assume en toutes circonstances le caractère secret du **Code PIN***, aussi l'utilisation de celui-ci fera présumer de manière irréfutable que le Porteur* est bien l'initiateur de l'action opérée (non-répudiation).

Code de révocation d'un Certificat : code adressé par courrier postal au Porteur* après avoir été généré automatiquement par l'AC* et permettant d'authentifier la demande de révocation du Certificat.

Common Name (CN) : identité réelle ou pseudonyme du Porteur* (exemple CN = Dupont Jean).

Compromission : une clé est dite compromise lorsqu'elle est connue par d'autres personnes que celles habilitées à la mettre en œuvre.

Déclaration des Pratiques de Certification (DPC) : énoncé des procédures et pratiques appliquées par l'AC* pour émettre et gérer des Certificats en respectant les engagements pris dans sa Politique de Certification

Demandeur (de certificats) : personne physique ou morale souhaitant obtenir les services de l'AC.

Distinguished Name (DN) : nom distinctif au sens X.500 du terme, pour lequel le Certificat est émis.

Dossier de Souscription (DDS) : ensemble des pièces justificatives à fournir à l'AE* afin de lui permettre de vérifier les informations demandées par l'AC* pour l'émission d'un Certificat. Ces pièces justificatives sont décrites dans la présente PC*.

Émission (d'un Certificat) : fait d'exporter un Certificat à l'extérieur d'une AC* (pour une remise à un Porteur*, ou une demande de publication).

Enregistrement (d'un Porteur) : opération qui consiste pour une Autorité d'Enregistrement* ou un Mandataire de Certification à constituer le profil* d'un demandeur de Certificat à partir de son Dossier de Souscription*, conformément à la Politique de Certification*.

Génération (d'un Certificat) : action réalisée par une AC* et qui consiste à signer un ensemble de champs comportant notamment le DN et la clé publique du futur Porteur.

Infrastructure à Clé Publique (ICP) : ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de Certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

Journaux : fichiers électronique ou registres papier collectant toutes les traces d'exécution des traitements, transactions et programmes produites par un système d'information (dénommés aussi "logs" ou "journaux d'événements").

Liste de Certificats Révoqués (LCR) : liste de numéros de Certificats ayant fait l'objet d'une révocation*.

AC @vocats Classe 3Plus

Politique de Certification

Module cryptographique : dispositif matériel, du type module cryptographique ou token muni de microprocesseur, permettant d'une part de générer et protéger les éléments secrets tels que les clés privées ou les codes PIN*, et d'autre part de procéder à des calculs cryptographiques mettant en œuvre ces éléments.

Politique de Certification (PC) : ensemble de règles, définissant les exigences auxquelles l'AC* se conforme dans la mise en place de prestations adaptées à certains types d'applications. La Politique de Certification doit être identifiée par un OID* défini par l'AC*.

Porteurs(de Certificats) : personne physique à qui est délivré un Certificat. Dans la phase amont de certification, il est un "demandeur" de Certificat, et dans le contexte du Certificat X.509V3, il est un "Subject".

Publication (d'un Certificat) : opération consistant à mettre un Certificat à disposition d'Utilisateurs* pour leur permettre de vérifier une signature (ex : annuaire X.500).

Renouvellement (d'un Certificat) : opération effectuée en fin de période de validité d'un Certificat et qui consiste à générer un nouveau Certificat pour un Porteur*. La re-génération de Certificat après révocation* n'est pas un renouvellement.

Représentant légal : personne physique qui, de par la loi, a qualité pour représenter une personne morale.

Révocation (d'un Certificat) : opération demandée par le Porteur*, l'AE*, l'AC* ou par toute autre personne autorisée dont le résultat est la suppression de la garantie d'engagement de l'AC* sur un Certificat donné, avant la fin de sa période de validité. Par exemple, la compromission* d'une clé ou le changement d'informations contenues dans un Certificat doivent conduire à la révocation du Certificat. L'opération de révocation est considérée comme terminée lorsque le numéro de Certificat à révoquer et la date de révocation sont publiés dans la Liste des Certificats Révoqués (LCR*).

RPVA : Réseau Privé Virtuel des Avocats :XXXX A Définir

Validation (de Certificat) : opération de contrôle du statut d'un Certificat ou d'une Chaîne de confiance*.

Vérification (de signature) : opération de contrôle d'une signature numérique.

2.3 Type d'applications concernées par la PC

L'Autorité de Certification AC @vocats Classe 3Plus distribue des Certificats qui peuvent être utilisés dans le cadre :

- d'applications internes par exemples celles mise en œuvre dans le cadre du RPVA;
- d'autres applications ayant signé un accord avec l'AC AC @vocats Classe 3Plus ;
- de téléprocédures
- d'échange de documents signés entre diverses parties.

Cette utilisation implique en particulier l'acceptation par les gestionnaires de l'application ou les utilisateurs de l'intégralité des chapitres contenus dans cette PC.

2.4 Type de certificats délivrés par l'AC AC @vocats Classe 3Plus

L'Autorité de Certification AC @vocats Classe 3Plus délivre un seul type de certificats aux Porteurs : un certificat de signature.

AC @vocats Classe 3Plus

Politique de Certification

Les certificats délivrés par l'AC AC @vocats Classe 3Plus présentent la particularité de n'être délivrés que suite à un face-à-face entre l'AE et le demandeur. Ils ont pour support un module cryptographique, dans laquelle le bi-clé est directement généré, stocké et protégé.

2.5 Modification de la PC

Cette PC sera revue périodiquement notamment pour :

- assurer sa conformité aux normes de sécurité attendues;
- mettre à jour la liste des applications concernées par la PC ;
- s'adapter aux évolutions technologiques.

La périodicité minimale de révision de cette PC est deux ans. Les modifications sont réalisées conformément au chapitre 9 du présent document.

2.6 Identification de la PC - OID

La présente PC est identifiée par l'OID 1.2.250.1.148.3.1, elle est ci-après désignée sous le nom de "PC"

2.7 Coordonnées des entités responsables de la présente PC

2.7.1 Organisme responsable

Le Conseil National des Barreaux est responsable de cette PC.

Conseil National des Barreaux
23 rue de la Paix
75008 Paris
FRANCE

2.7.2 Personne physique responsable

M. le Président du Conseil National des Barreaux
23 rue de la Paix
75008 Paris
FRANCE

2.7.3 Personne déterminant la conformité de la DPC à la PC

Le Conseil National des Barreaux détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans le domaine des Infrastructures à Clés Publiques.

3 DISPOSITIONS DE PORTEE GENERALE

3.1 Contrôle de conformité à la PC

3.1.1 Objet des contrôles de conformité

L'Autorité de Certification AC @vocats Classe 3Plus a la responsabilité du bon fonctionnement des composantes de l'ICP, conformément aux dispositions énoncées dans le présent document. L'AC effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette ICP.

Par ailleurs, l'AC AC @vocats Classe 3Plus souhaite obtenir le statut d'AC Qualifiée donnant aux certificats qu'elle émet une valeur légale (présomption de fiabilité). Dans ce cadre, l'AC accepte les audits demandés par les autorités concernées.

3.1.2 Indépendance et qualifications du contrôleur

Le contrôleur est désigné par l'AC ou par les autorités concernées. Le contrôleur est choisi selon des critères d'indépendance et d'expertise dans le domaine de la sécurité informatique et, en particulier, des ICP.

3.1.3 Fréquence du contrôle de conformité

Un contrôle est réalisé au moins une fois par an à la demande de l'AC.

Le contrôle de conformité est réalisé en cas de renouvellement d'un bi-clés d'AC, avant toute nouvelle émission et signature de Certificats par cette dernière.

3.1.4 Périmètre du contrôle de conformité

Le contrôle de conformité porte sur les points suivants

- dispositions générales (cf chapitre 3) ;
- identification et authentification (cf. chapitre 4) ;
- besoins opérationnels.(cf. chapitre 5) ;
- contrôles de sécurité physique, contrôle des procédures, contrôle du personnel.(cf. chapitre 6) ;
- contrôles techniques de sécurité . (cf. chapitre 7) ;
- profil des certificats et LCR. (cf. chapitre 8) ;
- spécifications d'administration. (cf. chapitre 9) ;

3.1.5 Communication des résultats

Les résultats du contrôle de conformité sont communiqués par le contrôleur au demandeur (Conseil National des Barreaux ou les autorités concernées).

Eu égard au caractère confidentiel de ces informations, la publication des résultats est limitée et strictement contrôlée.

3.1.6 Actions entreprises en cas de non-conformité

En cas de non-conformité, l'AC AC @vocats Classe 3Plus décide de toute action correctrice nécessaire.

En fonction du degré de non-conformité, l'AC AC @vocats Classe 3Plus peut :

AC @vocats Classe 3Plus

Politique de Certification

- demander la mise en place d'actions correctrices dont la réalisation sera vérifiée lors du prochain audit ;
- demander la correction des non-conformités selon un calendrier précis à la suite duquel un contrôle de mise en conformité sera effectué ;
- demander la révocation de son Certificat à l'AC racine CertEurope Root CA.

3.2 Respect et interprétation des dispositions juridiques

3.2.1 Droit applicable

La Loi française est applicable aux dispositions du présent document (y incluant l'ensemble des documents relatifs à l'abonnement au service de certification de l'AC AC @vocats Classe 3Plus). En cas de traduction, seule la version française du présent document fera foi. En cas de difficulté, les parties se conformeront à la procédure de règlement des litiges prévue aux Conditions Générales du Service de Certification AC @vocats Classe 3Plus.

Si une disposition de la présente PC s'avérait inapplicable ou incompatible avec une loi ou un règlement en vigueur, elle sera considérée comme nulle, cette nullité n'affectant en aucune manière la validité des autres dispositions de la présente PC.

3.2.2 Séquestre

Sans objet, l'AC AC @vocats Classe 3Plus ne met pas en œuvre de fonction de séquestre pour les clés privées associées au certificats qu'elle émet.

3.2.3 Arbitrage des litiges

Toute contestation relative aux dispositions du présent document sera soumise, préalablement à toute instance judiciaire, à la procédure décrite à l'article règlement des litiges des Conditions Générales du Service de Certification précisé dans le contrat d'abonné.

A défaut de règlement amiable, le litige sera porté devant le Tribunal de Commerce de Paris.

3.3 Obligations

3.3.1 Obligations de l'AC

L'AC AC @vocats Classe 3Plus garantit le respect des exigences définies dans la présente PC. Quels que soient les recours à des entités extérieures pour la mise en œuvre de son activité de certification, l'AC garantit le respect de ces exigences par chacune de ces entités.

3.3.2 Obligations de l'AE

Lorsque l'AE est saisie d'une demande de Certificat, elle doit :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives ainsi que l'exactitude des mentions qui établissent l'identité du demandeur, son inscription au tableau d'un Ordre, de la personne morale ou administrative qui l'emploie selon les procédures décrites au chapitre 4 de cette PC ;
- déclencher la génération des bi-clés du Porteur sur un module cryptographique vierge.
- transmettre les demandes de certificat à l'AC AC @vocats Classe 3Plus ;
- remettre le module cryptographique ainsi activé au demandeur;

AC @vocats Classe 3Plus

Politique de Certification

Note : L'AE ne peut utiliser le certificat du Porteur car elle n'a jamais connaissance du code PIN.

- Archiver les pièces du dossier.

Lorsque l'AE est saisie d'une demande de révocation de Certificat, elle s'engage à :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence de l'origine de la demande,
- mettre en œuvre les moyens permettant de traiter la demande de révocation selon les exigences décrites au § 4.4.

L'AE doit archiver les dossiers de souscription des porteurs (et éléments de confirmation d'acceptation) et de demandes de révocation suivant les modalités décrites au chapitre 4 de cette PC.

3.3.3 Obligations communes à toutes les composantes de l'ICP

Les composantes de l'ICP s'engagent à :

- protéger et garantir l'intégrité et la confidentialité de leurs clés privées ;
- n'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification ;
- respecter et appliquer la PC au moins pour les parties leur incombant;
- se soumettre aux contrôles de conformité effectués par le Conseil National des Barreaux ou les autorités concernées, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- respecter les accords ou contrats qui les lient entre elles ainsi qu'aux Porteurs de Certificats ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

3.3.4 Obligations relatives à la gestion des Certificats

L'AC AC @vocats Classe 3Plus s'engage à :

- pouvoir démontrer aux applications utilisatrices de ses certificats, qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, ceci implique entre particulier de pouvoir justifier de l'identité de tout Porteur ;
- tenir à disposition des Porteurs et des Utilisateurs, la liste des certificats ayant fait l'objet d'une révocation; cette liste est publiée sous la forme d'une LCR conformément au chapitre 3.3.7 ;
- garantir la cohérence entre la PC et la DPC associée ;

AC @vocats Classe 3Plus

Politique de Certification

- s'assurer que ses Porteurs connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des Certificats. La relation entre un Porteur et l'AC AC @vocats Classe 3Plus est formalisée par un document intitulé "Conditions Générales des Certificats AC @vocats Classe 3Plus" précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

3.3.5 Obligations relatives à la gestion des supports, des codes PIN et des codes de révocation

L'AC AC @vocats Classe 3Plus s'engage à :

- transmettre en toute confidentialité les codes PIN aux Porteurs par un moyen sécurisé différent de celui utilisé pour la remise du certificat (qui est délivré en mains propres par l'AE sur un module cryptographique) ;
- supprimer toute trace des codes PIN sur ses systèmes après transmission au Porteur ;
- assurer la confidentialité des codes de révocation d'urgence;
- assurer le caractère aléatoire des codes PIN générés.

3.3.6 Obligations relatives à l'identification

L'identification du Porteur est assurée par l'AE éventuellement assistée du MC.

L'identification du Porteur consiste en la vérification de son identité ainsi que celle de l'entreprise en se basant sur les pièces justificatives présentées, comme précisé au chapitre 3.3.2

3.3.7 Obligations relatives à la publication

L'AC AC @vocats Classe 3Plus s'engage à diffuser publiquement :

- Les différentes versions de sa Politique de Certification;
- la Liste de Certificats Révoqués (LCR) ;
- le certificat de l'AC à laquelle elle est subordonnée (i.e. le certificat de l'AC Certeurope ROOT CA) ;

L'AC AC @vocats Classe 3Plus s'engage par ailleurs à ce que la LCR soit :

- fiable, c'est-à-dire comportant uniquement des informations contrôlées et à jour ;
- protégée en intégrité ;
- d'un accès contrôlé quant à la mise à jour;
- publiée suivant les modalités décrites au chapitre 5.2 de cette PC ;
- disponible 24 heures sur 24 et 7 jours sur 7.

La prise en compte de la demande de certificat ou de révocation est immédiate : en cas de succès de l'authentification du demandeur (par l'AE) la requête (création ou révocation) est exécutée immédiatement. Ceci signifie en particulier que, pour une demande licite, la génération du certificat est immédiate ainsi que la publication de la LCR.

AC @vocats Classe 3Plus

Politique de Certification

3.3.8 Obligations relatives à la journalisation

L'AC AC @vocats Classe 3Plus enregistre tout événement relatif à son activité de certification. Ces enregistrements concernent :

- L'accès physiques aux machines de la plate-forme ;
- L'accès logique aux systèmes ;
- L'accès aux applications ;
- Les opérations effectuées sur ces applications.

Certains de ces journaux font l'objet de renseignements manuels, certains sont entièrement automatisés; tous concourent à assurer l'imputabilité de toute action sur la plate-forme de certification..

3.3.9 Obligations relatives à l'archivage

L'AC AC @vocats Classe 3Plus s'engage à archiver non seulement les journaux d'événement tels que décrits au chapitre 3.3.8, mais également tout les dossiers des demandeurs (pièces justificatives...).

Bien entendu ces archives sont disponibles en cas de nécessité (litige ou autre).

3.3.10 Obligations relatives au séquestre

Sans Objet . L'AC AC @vocats Classe 3Plus ne réalise pas de fonction de séquestre.

3.3.11 Obligations du Mandataire de Certification.

Le MC est une personne en relation directe avec l'AE pour le compte de demandeurs de Certificats. Il assure les fonctions d'identification des demandeurs pour le compte de l'AE. Il est dûment authentifié par une AE habilitée et lié contractuellement avec l'AC AC @vocats Classe 3Plus.

Les engagements du MC à l'égard de l'AC sont précisés dans un contrat dans lequel le MC s'engage en particulier à effectuer correctement et de façon indépendante les contrôles d'identité du demandeur.

Le MC s'engage à :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives et l'exactitude des mentions qui établissent l'identité du Porteur* de l'Entreprise selon les procédures décrites au chapitre 3 ;
- vérifier avec un soin raisonnable l'origine et l'exactitude d'une demande de révocation de certificat, et mettre en œuvre les moyens permettant de traiter la demande de révocation selon les exigences décrites au §4.4 ;
- effectuer correctement et de façon indépendante les contrôles du dossier du demandeur ;
- protéger la confidentialité des codes de révocation d'urgence qui lui seront transmis par les Porteurs.

La relation entre le MC et l'AC AC @vocats Classe 3Plus est formalisée par un engagement contractuel du MC.

AC @vocats Classe 3Plus

Politique de Certification

Note : Ces engagements ne changent en rien ceux de l'AE.

3.4 Obligations du Porteur

Le Porteur a l'obligation de :

- communiquer des informations exactes lors de la demande de certificat ;
- informer l'AC ou l'AE AC @vocats Classe 3Plus en cas de modifications de ces informations ;
- protéger sa clé privée par des moyens appropriés à l'environnement dans lequel se trouve cette clé, contre la perte, la divulgation, la compromission, la modification ou l'usage non autorisé ;
- définir son code de révocation. Ce code doit impérativement être défini dès réception du code PIN par le Porteur afin de permettre à celui-ci de demander une révocation d'urgence de son certificat. La procédure à suivre pour la définition est indiquée dans le courrier accompagnant le code PIN. Dans le cas où le Porteur ne définirait pas ce code de révocation, la révocation d'urgence ne sera pas possible.
- protéger son code PIN et son code de révocation d'urgence ;
- transmettre son code de révocation d'urgence à son MC lorsque celui-ci existe.
- respecter les conditions d'utilisation de sa clé privée et du Certificat correspondant ;
- informer sans délai son MC, l'AE ou l'AC AC @vocats Classe 3Plus en cas de compromission ou de soupçon de compromission de sa clé privée.

La relation entre le Porteur et l'AC AC @vocats Classe 3Plus est formalisée par un engagement contractuel du Porteur.

3.5 Obligations des applications utilisatrices et des utilisateurs de Certificats

Les applications utilisatrices et les utilisateurs de Certificats doivent :

- respecter l'usage pour lequel un Certificat a été émis ;
- vérifier la signature numérique de l'AC AC @vocats Classe 3Plus émettrice du Certificat ainsi que celle de l'AC Certeurope Root CA ;
- contrôler la validité des Certificats (date de validité et statut de révocation).
- Contrôler l'usage autorisé des certificats

3.6 Responsabilités

3.6.1 *Responsabilité de l'AC*

L'AC AC @vocats Classe 3Plus s'engage à respecter la conformité de son dispositif de gestion des Certificats et de ses procédures avec les exigences décrites dans cette PC.

L'AC AC @vocats Classe 3Plus fait son affaire personnelle de toute conséquence dommageable résultant du non-respect du présent document par elle-même ou l'une de ses composantes

AC @vocats Classe 3Plus

Politique de Certification

L'AC AC @vocats Classe 3Plus est responsable en cas de négligence ou de faute intentionnelle des préjudices causés à une personne physique ou morale qui s'est fiée raisonnablement au certificats @vocat

Le détail des engagements pris envers les Porteurs et les Entreprises est détaillé dans les Conditions Générales du contrat d'abonnement et dans les Conditions Générales des Certificats @vocat.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes.

3.6.2 Responsabilité de l'AE

Seule l'AC AC @vocats Classe 3Plus peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les Porteurs et les utilisateurs finaux.

3.7 Politique de confidentialité de l'AC

3.7.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux Certificats ;
- les Codes PIN pour les Porteurs ;
- les données d'identification ou autres informations personnelles du Porteur contenues dans son certificat, sauf
 - si le Porteur a donné explicitement son consentement préalablement à la publication du Certificat ;
 - si leur publication a été demandée sur décision judiciaire ou administrative ;
- les causes de révocation des Certificats ;
- les journaux d'événements des composantes de l'ICP AC @vocats Classe 3Plus ;
- le dossier de demande de certificat du Porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les Certificats) ;
- les rapports d'audit ;
- la DPC.

Ces données ne seront utilisées et ne feront l'objet de communication extérieure que pour les strictes nécessités de la gestion des opérations effectuées en exécution de la DPC associée à la présente PC, pour répondre aux exigences légales ou pour l'exécution de travaux ou de prestations de services confiés à des prestataires.

Les personnes sur lesquelles portent ces informations nominatives auront le droit d'en obtenir communication, auprès de l'AE, et d'en exiger le cas échéant, la rectification comme précisé dans la loi 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3.7.2 Divulgence des causes de révocation

La cause de la révocation n'est pas publiée dans la LCR.

AC @vocats Classe 3Plus

Politique de Certification

3.7.3 Remise sur demande du propriétaire

L'AC AC @vocats Classe 3Plus ne dispose pas d'information que le Porteur ne possède (en particulier la clé privée et le code PIN), en conséquence elle ne remettra aucune donnée sur demande du propriétaire hormis bien entendu les informations protégées par la loi 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3.7.4 Délivrance aux autorités habilitées

L'activité de l'AC AC @vocats Classe 3Plus s'exerce dans le cadre de la législation française, aussi sur requête d'une autorité habilitée, l'AC AC @vocats Classe 3Plus peut être amenée à fournir certaines informations confidentielles selon la loi L90-1170.

3.7.5 Droits de propriété intellectuelle

Lors de l'exécution des prestations de services définies dans le présent document et/ou de tout autre document contractuel relatif au Service de Certification AC @vocats Classe 3Plus, il peut être livré des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire de ces services aura le droit de reproduire ces éléments pour son usage interne. Mais il ne pourra, sans l'autorisation préalable du détenteur des droits d'auteur, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.

Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant et ayant été réalisés hors du présent document et/ou de tout autre document contractuel relatif au Service de Certification AC @vocats Classe 3Plus.

4 IDENTIFICATION ET AUTHENTIFICATION

4.1 Enregistrement initial d'un Porteur

4.1.1 Conventions de noms

Les Certificats émis par l'AC AC @vocats Classe 3Plus contiennent dans le champ "Subject", le nom distinctif X501 (DN) du Porteur du Certificat au format *printableString*. Cette mention est obligatoire. En cas d'homonymie, un champ supplémentaire sera utilisé afin de différencier les 2 homonymes.

4.1.2 Nécessité d'utilisation de noms explicites

Les informations portées dans le champ "Subject" du Certificat @vocat sont décrites ci-dessous de manière explicite selon les différents champs X509:

- dans le champ Country : les caractères FR ;
- dans le champ Locality : le siège du Barreau d'appartenance du Porteur.
- dans le champ Organization : le numéro de SIREN de la personne morale employant le Porteur, tel que figurant au K-Bis ou dans l'avis SIRENE pour les Avocats exerçant en indépendant ; ce numéro sera précédé de la chaîne de caractères « 0002 » ;
- dans le champ Organizational Unit : le numéro CNBF du Porteur
- dans le champ Common Name le prénom suivi du nom du Porteur ;
- dans le champ First Name : le nom du Porteur

4.1.3 Règles d'interprétation des différentes formes de noms

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Subject" des Certificats.

Ces informations sont établies par l'AE et reposent essentiellement sur les règles suivantes :

- tous les caractères sont au format printableString, i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501 ;
- les prénoms et noms composés sont séparés par des tirets " - ".

4.1.4 Unicité des noms

L'unicité d'un Certificat est établie par l'unicité de son numéro de série.

L'unicité du DN est elle-même garantie par l'unicité des informations permettant de construire ce dernier notamment le numéro CNBF est un identifiant unique.

4.1.5 Procédure de résolution de litige sur déclaration de nom

Sans objet . Le numéro CNBF assurant à lui seul l'unicité du DN.

4.1.6 Reconnaissance, authentification et rôle des noms de marques

Sans objet . Aucun nom de marque n'est inscrit dans le certificat.

AC @vocats Classe 3Plus

Politique de Certification

4.1.7 Authentification du MC

La distribution des certificats par l'AE nécessite impérativement un face-à-face. Ce face-à-face peut se faire entre un MC et l'AE auquel cas l'AE vérifie :

- d'un original d'une pièce d'identité officielle du mandataire de sécurité comportant sa photo et sa signature et en prend copie ;
- du mandat signé par le représentant légal de l'entreprise désignant le MC à qui le certificat doit être délivré ;
- d'un engagement signé par le MC, l'engageant à effectuer correctement les contrôles des dossiers des demandeurs ;
- du DDS.

4.1.8 Authentification du demandeur

La distribution des certificats par l'AE nécessite impérativement un face-à-face. Ce face-à-face peut se faire directement entre le demandeur et l'AE auquel cas l'AE vérifie un original d'une pièce d'identité officielle du demandeur comportant sa photo et sa signature et en prend une copie.

4.1.8.1 Contenu du dossier déposé par le demandeur

Les informations suivantes doivent au moins figurer dans le DDS :

- Une preuve de l'appartenance du demandeur à la personne morale dont le SIREN sera porté dans le certificat (extraction du tableau de l'Ordre ou courrier du représentant légal)
- le contrat Porteur signé par le demandeur, portant l'acceptation des engagements de l'Abonné et désignant éventuellement le MC pour le représenter auprès de l'AE et se faire remettre le certificat ;
- une preuve que le numéro d'identification de la personne morale demandé est correcte (extraction du tableau de l'Ordre, extrait Kbis ou avis SIRENE) ;
- une adresse postale du demandeur;
- un justificatif d'identité (du demandeur) muni d'une photo (permis de conduire, carte d'identité nationale, passeport) ainsi qu'une copie de ce justificatif comportant la mention « copie certifiée conforme » . Cette copie sera signée par l'AE et le demandeur;
- le prénom et le nom à utiliser dans le champ CN du certificat ;
- éventuellement l'adresse de courrier électronique du demandeur.

4.1.8.2 Contenu du dossier déposé par un MC

En sus des données décrites au chapitre 4.1.8.1, et conformément au chapitre 4.1.7 le DDS doit contenir :

- un justificatif d'identité du MC muni d'une photo (permis de conduire, carte d'identité nationale, passeport) de l'Abonné ainsi qu'une copie de ce justificatif ;

- Un mandat signé par le représentant légal de l'entreprise désignant le MC comme tel ;
- Un engagement signé par le MC, l'engageant à effectuer correctement les contrôles des dossiers des demandeurs.

4.2 Authentification d'une demande de révocation

La procédure suivie pour authentifier une demande de révocation varie selon le mode de révocation:

- Selon la même procédure que pour l'enregistrement initial ;
- Par l'échange d'informations secrètes (code de révocation d'urgence) entre le demandeur de la révocation (Porteur ou MC) et l'Autorité d'Enregistrement. Le code de révocation d'urgence est défini par le Porteur et n'est connu que de lui-même et de son MC si celui-ci existe.

4.3 Renouvellement de clés (hors révocation)

L'Autorité de Certification AC @vocats Classe 3Plus ne permet pas le renouvellement des certificats et donc des clés.

4.4 Régénération de clés après révocation

Le Porteur suit le processus normal de demande de certificat décrit au § 4.1, si celle-ci intervient après une révocation.

5 BESOINS OPERATIONNELS

5.1 Demande de Certificat

5.1.1 Origine de la demande

Une demande de certificat AC @vocats Classe 3Plus doit émaner soit du demandeur dans le cas où le demandeur exerce en indépendant, soit du représentant légal de la personne morale employant le demandeur.

5.1.2 Informations à fournir

Les informations à fournir sont celles transmises dans le DDS (voir chapitre 4.1.8.1)

5.1.3 Procédure de demande

La demande de certificat se fait en quatre étapes (les 3 premières s'enchaînant immédiatement l'une après l'autre) :

- étape 1 : Face-à-face entre l'AE et le demandeur (ou le MC représentant le demandeur). Vérification de l'identité du demandeur ou du MC. Vérification du DDS.
- étape 2 : Emission du module cryptographique du porteur (contenant son certificat et son bi-clés) par l'AE ;
- étape 3 : Remise du module cryptographique en mains propres au Porteur ou au MC le représentant par l'AE ;
- étape 4 : Envoi par l'AC par courrier postal du code PIN au Porteur.

5.1.4 Preuve de possession de la clé privée.

Sans objet les bi-clés étant générés par la même personne que celle faisant la demande technique de certification (l'AE).

5.1.5 Acceptation du Certificat

La signature du contrat par le Demandeur vaut acceptation du certificat par celui-ci.

5.1.6 Dossier de Souscription (DDS)

5.1.6.1 Dossier déposé auprès d'une AE

Le dossier doit comprendre au moins l'équivalent des pièces suivantes :

- un mandat signé par un représentant de la personne morale employant le demandeur désignant la personne physique à qui le certificat doit être délivré. Ce mandat doit être signé pour acceptation par la personne physique bénéficiaire ;
- une pièce portant l'identification officielle de l'Entreprise retenue dans le certificat (généralement cette identification sera le numéro SIREN de l'Entreprise et la pièce un extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements) ;
- un justificatif d'identité de la personne physique mandatée entendus comme tels par la législation française (carte d'identité nationale, passeport, livret de famille, permis de conduire, etc...).

AC @vocats Classe 3Plus

Politique de Certification

- Lorsque le Demandeur est représenté par un MC, celui-ci doit de plus présenter un mandat du futur porteur le désignant comme MC

5.1.6.2 Dossier du MC d'une entreprise

Le MC n'a pour l'AC AC @vocats Classe 3Plus qu'un rôle de porteur de DDS et de modules cryptographiques, son dossier ne sert pas à compléter ou bâtir les dossiers des Porteurs.

5.1.7 Archivage des dossiers

Chaque DDS est archivé par l'AE conformément à la législation en vigueur, pendant cinq ans à partir de la date de clôture du dossier de souscription (fin d'abonnement).

Durant cette période d'archivage, le Dossier de Souscription est consultable sur demande justifiée par les autorités habilitées, par le Porteur et le représentant légal de l'Entreprise avant destruction des dites archives.

5.1.8 Opérations à effectuer

L'AE ou le MC s'engagent à effectuer les vérifications suivantes :

- établir l'identité (réelle) du futur Porteur ;
- s'assurer que le futur Porteur appartient bien à la personne morale par laquelle il prétend être employé ;
- s'assurer que le futur Porteur a pris connaissance des modalités applicables pour l'utilisation du Certificat ;
- s'assurer qu'il n'existe pas d'homonyme déjà porteur de certificat dans l'Entreprise.

L'AE s'engage à effectuer les opérations suivantes :

- attribuer un module cryptographique au demandeur, et faire générer par ce module le bi-clé du Porteur ;
- saisir les informations nominatives qui se trouveront ensuite dans le certificat ;
- signer la demande de certificat qui est envoyée au serveur de l'AC AC @vocats Classe 3Plus ;
- installer le certificat signé reçu de l'AC AC @vocats Classe 3Plus dans le module cryptographique ;
- remettre le module cryptographique contenant la clé privée et le certificat au demandeur (Porteur ou MC) ;
- archiver le dossier (DDS) conformément à la procédure d'archivage.

Le MC s'engage à remettre le module cryptographique à son porteur.

5.1.9 Emission et distribution d'un Certificat

A l'issue de la procédure d'enregistrement, le Certificat est transmis par l'AC AC @vocats Classe 3Plus au module cryptographique du Porteur où il est sauvegardé.

L'émission d'un certificat par l'AC AC @vocats Classe 3Plus indique que celle-ci a définitivement et complètement approuvé la demande de certificat selon les procédures décrites dans la DPC. Le

AC @vocats Classe 3Plus

Politique de Certification

certificat est considéré comme valable dès le moment où le demandeur accepte le module cryptographique, support du certificat.

5.1.10 Acceptation d'un Certificat

Lors du face à face avec l'AE AC @vocats Classe 3Plus ou le MC de l'Entreprise, le demandeur :

- valide les informations constituant la demande de certificat.

Lorsque son Certificat lui est remis, le Porteur :

- Vérifie les informations qu'il contient par exemple via le site web du CNB (<http://www.avocat-conseil.fr/cru>);
- Procède à la définition de son code de révocation d'urgence via le site web du CNB (<http://www.avocat-conseil.fr/cru>)

5.2 Révocation de Certificat

Un Certificat AC @vocats Classe 3Plus ne peut être que dans l'un des trois états suivants : valide, expiré ou révoqué.

Les cas de figures suivants peuvent être à l'origine de la révocation d'un Certificat Porteur, et notamment :

- les informations du Porteur figurant dans son Certificat ne sont pas ou plus exactes, ceci avant l'expiration normale du Certificat ;
- les informations figurant dans le DDS ne sont plus exactes ou s'avèrent frauduleuses ;
- le Porteur n'a pas respecté des règles d'utilisation du Certificat ;
- la clé privée du Porteur est suspectée de compromission, est compromise ou perdue ;
- la résiliation du contrat Porteur ou le non-paiement des sommes dues à l'AC AC @vocats Classe 3Plus selon les modalités du contrat Porteur;
- le départ, le décès du Porteur, ainsi que la cessation d'activité de la personne morale l'employant

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a eu connaissance, le Certificat concerné est révoqué et placé dans la Liste de Certificats Révoqués (LCR).

Note : cas de la révocation de la clé de l'AC. Lorsque le certificat de l'AC AC @vocats Classe 3Plus est révoqué, l'ensemble des certificats Porteurs a déjà été révoqué comme détaillé au chapitre 5.8.3

5.2.1 Origine d'une demande de révocation d'un Certificat Porteur

La révocation d'un Certificat Porteur peut émaner :

- du Porteur au nom duquel le Certificat a été émis ;
- du représentant légal de la personne morale employant le Porteur;
- du Mandataire de Certification ;

AC @vocats Classe 3Plus

Politique de Certification

- de l'AC AC @vocats Classe 3Plus émettrice du Certificat
- de l'AE.

5.2.2 Informations à fournir

La demande de révocation doit comporter au minimum

- le nom du demandeur de la révocation ;
- l'identité du Porteur ;
- le DN du Porteur ou toute autre information (par exemple le code de révocation d'urgence) permettant d'identifier de façon certaine le certificat devant être révoqué.

5.2.3 Procédure de demande de révocation d'un Certificat Porteur

Les demandes de révocation par les Porteurs, les MC et les représentants légaux peuvent être réalisées auprès de l'AE en face-à-face (pendant ses heures d'ouverture), par l'envoi d'une demande sous forme électronique signée à l'aide d'un Certificat émis par l'AC, ou encore via Internet (pour les Porteurs et MC en possession du code de révocation du certificat concerné).

Les procédures de révocation sont détaillées dans la DPC ainsi que dans les guides d'AE.

A la réception d'une demande de révocation, l'identité du demandeur est vérifiée. Cette vérification est réalisée par l'AE lors d'un face à face, par la saisie de codes confidentiels ou par échange de documents signés électroniquement. Si la demande est recevable, l'AE demande la révocation du Certificat en demandant à l'AC d'introduire le numéro de série du Certificat et la date de révocation du Certificat dans la Liste des Certificats Révoqués.

Si la demande n'est pas recevable, l'AE en informe le demandeur.

Le Porteur est notifié de la publication de la révocation.

L'opération est enregistrée dans les journaux d'événements de l'AC AC @vocats Classe 3Plus.

5.2.4 Délai de traitement d'une révocation

Le délai de publication de la révocation d'un Certificat n'excède jamais 24 heures ouvrées à partir de la réception de la demande de révocation.

5.2.5 Publication des motifs de révocation d'un Certificat.

Les motifs de révocation d'un Certificat Porteur sont demandés lors de la révocation (cf. contrat entre le Porteur et l'AC AC @vocats Classe 3Plus).

Ces motifs ne sont pas publiés dans les LCR de l'AC AC @vocats Classe 3Plus. Le Conseil National des Barreaux se réserve le droit de fournir les motifs de révocation sur demande d'une autorité habilitée.

5.2.6 Besoins spécifiques en cas de révocation pour compromission de clé

Aucune procédure spécifique n'est mise en place si la cause de révocation est la compromission de la clé privée de Porteur..

5.2.7 Suspension de Certificats

Le service de suspension n'est pas proposé dans le cadre de cette PC.

5.3 Renouvellement d'un Certificat

La durée de vie d'un certificat est de quatre ans et l'Autorité de Certification AC @vocats Classe 3Plus ne permet pas le renouvellement de ses Certificats.

Le porteur est prévenu par courrier trois mois avant la date de fin de validité de son certificat.

5.4 Emission des nouveaux certificats après révocation

Après une révocation, la génération d'un Certificat pour un Porteur suit la même procédure que pour l'enregistrement initial.

5.5 Suspension de certificats

L'AC AC @vocats Classe 3Plus ne gère pas la suspension des certificats

5.6 Vérification de la validité des certificats

5.6.1 Contrôle en ligne du statut de révocation de Certificat

Il est possible de vérifier en ligne si un Certificat émis par l'AC AC @vocats Classe 3Plus est révoqué.

Il est de la responsabilité des applications utilisatrices des Certificats et des utilisateurs de contrôler la validité d'un Certificat avant toute utilisation.

Les adresses de distribution des listes de révocation de l'AC AC @vocats Classe 3Plus sont définies au chapitre XXX et sont également présentes dans le champ CertificateRevocationListDistributionPoint des Certificats.

5.6.2 Formes de publication des LCR

L'accès à la Liste de Certificats Révoqués est possible via un annuaire LDAP V3 et via un serveur HTTP

Les LCR sont au format dénommé "LCR V2".

5.7 Renouvellement de clé d'une composante de l'ICP

5.7.1 Clé de signature de l'AC

La durée de vie des certificats Porteur étant de 4 ans, le renouvellement de la clé de signature de l'AC devra intervenir au plus tard quatre (4) ans avant la fin de sa validité. L'AC se réserve la possibilité de la renouveler avant sa limite de validité. La décision de son renouvellement pourra être prise plus tôt en fonction de divers critères (évolution de la technique cryptographique, allongement de la longueur, ...).

Le nouveau bi-clé généré servira à signer les nouveaux Certificats Porteurs émis ainsi que la LCR.

Le certificat précédent restera utilisable pour la validation de certificats émis avant le renouvellement.

5.7.2 Clé de signature des autres composantes de l'ICP

L'AC AC @vocats Classe 3Plus renouvellera les bi-clés des autres composantes de l'ICP 3 mois avant leur expiration.

5.8 Révocation d'un certificat d'une composante de l'ICP

Afin d'assurer la continuité et la sécurité de ses activités, l'AC AC @vocats Classe 3Plus se doit également de gérer de façon spécifique les clés et certificats des diverses composantes de l'AC.

AC @vocats Classe 3Plus

Politique de Certification

5.8.1 Causes de révocation d'un certificat d'une composante de l'ICP

Dans les circonstances suivantes, l'AC pourra révoquer la clé d'une composante de l'ICP :

- Cessation d'activité de la composante ;
- Non conformité des procédures appliquées par la composante ;
- Compromission ou suspicion de compromission perte ou vol de la clé privée de la composante.

5.8.2 Révocation d'un certificat d'une composante de l'ICP

La procédure de révocation d'un certificat d'une composante de l'ICP est définie dans la DPC et est à nouveau précisée dans le contrat liant l'AE à l'AC AC @vocats Classe 3Plus.

5.8.3 Révocation du certificat de signature de l'AC

Cette révocation doit avoir lieu en trois étapes :

5.8.3.1 Etape 1 : Alerte administrative

L'AC prévient l'ensemble des applications utilisatrices de ces certificats de l'imminence de la révocation de son certificat et des certificats Porteurs. Ceci s'applique bien entendu uniquement aux applications pour laquelle l'AC a connaissance de leur utilisation de ses certificats et avec lesquelles elle a signé un accord en ce sens.

Elle doit enfin signaler l'imminence de la révocation de son certificat à toute entité lui ayant attribué une quelconque accréditation, qualification,.....

5.8.3.2 Etape 2 : Révocation des certificats Porteurs

L'AC doit révoquer l'ensemble des certificats qu'elle aura générés et en avertir les Porteurs.

5.8.3.3 Etape 3 : Révocation du certificat de l'AC

L'AC doit faire une demande de révocation de son certificat à l'AC Certeurope Root CA.

L'AC Certeurope Root CA doit révoquer le certificat de signature de l'AC AC @vocats Classe 3Plus et mettre à jour sa LCR.

5.8.4 Délai de traitement

La révocation des certificats des composantes de l'ICP doit avoir lieu dans les plus brefs délais. Eut égard à l'importance de l'impact (révocation de l'ensemble des Certificats) les vérifications les plus approfondies devront être menées pour s'assurer de la justesse de la demande de révocation du certificat de l'AC AC @vocats Classe 3Plus.

5.9 Journalisation des événements

La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés.

Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité ainsi que de s'assurer que la séparation des fonctions est effective. Ce système permet également de collecter des preuves et de détecter des anomalies. La journalisation des événements est protégée, sauvegardée, intègre et fait l'objet de règles strictes d'exploitation.

Les actions de journalisation sont décrites précisément dans la DPC et abordent notamment les thèmes suivants :

- événements enregistrés par l'AC ;

AC @vocats Classe 3Plus

Politique de Certification

- processus de journalisation des événements ;
- collecte des journaux d'événements (interne ou externe) ;
- conservation des journaux d'événements ;
- protection des journaux d'événements ;
- anomalies et audit ;
- imputabilité.

5.9.1 Information enregistrées

Ces enregistrements d'événements devront contenir au minimum les champs suivants, s'ils sont pertinents :

- type d'opération ;
- destinataire de l'opération ;
- nom du demandeur de l'opération ;
- nom de l'exécutant ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- date et heure de l'opération ;
- cause de l'évènement
- résultat de l'évènement (échec ou réussite).

5.9.2 Imputabilité

L'objectif principal de la journalisation est de permettre d'imputer toute action à son auteur que ce soit une personne physique ou un système.

5.9.3 Evènements enregistrés par l'AE

L'AE doit consigner au moins les évènements suivants :

- demandes de certificats ;
- demandes de révocation ;
- sollicitation et accusés de réception de l'AC.

5.9.4 Evènements enregistrés par l'AC

Les évènements suivants seront enregistrés par l'AC, ce sont essentiellement des évènements générés par des systèmes informatiques :

- tous les événements ayant trait à la sécurité des systèmes informatiques impliqués dans l'ICP ;
- demandes de certificats ;

AC @vocats Classe 3Plus

Politique de Certification

- demandes de révocation ;
- démarrage et arrêt des systèmes informatiques ;
- démarrage et arrêt des applications ;
- opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système d'exploitants privilégiés ;
- génération des clés de ses composantes ;
- la génération et la révocation de certificats ;
- changements des caractéristiques de l'AC et (ou) de ses composantes ;
- la publication de la LCR;
- événements relatifs aux supports cryptographiques (génération des données d'activation à enregistrer).

5.9.5 Evènements divers

D'autres évènements non issus de systèmes informatiques mais essentiels pour la sécurité de l'AC, doivent être enregistrés, ce sont en particulier :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration du système ;
- les changements apportés au personnel ;
- les actions de destruction : des supports contenant des clés, des données d'activation ou des renseignements personnels sur les Abonnés.

5.9.6 Processus de journalisation

Le processus de journalisation est effectué en tâche de fond et permettre un enregistrement en temps réel des opérations effectuées. Le processus de journalisation est conçu de façon à être incontournable.

En cas de saisie manuelle l'écriture se fait dans le même jour ouvré que l'évènement.

5.9.7 Protection d'un journal d'évènements

L'écriture dans les journaux d'évènements est conditionnée par des contrôles de droits d'accès. Les enregistrements et l'horloge des composantes de l'ICP sont protégés contre les tentatives non autorisées de modification et de destruction.

5.9.8 Copies de sauvegarde des journaux d'évènements

Aucune exigence n'est stipulée.

5.9.9 Système de collecte des journaux (interne ou externe)

L'enregistrement des événements commence au démarrage des systèmes concernés par les événements à enregistrer et se termine à l'arrêt de ces systèmes.

5.9.10 Anomalies et audit

Les composantes de l'AC responsables de la fonction de journalisation sont en mesure de détecter toute tentative de violation de l'intégrité du système de gestion des certificats, y compris les équipements physiques, l'environnement d'exploitation et le personnel.

Les journaux d'événements journaliers sont contrôlés pour identifier des anomalies liées à des tentatives en échec.

Les journaux sont revus avec une fréquence hebdomadaire. Cette révision donnera lieu à un résumé dans lequel les éléments importants sont analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Les mesures à prendre à la suite de ces analyses sont documentées dans la DPC.

5.10 Archives

L'archivage est réalisé par l'AE et l'AC dans le but d'assurer la continuité de service, l'auditabilité et la non-répudiation des opérations.

Les mesures nécessaires sont mises en place par l'AE et l'AC afin que ces archives soient disponibles, exploitables, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

5.10.1 Types de données à archiver

Doivent être archivées au minimum, les données suivantes

- les logiciels et les fichiers de configuration des équipements informatiques de l'ICP ;
- la PC et la DPC ;
- les agréments contractuels ou les conventions avec d'autres AC ;
- les journaux d'événements ;
- les certificats tels qu'émis ;
- les LCR telles qu'émisses ou publiées ;
- les notifications de révocation ;
- le DDS de l'Abonné ou du MC.

5.10.2 Protection des archives

Les archives doivent être protégées durant leur conservation, cette protection concerne :

- leur intégrité ;
- leur confidentialité ;
- leur lisibilité.

Les moyens mis en œuvre pour atteindre ce triple objectif seront décrits dans la DPC

AC @vocats Classe 3Plus

Politique de Certification

5.10.3 Période de rétention des archives

5.10.3.1 Certificats et LCR

Les LCR produites par l'AC sont archivées pendant au moins cinq ans après l'expiration du certificat de l'AC.

Les certificats générés par l'AC sont archivés pendant 5 ans après leur expiration.

Les moyens mis en œuvre pour atteindre cet objectif seront décrits dans la DPC

5.10.3.2 Dossier de demande de certificat

Tout dossier de demande de certificat est archivé pendant trois (3) ans après l'expiration du certificat

Les moyens mis en œuvre pour atteindre cet objectif sont décrits dans la DPC

5.10.3.3 Journaux d'évènements

Les journaux de l'AC seront pendant au moins cinq ans après l'expiration du certificat de l'AC.. Bien entendu le triple objectif de confidentialité, intégrité, lisibilité est maintenu durant leur conservation.

Les moyens mis en œuvre pour atteindre cet objectif sont décrits dans la DPC

5.10.3.4 Autres journaux

Aucune exigence n'est stipulée.

5.10.4 Duplication des archives

Les archives des journaux de l'AC sont dupliqués afin d'en augmenter la disponibilité.

5.10.5 Horodatage des enregistrements

Les enregistrements des certificats et des LCR sont horodatés conformément à la politique de sécurité de l'AC en matière d'horodatage des évènements.

5.10.6 Procédure de collecte des archives

Aucune exigence n'est stipulée.

5.10.7 Procédure de récupération des archives

Hormis l'AC qui a nécessairement accès à toutes les archives, une composante de l'ICP ne peut récupérer et consulter que ses propres archives.

Le processus de récupération fait l'objet d'une procédure et figure dans la DPC.

Une archive peut être récupérée sous un délai inférieur à 2 jours ouvrés.

Les procédures sont décrites dans la DPC

5.11 Cessation d'activité de l'AC

5.11.1 Transfert d'activité

Si l'AC décide de transférer son activité de certification, elle doit tout d'abord en informer les applications utilisatrices et les Abonnés dans un délai de 4 mois avant le transfert effectif d'activité.

Elle doit également informer les applications utilisatrices et les utilisateurs des modifications liées à ce transfert d'activité..

Les archives de l'AC devront être reprises en charge par la société reprenant l'activité.



AC @vocats Classe 3Plus

Politique de Certification

5.11.2 Cessation définitive

En cas de cessation définitive d'activité, l'AC AC @vocats Classe 3Plus procède comme indiqué au 5.8.3. L'AC AC @vocats Classe 3Plus respectera un délai de 3 mois entre les étapes 1 et 2.

6 CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES, CONTROLE DU PERSONNEL

Les différents contrôles décrits ici visent, par une gestion des risques adéquate, à assurer un niveau de confiance fort dans le fonctionnement de l'AC AC @vocats Classe 3Plus.

6.1.1 Situation géographique

Aucune exigence n'est stipulée.

6.1.2 Accès physique

Les zones hébergeant les systèmes informatiques de l'AC AC @vocats Classe 3Plus sont physiquement protégées contre un accès extérieur non autorisé.

La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

6.1.3 Energie et air conditionné

Les installations électriques et de conditionnement d'air sont suffisantes pour le bon fonctionnement des systèmes informatiques de l'AC AC @vocats Classe 3Plus

6.1.4 Exposition aux liquides

Les systèmes informatiques de l'AC AC @vocats Classe 3Plus ne sont pas situés en zone inondable, ni du fait d'intempéries, ni du fait de tuyauteries défaillantes.

6.1.5 Sécurité incendie

Les locaux d'hébergement des systèmes informatiques de l'AC AC @vocats Classe 3Plus sont protégés contre les incendies (détection et extinction automatiques). La distribution des machines permet par ailleurs d'assurer une disponibilité maximale aux services.

6.1.6 Site de secours

Afin d'assurer l'accès aux services de certification/révocation même en cas de désastre sur le site de production des mesures doivent être prises. Ces mesures doivent permettre la reprise des activités de l'AC AC @vocats Classe 3Plus dans les plus brefs délais.

L'accès à la LCR est maintenu quoiqu'il advienne grâce à une réplication permanente de la LCR sur 2 sites physiquement distincts.

L'accès à l'ensemble des services (état nominal) fait l'objet d'un plan de reprise d'activité.(PRA).

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

6.1.7 Conservation des médias

Les médias contenant des données sauvegardées ou archivées sont conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

Les moyens mis en œuvre pour atteindre cet objectif sont précisés dans la DPC.

6.1.8 Destruction des supports

La destruction des supports sera assurée avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

AC @vocats Classe 3Plus

Politique de Certification

6.1.9 Sauvegarde hors site

L'organisation des sauvegardes des information sera adaptée de façon à assurer une reprise après désastre la plus rapide possible, en particulier pour les services impliqués dans la révocation de certificats.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

6.2 Contrôles des procédures

Des contrôles des procédures sont mis en place par l'AC AC @vocats Classe 3Plus et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

6.2.1 Rôles de confiance

L'AC AC @vocats Classe 3Plus s'appuie sur du personnel réparti en 5 catégories (rôles)

- ingénieur système : mise en place et maintenance des systèmes ;
- administrateur sécurité gestion de la sécurité des systèmes ;
- opérateur : exploitation basique du système ;
- responsable sécurité : Application de la politique de sécurité ;
- responsable qualité : assurance de la qualité des services rendus par l'AC AC @vocats Classe 3Plus.

Les attributions nominatives de chaque rôle sont décrites dans la DPC.

6.2.2 Nombre de personnes nécessaires à l'exécution de tâches sensibles

Selon la tâche à effectuer un ou plusieurs personnes devront être présentes lors de l'exécution de la tâche.

La DPC précisera pour chacune des tâches liées à la gestion des certificats le nombre et le rôle de personnes nécessaires.

6.2.3 Identification et authentification des rôles

Chaque composante de l'AC doit vérifier l'identité et les autorisations de son personnel devant intervenir, avant :

- que son nom soit ajouté aux liste des personnes ayant accès physiquement aux systèmes informatiques de l'AC. ;
- qu'un compte lui soit ouvert dans les systèmes informatique de l'AC AC @vocats Classe 3Plus.

6.3 Contrôle du personnel

6.3.1 Passé professionnel, qualifications, expérience, et exigences d'habilitations

L'AC AC @vocats Classe 3Plus vérifie le passé professionnel de la personne et son adéquation aux exigences de la gestion de l'AC AC @vocats Classe 3Plus

L'AC AC @vocats Classe 3Plus informera toute personne intervenant dans la Gestion de l'AC AC @vocats Classe 3Plus de ses responsabilités relatives aux services de l'AC ainsi que des procédures liées à la sécurité.

AC @vocats Classe 3Plus

Politique de Certification

L'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC:

- sont nommés à leur poste par écrit ;
- sont tenus par contrat ou par la loi de respecter les obligations, notamment de confidentialité, du poste qu'ils occupent ;
- n'ont pas de tâches ou d'intérêts susceptibles d'entrer en conflit avec les obligations qui leur incombent à l'égard de l'AC.

6.3.2 Procédures de contrôle du passé professionnel

Les précisions seront données dans la DPC.

6.3.3 Exigences de formation

L'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches touchant la gestion de l'AC ont reçu une formation adaptée concernant les principes de fonctionnement et des mécanismes de sécurité de l'AC, et sont familiarisés aux règles de sécurité en vigueur.

6.3.4 Fréquence des formations

Les précisions seront données dans la DPC.

6.3.5 Gestion des métiers

Les précisions seront données dans la DPC.

6.3.6 Sanctions pour des actions non-autorisées

Sur faute avérée ou soupçonnée d'un membre de l'AC dans l'accomplissement de ses tâches, l'AC lui interdit l'accès aux systèmes et, le cas échéant, prend toute sanction disciplinaire adéquate.

6.3.7 Contrôle des personnels contractants

Les précisions seront données dans la DPC.

6.3.8 Documentation fournie au personnel.

L'AC doit s'assurer que son personnel dispose de l'accès à toute loi, ou tout contrat qui s'applique aux postes occupés.

Les documents dont doit disposer le personnel sont notamment les suivants :

- la PC supportée par la composante à laquelle il appartient ;
- la DPC propre au domaine de certification ;
- les procédures internes de fonctionnement ;
- les documents constructeurs des matériels et logiciels utilisés.

7 CONTROLES TECHNIQUES DE SECURITE

7.1 Génération et installation de bi-clés

7.1.1 *Génération des bi-clés de Porteur*

Les clés issues de l'AC AC @vocats Classe 3Plus ont comme usage au sens X509 du terme :

- La signature électronique et la non répudiation;

Dans la procédure de génération de clés pour les Certificats @vocat, l'AE génère le bi-clé sur le module cryptographique en présence du Porteur. La clé privée n'est donc jamais accessible ou utilisable ni par l'AC ni par l'AE.

Le code d'activation du module est transmis par l'AC au porteur, l'AE n'a donc jamais connaissance de ce code

Le Porteur est par suite réputé assumer l'entière responsabilité de toutes les signatures exécutées avec sa clé privée.

7.1.2 *Transmission de la clé publique de signature (du Porteur) à l'AC*

Les clés publiques du porteur sont transmises à l'AC avec les informations nominatives que le certificat comportera via un protocole d'échange qui en assure l'intégrité. La DPC précise les modalités de cette transmission.

7.1.3 *Fourniture d'un Certificat d'AC*

La clé publique de l'AC est téléchargeable gratuitement sur le site Internet de l'AC <http://www.avocat-conseil.fr/reference/Avocats.der> (XXXXXX A valider), elle est de plus stockée sur le module cryptographique du Porteur ?

L'empreinte du Certificat de la clé publique de l'AC permet d'en établir l'authenticité.

7.1.4 *Tailles des clés*

Les clés RSA des Porteurs utilisées ont une taille de 1024 bits. Cette taille sera augmentée au fur et à mesure de l'évolution de la technique et/ou de la législation.

La taille de la clé RSA de l'AC AC @vocats Classe 3Plus est de 2048 bits.

La taille de la clé RSA de l'AC CertEurope Root CA est de 2048 bits.

7.1.5 *Paramètres de génération des clés*

Les modules cryptographiques des Porteurs utilisent des paramètres standard ou normalisés pour garantir l'aspect aléatoire de la génération des bi-clés.

7.1.6 *Contrôle de la qualité des paramètres des clés*

Les modules cryptographiques des Porteurs vérifient la qualité des bi-clés qu'ils génèrent.

7.1.7 *Mode de génération du biclé de l'AC*

Le bi-clé de l'AC (pour la de signature de certificats et de CRLs) est généré et protégé par un module cryptographique matériel.

Ce module est certifié selon les Critères Communs avec assurance EAL4+ au moins ou selon les critères FIPS 140-1 niveau 4

AC @vocats Classe 3Plus

Politique de Certification

La génération ou le renouvellement du bi-clé de l'AC par ce module nécessite la présence d'au moins 2 personnes.

7.1.8 Usage de la clé publique des Porteurs

Les bi-clés associés aux certificats de signature générés par l'AC AC @vocats Classe 3Plus ne sont utilisables que pour la signature et la non-répudiation. Ces usages sont précisés dans le champ keyUsage des certificats @vocat; ce champ a donc les valeurs **digitalSignature** et **nonRépudiation**.

7.2 Protection de la clé privée

7.2.1 Dispositifs de gestion des éléments secrets du Porteur

Le bi-clé du Porteur est généré par et stocké sur sa module cryptographique. Un code d'activation (code PIN fourni au porteur par l'AC AC @vocats Classe 3Plus) protège l'accès à la clé privée. Le Porteur est responsable de la confidentialité du code PIN lié à sa clé privée.

7.2.2 Contrôle de la clé privée de signature de l'AC par plusieurs personnes

Le contrôle des clés privées de l'AC AC @vocats Classe 3Plus (pour la signature de certificats et de CRL) nécessite la présence de plusieurs personnes.

7.2.3 Récupération de clé privée de confidentialité* du Porteur.

L'AC AC @vocats Classe 3Plus n'offre pas de service de recouvrement de clé.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques des Porteurs

Les clés publiques des Porteurs sont contenues dans les certificats et donc conservées conformément au chapitre 5.10.3.1..

7.3.2 Durée de vie des Certificats

La durée de vie des Certificats fournis dans le cadre de AC @vocats Classe 3Plus est de 4 ans.

7.4 Code PIN des Porteurs

7.4.1 Génération et utilisation des codes PIN

Les modules cryptographiques sont fournis aux Abonnés protégés par un code PIN. Le code PIN est défini par l'AC de façon à le rendre imprévisible.

Une fois envoyé ce code est détruit et ne sera pas récupérable.

7.4.2 Protection des codes PIN

Il est de la responsabilité du Porteur de protéger les clés privées de son bi-clés. Le code PIN doit être considéré par le Porteur comme confidentiel.

L'AC ne conserve pas les codes PINs des Porteurs au delà de leur envoi au Porteur

7.5 Sécurité des postes de travail des composantes de l'ICP

Les postes de travail des composantes de l'ICP nécessitent un niveau de sécurité optimal, ce niveau est défini dans la DPC et permet de satisfaire les besoins suivants

- identification et authentification des utilisateurs du poste

AC @vocats Classe 3Plus

Politique de Certification

- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'Utilisateur),
- protection contre les virus informatiques,
- protection du réseau (confidentialité, intégrité...)
- imputabilité

Le niveau minimal d'assurance recherché doit au moins répondre à ces objectifs de sécurité. Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires, à prendre en compte dans la recherche du niveau minimal d'assurance offert par les postes de travail.

7.6 Contrôles techniques du système durant son cycle de vie

7.6.1 Contrôles des développements des systèmes

Les applications de l'AC ont été implémentées dans le strict respect de l'analyse de risque préalable et de la politique de sécurité qui en découle.

L'implémentation de l'AC et de la plate-forme qui l'héberge est documentée.

Toute modification de l'AC et de la plate-forme qui l'héberge est documentée

7.6.2 Contrôles de la gestion de la sécurité.

Toute évolution des systèmes est enregistrée sur le livre d'activité de l'AC et fait l'objet d'un rapport.

7.7 Contrôles de la sécurité réseau

L'AC est implantée sur une réseau protégée par au moins deux niveaux de passerelles de type « coupe-feu ». Ces passerelles sont configurées de façon à n'accepter que les flux strictement nécessaires.

7.8 Contrôles des modules cryptographiques

Les modules cryptographiques utilisés par l'AC sont évalués selon les critères FIPS 140-1 au niveau 4.

AC @vocats Classe 3Plus

Politique de Certification

8 PROFILS DE CERTIFICATS ET DE LCR

8.1 Profil des Certificats

Les Certificats de l'AC AC @vocats Classe 3Plus contiennent les champs primaires et les extensions suivantes :

Champ	Valeur	Détail valeur	Explications
Version	V3	2	Version du Certificat X.509
Numéro de série	1506 38D4 36F3 K231 C692 B849 E3F7 B943		Le numéro de série unique du Certificat attribué par le module cryptographique
Algorithme de signature	Sha1RSA = 1.3.14.3.2.29		Identifiant de l'algorithme de signature de l'AC
Emetteur	/C=FR /O=CNB /CN= AC @vocats Classe 3Plus	XXXXXX Avérier	Le nom de l'AC émettrice est le Distinguished Name (X.500) de l'AC signant les Certificats
Valide à partir du	19 Juillet 2005 00:00:00		Dates et heures d'activation et d'expiration du Certificat
Valide jusqu'au	23 Mai 20014 00:00:00		
Objet	E = emartin@societe.fr CN = ERIC MARTIN OU = 123456 O = 0002 123456789 L = LILLE C = FR		Nom distinctif de l'entité identifiée
Clé publique	RSA(1024 Bits)	7C28 8902 8181 3963 8424 B08C CD71 9110 7E44 2B2E 8014 35F0 49CE B4D2 8CA9 3516 5FC7 9EB8 9A89 637C 20C4 DB30 97AF ECB3 37F2 A000 00E8 E350 BA90 2B20 EEE5 9D5B 4A87 E0D5 895A B6A4 05A6 B2C4 2715 555F 3081 0A68 95AD 00CF 6071 4C00 8431 7693 7EC0 20F9 8C31 EC2A 8585 9054 3478 4DD1 366B 9024 67B7 E8C8 C812 6EE9 E35B 5D04 700D 6699 2702 0301 0001	Identifiant de l'algorithme d'usage de la clé publique contenue dans le Certificat, et valeur de la clé publique
Contrainte de base	Subject Type=End Entity Path Length Constraint=None		
Point de distribution de la LCR	CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://lcr1.avocat-conseil.fr/CN= AC @vocat Classe 3Plus, O=CNB, C=FR?CertificateRevocationList URL=ldap://lcr2.avocat-conseil.fr/CN= AC @vocat Classe 3Plus, O=CNB, C=FR?CertificateRevocationList URL=http://www.avocat-conseil.fr/reference/Avocats.crl		
Certificate Policies	Certificate Policy: PolicyIdentifier=1.2.250.1.148.3.1 Policy Qualifier Info: Policy Qualifier Id= Qualifier=	OBJECT IDENTIFIER ' XXXXXX Avérier OBJECT IDENTIFIER cps http://www.avocat-conseil.fr/reference/Avocat_V1.0.pdf	Identifiant de la Politique de Certification
2.16.840.1.113733.6.1.9	01 01 FF		
Algorithme d'empreinte numérique	Sha1 = 1.3.14.3.2.29		
Empreinte numérique	07F2 AC3F 4E3A 30D5 277C 2A1A 6AD2 6BA4 F019 E130	8C 62 E9 57 0B 94 DF EB 73 14 AE 15 0F A9 36 2B 22 84 81 28 0F 25 06 FF 1C D3 10 EC A5 BC 43 1C AB 02 1D CD 7E 9E D7 B9 A0 DA 13 59 22 26 DF 72 EB 6D B3 AA 4E 2C B0 B3 1B 38 A4 E5 C4 3A 4C 15 2F E2 B2 AD 1C 9D 8F 5A FE D6 05 BC 6D 2E 81 D4 67 96 3D 74 BB F1 3F 37 7C 27 75 8C 9A 9A 9D 56 63 F1 BD 1E 76 89 09 ED 71 AA E1 F0 65 E1 A5 C8 0E DC AE 50 E1 C6 0D BF 76 6F A8 EC D0 D7 55 B9	Champ d'octets caractérisant le Certificat de l'AC ayant signé le Certificat

8.2 Profil de LCR

8.2.1 Champs des LCR

Les LCR de l'AC AC @vocats Classe 3Plus contiennent les champs suivants :

- Version : la version de la LCR. Dans le cadre de la présente AC, il s'agit de la version 2;
- Signature : l'identifiant de l'algorithme de signature de l'AC soit Sha1-RSA ;
- Issuer : le nom de l'AC émettrice qui signe les Certificats soit l'AC AC @vocats Classe 3Plus ;
- ThisUpdate : date de génération de la LCR ;
- NextUpdate : prochaine date à laquelle cette LCR sera mise à jour ;
- RevokedCertificates : liste des numéros de série des Certificats révoqués ;
- UserCertificate : numéro de série de Certificat révoqué ;
- RevocationDate : date à laquelle un Certificat donné à été révoqué.
- crlExtensions : liste des extensions de la LCR.

8.2.2 Extensions des LCR

Les LCR de l'AC AC @vocats Classe 3Plus comportent deux extensions :

- authorityKeyIdentifier : cette extension non critique identifie la clé publique à utiliser pour vérifier la validité de la LCR. Cet identifiant a la même valeur que le champ SubjectKeyIdentifier des certificats émis par l'AC AC @vocats Classe 3Plus ;
- CRLNumber : cette extension non critique contient le numéro de série de la LCR.

9 ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente Politique de Certification.

9.1 Procédures de modification de la PC

Le responsable de l'AC doit signaler aux Porteurs et aux applications utilisatrices toute modification de la présente politique sans préavis.

9.1.1 *Causes de modification*

Cette PC devra être revue en raison de projets de modifications suivants :

- les certificats référencés ;
- la composition de l'AC ;
- à chaque modification des documents de référence de l'AP ainsi que chaque année pour assurer sa conformité aux normes de sécurité et à l'évolution des mises en œuvre du marché.

9.1.2 *Délai de préavis*

Le responsable de l'AC doit donner un préavis de trente (30) jours aux Porteurs et aux applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, a un impact majeur sur eux.

Le responsable de l'AC doit donner un préavis de quinze (15) jours aux Porteurs et aux applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact mineur sur eux.

Le responsable de l'AC doit donner un préavis aux Porteurs et aux applications utilisatrices dans les sept (7) jours d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, si ce changement ait un impact sur eux.

En cas de changement intervenant dans la composition de l'AC ou de la présente Politique de Certification, l'AC doit prévenir ses clients :

- au plus tard un mois avant le début de l'opération si elle a un impact sur le niveau de qualité et de sécurité des fonctions de l'AC vis à vis des certificats référencés ;
- au plus tard un mois après la fin de l'opération s'il n'y a pas d'impact.

9.2 Procédures de publication et de notification

La PC est disponible depuis la source suivante : http://www.avocat-conseil.fr/reference/Avocats_v1.0.pdf (XXXX A vérifier)

9.3 Procédures d'approbation de la PC

L'approbation de la PC de l'AC est réalisée par l'AP qui notamment vérifie son adéquation aux documents de référence de l'AP, suivant une procédure de revue documentée.

La décision du Porteur de ne pas demander la révocation de son certificat suite à la notification d'un changement proposé constitue l'acceptation du changement.

10 ANEXE 1 – TEXTES LEGISLATIVES ET REGLEMENTAIRES

- Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive européenne 95/46/EC relative à la protection des données personnelles
- Directive européenne (1999/93/EC) relative à la signature électronique été adoptée le 13/12//1999
- Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- Décret no 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
- Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie dispensées de toute formalité préalable.
- Arrêté du 17 mars 1999 définissant la tome et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptographie.
- Arrêté définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fournitures d'un moyen ou d'une prestation de cryptographie, no PRMX9802730A du 13 mars 1998
- Arrêté définissant le modèle de notification préalable par le fournisseur des identités des intermédiaires utilisés pour la fourniture des moyens ou prestations de cryptographie soumis à autorisation, no PRMX9802732A du 13 mars 1998.