Autorité de Certification AC @vocats
Classe 3Plus

DECLARATION DES PRATIQUES DE CERTIFICATION

Date : 13/04/2011
Version : 2.0

Version	Date	Rédigée par	Validée par
2.0	13/04/2011	CertEurope	CNB

AC @vocats Classe 3Plus
Politique de Certification

Sommaire :

1 PREAMBULE

Ce document constitue la Déclaration des Pratiques de Certification de l'Autorité de Certification AC @vocats Classe 3Plus, c'est-à-dire la description des mesures effectivement prises pour assurer l'ensemble des obligations et engagements définis dans la Politique de Certification 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).

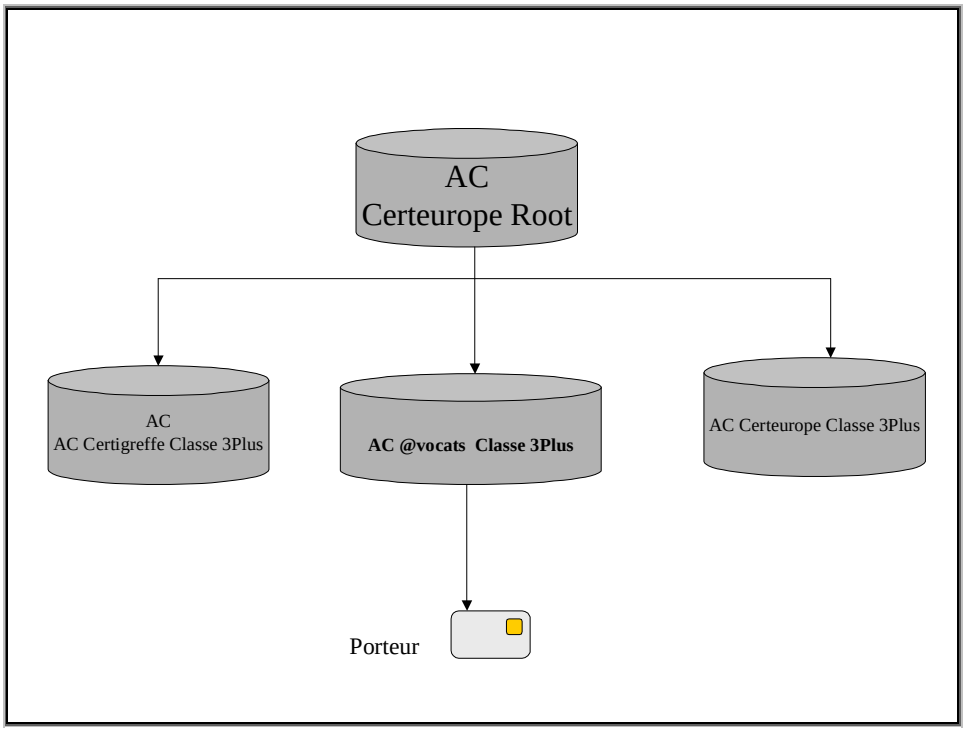
L'infrastructure à Clés Publiques repose sur les acteurs suivants :

- 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
Certeurope Root
AC
AC Certigreffe Classe 3Plus
AC @vocats Classe 3Plus
AC Certeurope Classe 3Plus
Porteur

2 PRESENTATION GENERALE DE LA DPC

2.1 Liste des acronymes utilisés

Voir PC même chapitre

2.2 Définitions des termes utilisés dans la PC

Voir PC même chapitre

2.3 Type d'applications concernées par la PC

Voir PC même chapitre

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

Voir PC même chapitre

2.5 Modification de la DPC

Cette DPC 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 DPC est deux ans. Les modifications sont réalisées conformément au chapitre 9 du présent document.

2.6 Identification de la DPC - OID

La présente Déclaration des Pratiques de Certification est identifiée par l'OID 1.2.250.1.148.3.2.1, elle est ci-après désignée sous le nom de "DPC"

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

22 rue de Londres

75009 Paris 9

FRANCE

2.7.2 Personne physique responsable

M. le Président du Conseil National des Barreaux

22 rue de Londres

75009 Paris 9

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

Voir PC même chapitre

3.1.2 Indépendance et qualifications du contrôleur

Voir PC même chapitre

3.1.3 Fréquence du contrôle de conformité

Voir PC même chapitre

3.1.4 Périmètre du contrôle de conformité

Voir PC même chapitre

3.1.5 Communication des résultats

Voir PC même chapitre

3.1.6 Actions entreprises en cas de non-conformité

- Voir PC même chapitre

3.2 Respect et interprétation des dispositions juridiques

3.2.1 Droit applicable

Voir PC même chapitre

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

Voir PC même chapitre

3.3 Obligations

3.3.1 Obligations de l'AC

Voir PC même chapitre

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;

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 ;

- 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.

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.

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

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 Divulgation des causes de révocation

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

3.7.3 Remise sur demande du propriétaire

L'AC AC @vocats Classe 3Plusne 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

Voir PC même chapitre

4.1.2 Nécessité d'utilisation de noms explicites

Voir PC même chapitre

4.1.3 Règles d'interprétation des différentes formes de noms

Voir PC même chapitre

4.1.4 Unicité des noms

L'unicité d'un Certificat est établie par l'unicité de son numéro de série. Ce numéro de série est défini par l'Autorité de Certification lors de la génération du certificat .La définition du numéro de série suit deux règles : le numéro de série est compris entre XXX et XXX, le numéro de série d'un certificat B généré après le certificat A est strictement supérieur au numéro de série du certificat A. La définition/modification de la plage d'adresse [XXXX ;XXXX] est décrite dans le document [3] Configuration de l'AC @vocats Classe 3Plus.

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. Il ne peut donc exister deux personnes ayant le même DN. De plus le serveur d'enregistrement avant de demander la génération d'un certificat vérifie dans l'annuaire de l'AC si un certificat ayant le même DN a déjà été généré et le signale à l'AE. Par contre il convient de préciser que plusieurs certificats ayant le même DN peuvent coexister. En effet les certificats de l'AC @vocats Classe 3Plus ayant vocation à devenir un outil essentiel pour les Avocats, il doit être possible pour un Porteur de demander un second certificat pour par exemple pallier sans aucun délai à une perte de support cryptographique.

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.

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 :

- un original d'une pièce d'identité officielle du mandataire de certification comportant sa photo et sa signature et en prend copie qu'elle marque de la mention « Copie conforme » et signe ;
- le 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.
- l'appartenance du demandeur au tableau de l'Ordre, cette appartenance est vérifiée soit à l'aide de l'outil utilisé par l'Ordre pour gérer le tableau, soit par consultation du tableau auquel cas l'AE prendra une copie du tableau qu'elle datera et signera.
- l'appartenance du demandeur à la personne morale dont le SIREN sera porté dans le certificat. Cette appartenance est vérifiée soit à l'aide de l'outil utilisé par l'Ordre pour gérer le tableau, soit par consultation du tableau auquel cas l'AE prendra une copie du tableau qu'elle datera et signera.
- Le N° CNBF : XXXX Comment le vérifie-ton ?
- le DDS

4.1.8.1 Contenu du dossier déposé par le demandeur

Chaque élément du DDS est vérifié comme suit ::

- preuve de l'appartenance du demandeur à la personne morale dont le SIREN sera porté dans le certificat
  - Soit vérification du courrier du représentant légal et de la copie d'un justificatif d'identité du représentant légal muni d'une photo (permis de conduire, carte d'identité nationale, passeport).
  - Soit vérification à l'aide de l'outil utilisé par l'Ordre pour gérer le tableau
- preuve que le numéro d'identification de la personne morale demandé est correct
  - soit vérification extrait Kbis ou avis SIRENE,
  - Soit vérification à l'aide de l'outil utilisé par l'Ordre pour gérer le tableau
- le contrat Porteur
  - vérification que la signature correspond bien à celle présente sur le justificatif d'identité du demandeur;
- la copie d'un justificatif d'identité
  - Vérification qu'il s'agit bien de la pièce justificative présentée. La mention « copie certifiée conforme » sera portée sur cette copie qui sera signée par l'AE et le demandeur;
- le prénom et le nom à utiliser dans le champ CN du certificat ;
  - Vérification que ces deux informations correspondent à celles du justificatif d'identité du demandeur
- l'adresse de courrier électronique du demandeur si elle est fournie dans le DDS.
  - Vérification que cette adresse ne comporte pas d'erreur syntaxique (caractères autres que les caractères ANSI, omission du signe @…..)

4.1.8.2 Contenu du dossier déposé par un MC

En sus des vérifications décrites au chapitre 0, et conformément au chapitre 4.1.7 l'AE vérifie les éléments d'identification propres au MC comme suit

- le mandat signé par le représentant légal de l'entreprise désignant le MC à qui le certificat doit être délivré, un modèle de ce mandat est accessible à l'adresse http://www.avocat-conseil.fr/reference/Mandat_MC.doc
- l'engagement signé par le MC, l'engageant à effectuer correctement les contrôles des dossiers des demandeurs ; un modèle de cet engagement est accessible à l'adresse http://www.avocat-conseil.fr/reference/Contrat_MC.doc

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 (chapitre 4.1.8.1);
- Par l'échange d'informations secrètes (le code de révocation d'urgence) entre le demandeur de la révocation (Porteur ou MC) et l'Autorité d'Enregistrement. Le processus de la définition du CRU et de son utilisation est décrit dans le document [4] La révocation d'urgence.

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

Voir même chapitre de la PC

5.1.2 Informations à fournir

Voir même chapitre de la PC

5.1.3 Procédure de demande

Les quatre étapes de la procédure peuvent s'enchaîner de deux façons

Cas de la génération du certificat en présence du demandeur :

- Etape 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.
- Etape 2 : Emission du module cryptographique (contenant son certificat et son bi-clé) par l'AE ;
- Etape 3 : Remise du module cryptographique en mains propres au Porteur ou au MC le représentant par l'AE ;
- Etape 4 : Envoi par l'AC par courrier postal du code PIN au Porteur.

Cas de la génération du certificat avant le face-à-face:

- Etape 1 : Emission du module cryptographique (contenant son certificat et son bi-clés) par l'AE ;
- Etape 4 : Envoi par l'AC par courrier postal du code PIN au Porteur.
- Etape 2: 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.
- Etape 3 : Remise du module cryptographique en mains propres au Porteur ou au MC le représentant par l'AE ;

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

Voir chapitre 4.1.8.1

5.1.6.2 Dossier du MC

Voir chapitre 4.1.8.2

5.1.7 Archivage des dossiers

Les dossiers des Porteurs sont archivés selon les mêmes procédures que pour les dossiers ordinaux des Avocats, cet archivage suit l'Avocat durant toute son appartenance au Barreau et même au delà XXXX A vérifier XXXX

Durant cinq ans, le DDS est consultable sur demande justifiée au Barreau dont dépend le Porteur, 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

En sus des vérifications détaillées aux chapitres 4.1.8.2 et 4.1.8.1, l'AE conformément au document [5] Guide de l'AE:

- se connecte au serveur d'enregistrement à l'aide du support cryptographique qui lui a été fourni lors de sa formation d'AE
- saisit les informations nominatives qui constitueront le DN
- saisit l'adresse postale du Porteur (pour l'envoi du code PIN)
- fait générer par un support cryptographique vierge le bi-clé du Porteur ;
- signe la demande de certificat à l'aide du support cryptographique qui lui a été fourni lors de sa formation d'AE;
- installe le certificat reçu de l'AC AC @vocats Classe 3Plus dans le support cryptographique ;
- remet le support cryptographique contenant la clé privée et le certificat au Porteur ou au MC ;
- archive le dossier (DDS) conformément à la procédure d'archivage.

Le MC, lui, remet le module cryptographique en mains propres au Porteur.

*5.1.9 Emission et distribution d'un **Certificat***

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

5.1.10 Acceptation d'un Certificat

La remise du support au Porteur vaut acceptation par celui-ci :

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

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

Voir même chapitre de la PC

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 tout 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

A la réception d'une demande de révocation, L'AE vérifie l'identité du demandeur. Cette vérification est réalisée

- Soit lors d'un face à face et se déroule de la même façon que pour l'authentification de la demande (voir chapitre 4.1.8.1)
- Soit par la fourniture de codes confidentiels, voir document [4] La révocation d'urgence

Si la demande est recevable, l'AE conformément au document [5] Guide de l'AE

- se connecte au serveur d'enregistrement à l'aide du support cryptographique qui lui a été fourni lors de sa formation d'AE
- recherche le certificat à révoquer dans l'annuaire en se basant sur les informations fournies par le demandeur
- signe la demande de certificat à l'aide du support cryptographique qui lui a été fourni lors de sa formation d'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 @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 trois 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

Voir même chapitre de la PC

5.6.2 Formes de publication des LCR

Les LCR sont au format dénommé "LCR V2".

L'accès à la Liste de Certificats Révoqués est possible via deux annuaires LDAP V3 et via un serveur http.

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 3 ans, le renouvellement de la clé de signature de l'AC devra intervenir au plus tard trois (3) 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, …).

Dans le cas où un nouveau bi-clé serait généré, celui-ci 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 notamment celles des AE 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.

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 précisée dans le contrat liant l'AE à l'AC AC @vocats Classe 3Plus.

Si la révocation fait suite à une demande de la part de la composante, celle-ci doit la faxer à l'AC accompagnée d'une photocopie d'une pièce d'identité afin que l'AC puisse s'assurer de la validité de la demande. Si la demande n'est pas recevable, l'AC en informe la composante.

Si la révocation est décidée unilatéralement par l'AC aucun contrôle particulier n'est réalisé.

Après validation de la demande, l'AC conformément au document [5] Guide de l'AE

- se connecte au serveur d'enregistrement à l'aide du support cryptographique particulier qu'elle détient aux fins de génération et de révocation de certificat de composantes.
- recherche le certificat à révoquer dans l'annuaire
- signe la demande de certificat à l'aide du support cryptographique particulier qu'elle détient aux fins de génération et de révocation de certificat de composantes
- 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.

La composante est notifiée de la publication de la révocation.

L'opération est enregistrée dans les journaux d'événements de 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 ;
- 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'événement (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 ;
- 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'événement.

5.9.7 Protection d'un journal d'événements

L'écriture dans les journaux d'événements 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. En particulier les journaux sont inaccessibles en dehors de la console des serveurs considérés.

5.9.8 Copies de sauvegarde des journaux d'évènements

Ces journaux sont par ailleurs dupliqués quotidiennement sur des serveurs distincts.

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.

Un ingénieur système analyse quotidiennement les journaux d'événement du serveur hébergeant l'AC ainsi que ceux du Serveur d'Enregistrement. Les enregistrements considérés comme normaux (dont la liste est donnée dans le document [6] Analyse des logs) sont masqués de façon à ne faire apparaître que les événements susceptibles de signaler une anomalie. Par corrélation entre ces journaux et en tenant compte des interventions réalisées dans le même laps de temps (par exemple un redémarrage est une vraie anomalie sauf si il a lieu après une intervention ayant nécessité le redémarrage des serveurs), seules les véritables anomalies sont remontées au RSSI, Pour traitement immédiat.

En fonction de son analyse de risque, le RSSI décide de l'action à mener s'il y a lieu.

5.10 Archives

5.10.1 Types de données à archiver

Sont archivées par l'AC sur support de type CD en double exemplaire, les données suivantes

- la PC et la DPC ;

- les logiciels et les fichiers de configuration des équipements informatiques de l'ICP ;

Sont archivés en recourant mensuellement aux services d'un Tiers Archiveur (Orsid) les données suivantes :

- les journaux d'événements ;
- les certificats tels qu'émis ;
- les LCR telles qu'émises ou publiées ;
- les notifications de révocation ;

Est archivé sous sa forme papier, le DDS de l'Abonné

5.10.2 Protection des archives

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

- leur intégrité ;
- leur confidentialité ;

La lisibilité des archives électroniques est garantie

- de première part par l'utilisation de formats standard pour ces données
  - PDF pour la PC/DPC/contrats…..
  - Texte brut : pour les journaux
  - X509 pour les Certificat et LCR
- de seconde part par la non utilisation d'outils de compression.
- de troisième part par la vérification régulière des supports optiques

La confidentialité des archives est garantie par des droits d'accès renforcés par rapport à ceux affectés à ces mêmes données avant leur archivage. Ainsi les archives des journaux, certificats, LCR et de la DPC ne sont accessibles qu'au RSSI de l'OSC, le contrôle d'accès est défini contractuellement avec le Tiers Archiveur.

La PC ne présente pas de caractère confidentiel.

Les fichiers de configuration des équipements informatiques de l'ICP ne sont accessibles qu'aux personnels de la Direction Technique de l'OSC ainsi qu'à son RSSI.

5.10.3 Période de rétention des archives

5.10.3.1 Certificats et LCR

Les LCR produites par l'AC sont archivées pendant 10 ans après leur génération.

Les certificats générés par l'AC sont archivés pendant 10 ans après leur génération.

Cette durée est contractuellement fixée entre l'OSC et le Tiers Archiveur.

5.10.3.2 Dossier de demande de certificat

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

Le DDS est partie intégrante du dossier de l'Avocat qui est géré par l'Ordre, en conséquence, ce dossier est conservé dans les archives de l'Ordre.

5.10.3.3 Journaux d'évènements

Les journaux de l'AC sont conservés pendant 10 ans.

Cette durée est contractuellement fixée entre l'OSC et le Tiers Archiveur.

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. La solution retenue par le Tiers Archiveur auquel sont envoyées les données à archiver inclut notamment la duplication des données sur 2 supports physiques distincts stockés en deux lieux distincts.

5.10.5 Horodatage des enregistrements

Les serveurs mis en œuvre pour l'AC @vocats Classe 3Plus ont leur horloge système synchronisée sur deux serveurs de temps hautement sécurisés, ces serveurs sont ceux de l'Autorité d'horodatage Certid@te, ils reçoivent via une liaison Hertzienne de type DCF 77 l'heure émise par atomique.

Ces serveurs de temps sont situés dans les mêmes locaux que les serveurs de l'ICP et étant redondant l'un de l'autre, ils assurent une continuité du service de temps notamment à destination des serveurs de l'ICP. Ainsi les heures inscrites dans les LCR, les Certificats et les Journaux d'événement sont elles fiables à 1s près (dérive maximum des serveurs de temps)

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.

Pour toute récupération de ses archives, la composante envoie sa demande par fax accompagnée d'une copie d'une pièce d'identité. Après authentification de la demande, l'AC la retransmet à l'OSC qui demandera la restitution des archives concernées au Tiers Archiveur.

Une fois ces Archives restituées, l'AC les transmet à la composante les ayant demandées.

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.

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 situé 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.

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.

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 clés privée n'est donc jamais accessible ou utilisable ni par l'AC ni par l'AE.

Le code d'activation du module est transmis part 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/ac_avocats_classe_3Plus_v2.crt, 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

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

- 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.

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 :

Voir PC même chapitre.

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

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 ANNEXE 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.

Liste des documents référencés

[1] Politique de Certification

[2] Procès Verbal de la cérémonie des clés.

[3] Configuration de l'AC @vocats Classe 3Plus

[4] La révocation d'urgence

[5] Guide de l'AE

[6] Analyse des logs