Représentant les avocats d'Europe
Representing Europe's lawyers

NORMES TECHNIQUES POUR UNE INTEROPERABILITE DES CARTES D'IDENTITE ELECTRONIQUES

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.eu – www.ccbe.eu

Normes techniques pour une interopérabilité des cartes d'identité électroniques

1. Introduction **3**
1.1. Vue d'ensemble 3
1.2. Identification 5
1.3. Groupe d'utilisateur et application 6
1.4. Contacts 6

2. Dispositions d'ordre général **7**
2.1. Obligations 7
2.2. Responsabilité 7
2.3. Responsabilité financière 7
2.4. Interpretation et application 7
2.5. Prix 8
2.6. Publication et service de dépositaire 8
2.7. Contrôle de conformité 9
2.8. Confidentialité et protection des données 9
2.9. Droits sur la propriété intellectuelle 9

3. Identification et authentification **10**
3.1. Enregistrement initial 10
3.2. Renouvellement de clés 10
3.3. Re-génération de clés après révocation 11
3.4. Demande de révocation 11

4. Besoins opérationnels **12**
4.1. Demande de certificat 12
4.2. Génération du certificat 12
4.3. Acceptation d'un certificat 12
4.4. Suspension et révocation du certificat 12
4.5. Audit sécurité 13
4.6. Archives 13
4.7. Changement de clé 13
4.8. Compromission et plan anti-sisnistre 13
4.9. Fin de vie d'une AC 13

5. Contrôles de sécurité physique, contrôle des procédures et contrôle du personnel **14**

6. Contrôles techniques de sécurité **15**
6.1. Génération et installation de bi-clés 15
6.2. Protection de la clé privée 16
6.3. Autres aspects de la gestion des bi-clés 16
6.4. Données d'activation 16
6.5. Contrôles de sécurité des postes de travail 16
6.6. Contrôles de sécurité durant son cycle de vie 16
6.7. Contrôles techniques des modules cryptographiques 16

7. Profils des certificats et LRC **17**
7.1. Profil des certificats 17
7.2. Profil des LCR 18

8. Administration des spécifications **19**
8.1. Procédure de modification de ces spécifications 19
8.2. Politiques de publication et de notification 19

Annexe 1 ACRONYMES 20

1. Introduction

1.1. Vue d'ensemble

1.1.1. Le rôle du CCBE

Le Conseil des barreaux européens (CCBE) représente plus de 700.000 avocats européens à travers ses barreaux membres de l'Union européenne et de l'Espace économique européen. Outre ceux-ci, il inclut également des représentants de barreaux associés (des pays candidats à l'adhésion à l'UE) et observateurs d'autres pays européens.

Les objectifs du CCBE sont :

1. la représentation des barreaux membres, qu'ils soient effectifs ou observateurs, dans toutes les matières d'intérêt commun ayant trait à l'exercice de la profession d'avocat, au respect de l'Etat de droit et d'une bonne administration de la justice ainsi qu'aux développements importants du droit, tant au plan européen qu'international,
2. le rôle d'organe consultatif et intermédiaire entre ses membres, qu'ils soient effectifs ou observateurs, et entre ses membres et les institutions de l'Union européenne et de l'Espace économique européen dans toutes les matières transfrontalières d'intérêt commun reprises ci-dessus,
3. le respect de l'Etat de droit, des droits de l'homme et de la protection des droits et libertés fondamentales, en ce compris le droit à l'accès à la justice et la protection du client, ainsi que la protection des valeurs démocratiques intimement liées à l'exercice de tels droits.

En sa qualité d'organe représentatif des barreaux nationaux en Europe, le CCBE est le plus à même d'établir des normes communes/minimales pour l'identification des avocats sur Internet.

Le présent document détermine les exigences minimales qui devraient être respectées par les autorités de certification du barreau national qui identifient les avocats qui y sont inscrits à travers des certificats qualifiés sur Internet. Cette politique s'appelle « le certificat numérique qualifié pour les avocats ».

Ce document suivra les exigences établies dans la *Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques* (ci-après dénommée « la directive ») et les normes standards du RFC 2527 - *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework* et s'appuiera sur les spécifications techniques de la politique de l'ETSI TS 101 456 V1.2.1 (2004-2004) sur les exigences politiques pour les autorités de certification délivrant des certificats qualifiés.

La détention de toutes les marques et noms de propriété appartenant à des tiers est reconnue lorsque mentionnée dans le présent document.

1.1.2. Concept principal de la politique du CCBE

Comme indiqué déjà dans la proposition cadre du CCBE dont la présente politique sert d'annexe, le CCBE promeut l'insertion de puces à utiliser pour la création de signatures numériques dans sa propre carte européenne pour les avocats européens, et encourage l'usage des cartes d'identités électroniques au niveau européen. Pour une interopérabilité des cartes d'identité électroniques au niveau européen, le CCBE devrait être constitué comme une autorité compétente qui vérifie que les conditions nationales des cartes d'identité électroniques délivrées correspondent aux normes européennes et peuvent être reconnues pour l'exercice transfrontalier[1]. Une des fonctions

[1] L'expression "autorité compétente" ne vise pas à indiquer que le CCBE devrait délivrer un certificat numérique. L'expression « autorité compétente » tel qu'utilisée dans le présent document renvoie à un rôle technique plutôt que juridique pour le CCBE. Le CCBE, avec l'approbation de la présente politique créera uniquement des normes techniques communes pour évaluer et vérifier les politiques nationales de l'autorité nationale de certification. Ceci permettra à un avocat français disposant d'un certificat français d'avoir la garantie que sa politique respecte les normes du CCBE et fera confiance à un autre pays auquel le CCBE a accordé sa confiance dans le cadre de la politique européenne.

principales des cartes d'identité électroniques sont les certificats numériques pour lesquels la présente police établit une norme technique commune.

Une introduction, reprenant la politique du CCBE et n'entrant pas dans tous les détails techniques, est reprise dans les paragraphes suivants[2]. Certains des termes utilisés sont expliqués plus amplement dans la suite du document (voir table des matières).

L'utilisation des certificats numériques et des signatures numériques est généralement soutenue par une **infrastructure à clé publique (ICP)**. Une ICP est un système comprenant du matériel informatique, des logiciels, des personnes, des processus et des politiques sous-tendant l'utilisation de la **cryptographie à clé publique** (décrite ci-dessous) pour fournir différents services de sécurité et d'assurance. Plus précisément, une ICP cherche à établir des communications électroniques, transactions sécurisées et/ou des informations en assurant qu'elle inclut :

- des méthodes fiables pour authentifier l'identité et l'autorité des personnes et organisations communiquant par voie électronique ou leurs attributs[3] ;
- des méthodes fiables pour fournir des assurances d'intégrité des communications et archives électroniques et détecter la corruption ou des modifications non autorisées de celles-ci ;
- des méthodes fiables pour protéger les messages et archives électroniques de l'interception, de l'accès non autorisé et de la divulgation d'informations confidentielle ou sensibles contenues dans celles-ci ;
- des méthodes fiables pour contrôler l'accès aux informations sensibles et veiller à ce que seules certaines parties, certaines personnes dûment autorisées ou parties avec des attributs spéciaux puissent y accéder ;
- La collecte de preuves persuasives importantes pour empêcher les parties de refuser avec succès des transactions électroniques ;
- l'adéquation des technologies particulières, dont la technologie de l'ICP, avec les mandats juridiques émergents.

Les certificats numériques sont créés et vérifiés par cryptographie, un domaine de mathématique appliquée qui concerne la transformation des messages en des formes apparemment illisibles et l'inverse. Les signatures numériques utilisent ce qui est connu sous le nom de cryptographie à clé publique qui utilise deux clés :

1. la **clé privée** (connue uniquement du demandeur et utilisée pour créer la signature) ; et
2. la **clé publique** (connue plus largement et utilisée par les parties en confiance pour vérifier la signature).

Compte tenu du principe d'irréversibilité, il est impossible du point de vue informatique, de dériver la clé privée à partir de la connaissance de la clé publique. Donc, bien que de nombreuses personnes puissent connaître la clé publique d'un signataire donné et l'utiliser pour la vérifier, ils ne peuvent pas découvrir la clé privée et l'utiliser pour contrefaire des signatures électroniques.

Pour vérifier les signatures numériques, le vérificateur doit avoir accès à la clé publique du signataire et avoir l'assurance de sa correspondance avec un signataire disposant d'une certaine identité et/ou attribut ainsi qu'avec la clé privée du signataire. Toutefois, une paire de clé privée et publique n'a pas d'association intrinsèque avec une personne, c'est simplement une paire de

[2] Cette introduction a utilisé, les « *Digital Signature Guidelines* » and the « *PKI Assesment Guidelines* » 2003 publiés par le Comité *Information Security,* de la section Science and Technology Law de l'American Bar Association, comme base pour la description de l'aspect technologique. Le CCBE tient à remercier spécialement pour son aide Stephen S. Wu, co-rapporteur pour les « *PKI Assesment Guidelines* », ancien co-président du Comité *Information Security* et associé chez Cooke Kobrick & Wu LLP, Cupertino, Californie.

[3] Les attributs représentent les caractéristiques d'une personne ou d'une organisation. Dans le cas d'une personne, les exemples d'attributs incluent un cabinet ou une fonction occupée, des affiliations à des organismes internationaux, le statut de membre d'un groupe, les pouvoirs spécifiques détenus par la personnes ou les licences ou autres statuts professionnels. Une ICP peut également contenir l'authentification des appareils, comme des serveurs spécifiques utilisés pour le commerce électronique.

nombres. Une méthode fiable est nécessaire pour associer une personne ou entreprise donnée à la bi-clé. La solution à ce problème est l'utilisation d'une ou plusieurs **parties en confiance** pour associer un signataire identifié et/ou un signataire avec des attributs spéciaux à une clé publique particulière. Cette partie en confiance est dénommée **autorité de certification (AC) ou autorité nationale de certification (ANC)** dans la plupart des normes techniques et dans la présente politique.

Pour associer une clé publique à un signataire potentiel, l'**autorité (nationale) de certification** authentifie d'abord la personne, l'organisation ou l'appareil. Elle délivre ensuite un certificat, une archive électronique contenant la clé publique et reprenant la personne authentifiée, l'organisation ou l'appareil comme sujet du certificat détenant la clé publique. Dans le cadre de l'émission, elle confirme que le signataire potentiel identifié dans le certificat détient la clé privée correspondant à la clé publique à placer dans le certificat.

Le signateur potentiel qui reçoit le certificat est appelé **demandeur**. La fonction principale d'un certificat est de lier une bi-clé à un demandeur spécifique. Le récipiendaire du certificat souhaitant faire confiance à la signature numérique créée par le demandeur visé par le certificat (appelé **partie en confiance**) peut utiliser la clé publique du certificat pour vérifier que la signature numérique a été créée avec une clé privée correspondante. En d'autres termes, si une partie en confiance reçoit un message signé numériquement qui viendrait d'une personne donnée, elle souhaitera s'assurer que la personne dispose de la vraie clé publique du signataire présumé avant d'essayer de vérifier la signature.

Les certificats sont eux-mêmes une archive signée numériquement. Pour assurer aussi bien l'intégrité que l'identité de la source du certificat, l'autorité (nationale) de certification le signe de manière numérique. Une signature numérique, qu'elle soit créée soit par un demandeur pour authentifier un message, soit par une autorité (nationale) de certification devrait être datée de manière sûre pour permettre à la partie en confiance de déterminer de manière fiable si la signature numérique a été créée pendant la période de validité du certificat, une condition pour pouvoir vérifier une signature numérique en vertu de la politique. L'autorité (nationale) de certification) joue un rôle important pour **suspendre** (invalidation temporaire) ou **révoquer** (invalidation permanente) le certificat, par exemple car la sécurité de la clé privée du signataire est compromise. Les conditions de suspension ou de révocation sont expliquées plus en détail dans la présente police. Immédiatement lors de la suspension ou de la révocation de la signature numérique, l'autorité (nationale) de certification doit **émettre une notification de révocation ou de suspension** ou avertir les personnes qui font une demande ou dont on sait qu'elles ont reçu une signature numérique vérifiable en se référant au certificat non fiable.

1.2. Identification

Les identifiants pour la politique de certificat qualifié pour les avocats devrait être :

Nom	CP_CCBE_05
O.I.D.	Le CCBE devra obtenir un OID auprès de l'IANA ((http://www.iana.org/cgi-bin/enterprise.pl) qui vise à identifier les entités travaillant sur Internet
Description :	Politique de certification (PC)- certificat numérique qualifié pour les avocats
Version	003.0
Date d'émission	
Localisation	URL

1.3. Groupe d'utilisateur et application

1.3.1. Autorité de certification (AC)

L'autorité de certification devrait être un organe, ou une personne morale ou physique, qui délivre les certificats.

C'est un tiers investi d'une confiance qui accrédite la connexion entre la clé publique contenue dans le certificat et son détenteur, à savoir la personne ou l'entreprise visée dans le certificat.

L'AC gère le cycle de vie du certificat : délivrance, distribution, révocation et renouvellement des certificats ; et publie périodiquement des listes publiques des certificats révoqués.

1.3.2. Autorité d'enregistrement (AE)

L'autorité d'enregistrement (AE) est une entité qui est autorisée par l'AC et qui est chargée de l'identification et de l'authentification des demandeurs. L'AE identifie l'usage par le biais de :
la vérification des informations du registre (demande de certificat, révocation, suspension et changements).

Dans le cadre de la présente politique de certification, l'AE devrait être :

- le barreau ou ;
- le barreau national.

1.3.3. Le demandeur (ou signataire)

Dans le cadre de la présente politique, le demandeur doit être une personne physique qui détient un dispositif de création de signature et est autorisé à exercer ses activités professionnelles sous un des titres visés à l'article 2 de la directive 98/5/CE (JO L77 du 14 mars 1998) et des versions révisées.

1.3.4. Utilisateur

L'utilisateur est une personne physique ou morale qui fait confiance au certificat numérique créé dans le cadre de la présente politique.

1.3.5. Groupe d'utilisateurs et application

Les certificats numériques émis par cette politique doivent identifier une personne physique qui agit comme avocat dans sa profession.

Les certificats numériques émis par cette politique doivent respecter la norme RFC3280 (X.509).

Les certificats numériques émis par cette politique doivent être des certificats qualifiés selon la directive 1999/93/CE et le droit interne.

Les certificats numériques émis par cette politique doivent être créés par un dispositif sécurisé de création de signature.

1.4. Contacts

Nom de l'organisation :	CCBE
Personne de contact :	Birgit Beger
Courriel :	beger@ccbe.eu
Telephone	+32 2 234 6510
Direction	

2. Dispositions d'ordre général

2.1. Obligations

2.1.1. Autorité de certification (AC) / autorité nationale de certification (ANC)

L'autorité de certification (AC) qui délivre les certificats selon cette politique doit diposer d'un niveau raisonnable de capacité dans ses activités d'AC conformément à la directive 1999/93/CE et au droit interne concerné.

L'AC doit veiller à mettre en œuvre toutes les exigences imposées à celle-ci telles qu'applicables à cette politique.

Les autorités nationales de certifications qui souhaitent apparaître comme ANC « reconnues » sur le site Internet du CCBE doivent informer ce dernier de leur statut de conformité.

2.1.2. Autorité d'enregistrement (AE)

Si des autorités d'enregistrement (AE) sont chargées d'agir comme ANC, elles doivent agir conformément à cette politique de certification.

2.1.3. Le demandeur

Le demandeur doit lire et signer un accord de demandeur pour s'assurer qu'il respecte les obligations suivantes :

1. transmettre des informations exactes et complètes à l'AC selon les exigences visées dans le présent document, notamment pour ce qui est de l'enregistrement ;
2. utiliser uniquement la bi-clé pour les signatures électroniques selon la présente politique ;
3. éviter tout usage interdit du certificat ;
4. utiliser uniquement sa clé privée une fois qu'elle lui a été remise ;
5. avertir l'AC, dans un délai raisonnable, de tout changement de ses activités personnelles ou professionnelles avant la fin de la validité du certificat.

2.1.4. Utilisateur

L'utilisateur doit vérifier les éléments suivants:

1. la validité du certificat numérique en demandant le statut actuel des informations sur une révocation du certificat ;
2. prise en compte de la limite de l'usage du certificat numérique indiquée dans la présente politique.

2.1.5. Obligations de dépositaires

A déterminer par les ANC (autorités nationales de certification).

2.2. Responsabilité

Les ANC délivrant des certificats qualifiés selon la présente politique sont responsables comme le précisent l'article 6 de la directive 1999/93/CE et le droit interne en question.

2.3. Responsabilité financière

A déterminer par les ANC.

2.4. Interpretation et application

2.4.1. Loi

Les ANC émettant des certificats qualifiés selon la présente politique doivent respecter la directive 1999/93/CE et sa transposition juridique en droit interne.

2.4.2. Autonomie des dispositions, survie, fusion et notification

Dans le cas où une partie de la politique de certificat est jugée inapplicable ou non valable selon le droit applicable, cette partie sera appliquée de manière la plus maximale possible pour donner effet à son intention. Les clauses et conditions restantes continueront à être pleinement en vigueur et à avoir plein effet.
Chaque AC veillera à ce que chaque accord auquel elle est partie contienne des dispositions adéquates sur l'autonomie des dispositions, la survie, la fusion et la notification telles qu'applicables.

2.4.3. Procédures de résolution des litiges

Tout litige survenant ou lié à cette politique de certificat doit être résolu à travers un mécanisme de résolution de litiges adéquat.

2.5. Prix

A déterminer par les ANC

2.6. Publication et service de dépositaire

2.6.1. Publication d'information sur l'AC

2.6.1.1. Politique de certification et déclaration des pratiques de certificat

Les ANC qui agissent en vertu de la politique de certificat doivent s'assurer que la politique de certificat et les déclarations de pratiques de certificats (DPC) soient disponibles pour tous les demandeurs et les parties en confiance.

2.6.1.2. Information sur le statut du certificat

Les ANC doivent veiller à mettre à disposition les informations sur le statut du certificat à l'attention de tous les demandeurs et les parties en confiance.

2.6.1.3. Autre information

Les ANC doivent s'assurer que les informations sur leur conformité avec la politique soient disponibles pour tous les demandeurs et parties en confiance.. Chaque ANC décidera de la manière d'informer sur son statut.

Les ANC doivent créer une fonction courriel à travers laquelle l'utilisateur est informé que le certificat respecte la politique de certification (PC), créer un nouveau champ facultatif sur la puce de la carte électronique ou une autre méthode laissée à leur discrétion.

Le CCBE reprendra les AC « reconnues » sur son site Internet, soit tous les barreaux membres qui respectent la politique de certification et en ont informé le CCBE.

Le CCBE ne sera pas responsable du statut réel de la conformité avec l'ANC.

2.6.2. Fréquence de publication

La politique de certificat doit être publiée immédiatement dans les heures de bureau lors de son émission ou lors de sa mise à jour.

La liste des certificats révoqués (LCR) doit être émise et publiée de manière périodique, même s'il n'y a pas de changement aux informations sur le statut du certificat, ou plus fréquemment lorsque les certificats des demandeurs/entités finales sont suspendus ou révoqués.

Les certificats seront publiés chez le dépositaire de l'ANC dès qu'ils sont délivrés.

2.6.3. Contrôle d'accès

Les ANC n'imposent pas de contrôle d'accès à leur politique, leurs certificats délivrés et LCR. A l'avenir, les ANC pourront imposer des contrôles d'accès aux certificats délivrés, aux informations sur le statut et aux LCR à leur propre discrétion.

2.7. Cotrôle de conformité

Chaque ANC doit veiller à ce que sa PC soit conforme aux lignes directrices visées dans la présente PC.

2.8. Confidentialité et protection des données

L'AC délivrant des certificats qualifiés en vertu de la présente politique doit respecter la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et sa transposition juridique en droit interne.

2.8.1. Types d'information considérées comme non-confidentielles

Les PC, les DPC, les certificats, les LCR et les informations personnelles ou professionnelles y apparaissant ne sont pas considérés comme confidentiels et doivent donc être publics.

2.8.2. Divulgation des informations sur la révocation/suspension du certificat

Les LCR seront publiées périodiquement avec les certificats révoqués et suspendus.

2.8.3. Délivrance aux autorités légales

Les ANC doivent respecter les droits à la vie privée en vertu des lois applicables.

2.9. Droits sur la propriété intellectuelle

Cette politique, son OID et le logo du CCBE font partie de la propriété intellectuelle du CCBE, protégée par une marque, un droit d'auteur et d'autres lois sur la propriété intellectuelle et peuvent être utilisés uniquement sur la base d'une licence ou d'une autre autorisation expresse du CCBE et uniquement selon les dispositions de cette politique. Toute autre utilisation des éléments susmentionnés sans autorisation écrite expresse du propriétaire est expressément interdite.

3. Identification et authentification

3.1. Enregistrement initial

3.1.1. Type de nom

Chaque certificat délivré sur la base de la présente politique a un nom distinctif (ci-après DN) selon la norme X.501.

Le DN doit comprendre au minimum les éléments suivants, chacun devant être identifié par les ANC :

- **common name – CN** : cet élément contiendra le nom complet (prénom et nom) du demandeur tel que repris dans les documents de preuve d'identité ;
- **courriel – C** : ce sera le courriel du demandeur ;
- **organisation – O** : le nom officiel de l'institution où est inscrit le demandeur et l'indication qu'il est un avocat ;
- **unité d'organisation – UO** : cet élément contiendra le nom de l'ANC ou du barreau ;
- **titre – T** : cet élément identifiera le titre professionnel de l'avocat ;
- **state** – **ST** : cet élément indiquera l'état de l'ANC. Il est facultatif pour les ANC ;
- **country – C :** cet élément sera le pays de l'ANC.

3.1.2. Necéssité d'avoir des noms explicites

Les ANC doivent publier leur propre politique sur l'usage des noms explicites selon leur droit interne respectif.

3.1.3. Règles d'interprétation des différentes formes de nom

A déterminer par les ANC.

3.1.4. Unicité des noms

Les ANC doivent appliquer l'unicité au sein de l'espace nom X.500 pour lequel elles ont été autorisées à délivrer des noms.

3.1.5. Procédure de résolution de litige sur la déclaration d'un nom

A déterminer par les ANC.

3.1.6. Reconnaissance, authentification et rôle des noms de marque

A déterminer par les ANC.

3.1.7. Preuve de la possession d'une clé privée

La clé privée sera créée par le demandeur et doit être exclusivement en sa possession.

La preuve de la possession d'une clé privée doit être obtenue par la signature de la demande de certificat en utilisant une protocole standard reconnu, c'est-à-dire PKCS#10.

3.1.8. Authentification de l'identité de l'organisation

Les ANC doivent vérifier l'identité du demandeur. Il sera nécessaire que le demandeur se présente en personne et qu'il prouve son identité en présence de la personne autorisée. La présence en personne ne doit pas être nécessaire si le demandeur dispose d'une carte d'identité électronique admise selon le droit interne respectif comme méthode de preuve d'identité sur Internet.

Les ANC doivent vérifier les attributs du demandeur dans leurs propres bases de données.

Les ANC délivrant des certificats qualifiés en vertu de la présente politique doivent respecter la directive 1999/93/CE et sa transposition juridique en droit interne.

3.2. Renouvellement de clés

A déterminer par les ANC.

3.3. Re-génération de clés après révocation

A déterminer par les ANC.

3.4. Demande de révocation

Sur la base de la section 4.

4. Besoins opérationnels

4.1. Demande de certificat

Cette politique ne vise pas à imposer des besoins de mise en œuvre aux ANC émettrices ou aux demandeurs/entités finales. Toutefois, elle identifie les informations et procédures nécessaires qui constituent une assurance et une confiance à l'ANC.

Il appartient à chaque ANC de définir la procédure de demande qui doit décrire ce qui suit :

1. la procédure de demande (c'est-à-dire en ligne ou en personne) ;
2. la personne habilitée à identifier le demandeur ;
3. la preuve d'identité du demandeur ;
4. l'information à fournir par le demandeur avant la création d'un certificat numérique.

4.2. Génération du certificat

Les ANC doivent vérifier minutieusement la conformité et la validité des documents soumis par le signataire. Après avoir réalisé l'authentification selon les méthodes prévues dans le section 3.1, l'ANC doit délivrer le certificat.

En cas de délivrance, l'ANC doit en avertir le demandeur. Si pour une raison, l'AC décide de ne pas délivrer le certificat (même si les vérifications et l'authentification étaient correctes), elle doit avertir les demandeurs et donner les raisons de cette décision.

4.3. Acceptation d'un certificat

Par la livraison d'un dispositif sécurisé de création de signature, le signataire accepte la conservation de la clé privée.

4.4. Suspension et révocation du certificat

Les ANC délivrant les certificats qualifiés selon cette politique doivent respecter la directive 1999/93/CE et sa transposition juridique en droit interne.

4.4.1. Causes de révocation

Un certificat doit être révoqué lorsque l'on soupçonne que les informations contenues sont incorrectes ou compromises. Ceci comprend les situations où :

- la clé privée du demandeur est perdue ou suspectées d'être compromise ;
- les informations sur le certificat du demandeur sont suspectées d'être incorrectes ;
- le signataire n'a plus besoin du certificat pour accéder aux ressources des parties en confiance ;
- le signataire n'est plus habilité.

4.4.2. Procédure de la demande de révocation

Les ANC doivent décrire la procédure de révocation dans le DPC qui comprend :

- l'identification du certificat à révoquer ;
- une déclaration claire des raisons de la révocation ; et
- l'authentification du demandeur de la révocation comme décrit à la section 3.4.

4.4.3. Qui peut demander une révocation

La révocation du certificat peut être demandée par le détenteur du certificat à révoquer ou par une autre entité prouvant la connaissance d'une raison pour la révocation.

4.4.4. Cause de la suspension

Les ANC doivent préciser dans leur PC si elles soutiennent la suspension du certificat. Le cas échéant, les ANC doivent respecter la directive 1999/93/CE et sa transposition juridique en droit national.

4.4.5. Qui peut demander la suspension

Les ANC doivent préciser dans leur PC ou dans leur déclaration de pratique de certification qui peut demander la suspension du certificat.

4.4.6. Procédure de la demande de suspension

Les ANC doivent préciser, dans leur PC ou leur DPC, la procédure de demande de suspension d'un certificat. Les demandes de suspension doivent être authentifiées, justifiables et vérifiables.

Les ANC doivent avertir le demandeur de la procédure de demande de suspension de son certificat en lui fournissant les informations suivantes :

- identification du certificat devant être suspendu ;
- date et heure de la demande de suspension ;
- énonciation claire des raisons de la suspension ;
- la durée de la suspension (si c'est indiqué dans la PC ou DPC).

4.5. Audit sécurité

La présente politique reconnaît l'importance des procédures d'audit sécurité suggérant qu'une ANC en conformité précise tous les types de dispositions dans leur DPC.

4.6. Archives

A déterminer par les ANC.

4.7. Changement de clé

A déterminer par les ANC.

4.8. Compromission et plan anti-sisnistre

A déterminer par les ANC.

4.9. Fin de vie d'une AC

Les ANC doivent préciser dans leurs PC la procédure mettant fin à l'AC et la manière d'en informer les demandeurs.

5. Contrôles de sécurité physique, contrôle des procédures et contrôle du personnel

Les ANC doivent indiquer les exigences de sécurité nécessaires dans leur propre DPC.

Les ANC doivent mettre en place des contrôles appropriés de sécurité physique pour restreindre l'accès aux matériels et aux programmes (y compris le serveur, les stations de travail et tout module externe de matériel de cryptographie ou tokens) utilisés dans le cadre de la fourniture des services d'AC. L'accès à ce matériel et ces programmes sera limité au personnel de confiance.

6. Contrôles techniques de sécurité

6.1. Génération et installation de bi-clés

6.1.1. Génération de bi-clés
Les ANC doivent assurer dans leur PC et DPC que la clé privée du signataire et les clés privées de l'AC sont générées en utilisant un dispositif sécurisé de création de signature (c'est-à-dire CC EAL4+ FIPS 140-1 level 2, ITSEC High4).

Le dispositif sécurisé de création de signature utilisé par les ANC respectera le directive 1999/93/CE, sa transposition juridique en droit interne et la CEN CWA 14169.

6.1.2. Délivrance de la clé publique à un utilisateur
A déterminer par les ANC.

6.1.3. Délivrance d'une clé publique de l'AC à l'utilisateur
A déterminer par les ANC.

6.1.4. Taille de la clé
6.1.4.1. Taille de la clé de l'AC
Les ANC doivent utiliser une clé d'une taille minimale de 2048 bits.

6.1.4.2. Taille de la clé de l'utilisateur

Les ANC respecteront la directive 1999/93/CE, sa transposition juridique en droit interne en matière de validité de la clé de l'utilisateur.

Les clés doivent être générées en utilisant un algorithme RSA pour la clé publique et doivent avoir une taille minimale de 1024 bits.

6.1.5. Génération des paramètres de la clé publique
A déterminer par les ANC.

6.1.6. Contrôle de la qualité des paramètres
A déterminer par les ANC.

6.1.7. Matériel/programme de génération de la clé
Les ANC doivent s'assurer dans leur PC et DPC que la clé privée de l'utilisateur et les clés privées de l'AC sont générées en utilisant un dispositif sécurisé de création de clé (c'est-à-dire CC EAL4+ FIPS 140-1 level 2, ITSEC High4).

Le dispositif sécurisé de création de signature utilisé par les ANC respectera le directive 1999/93/CE, sa transposition juridique en droit interne et la CEN CWA 14169.

6.1.8. Usages de la clé
Les raisons pour lesquelles la clé peut être utilisées doivent être limitées par les ANC à travers l'usage de la clé et l'extension de l'usage de la clé dans le certificat.

C'est un champ qui indique la raison pour laquelle la clé publique certifiée est utilisée. Les certificats délivrés en vertu de cette politique doivent avoir l'extension de la clé reprise comme une étape cruciale de la procédure. Ceci signifie que le certificat doit être utilisé uniquement pour la raison pour laquelle l'usage correspondant de la clé a été défini au début.

6.2. Protection de la clé privée

6.2.1. Clé privée de l'AC

Les ANC doivent prévoir dans leurs PC et DPC une procédure de protection de la clé privée de l'AC selon les dispositions sur les certificats numériques qualifiés de la directive 1999/93/CE et sa transposition en droit interne.

6.2.2. Clé privée de l'utilisateur

La clé privée de l'utilisateur sera émise par un dispositif sécurisé de création de signature selon les dispositions sur les certificats numériques qualifiés de la directive 1999/93/CE et sa transposition en droit interne.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Durée de vie

Les ANC doivent prévoir dans leur PC ou DPC la durée de vie des clés privées et publiques selon la directive 1999/93/CE et sa transposition en droit interne.

6.4. Données d'activation

A déterminer par les ANC.

6.5. Contrôles de sécurité des postes de travail

Les ANC doivent prévoir dans leur PC et DPC la procédure effectuée sur l'ordinateur pour les contrôles de sécurité.

6.6. Contrôles de sécurité durant son cycle de vie

Les ANC doivent préciser dans leur PC et DPC la procédure de contrôle du cycle de vie du certificat.

6.7. Contrôles techniques des modules cryptographiques

A déterminer par les ANC.

7. Profils des certificats et LCR

7.1. Profil des certificats

Les certificats digitaux délivrés selon cette politique doivent être conformes à la norme X.509 V3, RFC3280 « *Internet X.509 Public Key Infrastructure Certificate and CRL Profile »,* ETSI TS 101 862 « *European profile for Qualified Certificates »* et la RCF 3739 « *Qualified Certificates Profile »*.

Les certificats digitaux délivrés selon cette politique sont des certificats qualifiés au terme de la directive 1999/93/CE, Annexe I et sa transposition juridique en droit interne et les spécifications techniques européenne TS 101 456.

Les certificats numériques délivrés selon cette politique doivent comprend au minimum les champs suivants :

- spécification de leur statut de certificats qualifiés ;
- numéro de série unique du certificat ;
- une signature émise par l'AC pour authentifier le certificat ;
- le nom de l'AC émettrice ;
- l'identification de l'utilisateur selon le nom de l'AC émettrice comme décrit au point 3.1 ;
- la date d'activation et de validité du certificat.

7.1.1. Description du profil du certificat

L'utilisation des extensions du certificat doit respecter les spécifications visées dans RCF 3280. Le certificat doit aussi respecter la norme X509:

Champs	
Version	V3
Numéro de série	Numéro de série unique pour le certificat
Algorithmes de la signature	Sha1WithRSAEncryption
Emetteur	
Valide à partir de	Certificat d'activation
Valider jusque	Certificat de validité
Sujet	(Comme décrit au point **3.1.1**)
Clé publique	RSA (1024 bits)

7.1.2. Extension des certificats / ajouts aux certificats

Les certificats digitaux doivent mentionner les options d'extension :

Champs	
Nom alternatif de l'émetteur	A déterminer par les ANC
Nom alternatif du sujet	A déterminer par les ANC
Usage de la clé	A déterminer par les ANC
Usage étendu de la clé	A déterminer par les ANC
Type de certification Netscape	A déterminer par les ANC
Netscape-AC-politique-url	A déterminer par les ANC
Commentaire Netscape	A déterminer par les ANC
Identificateur de la clé de l'autorité	A déterminer par les ANC
(Identificateur de la clé du sujet)	A déterminer par les ANC
Déclaration du sujet	A déterminer par les ANC
(Point de distribution LCR)	A déterminer par les ANC
Contraintes de base	A déterminer par les ANC

Accès aux informations sur l'autorité	A déterminer par les ANC
1.3.6.1.5.5.7.1.3 Qc Statements x.509v3 certificate extension from RFC 3039	A déterminer par les ANC

7.1.3. Identificateurs d'algorithmes

L'identificateur de la signature d'algorithme doit être:
1. 2. 840. 113549. 1. 1. 5 SHA-1 avec cryptage RSA

L'identificateur pour la clé publique d'algorithme doit être
1.2.840.113549.1.1.1 cryptage RSA

7.1.4. Format des noms

A déterminer par les ANC.

7.1.5. Contrainte de nom

Les ANC doivent éviter tout accent dans les noms inclus dans le certificat.

7.1.6. Identificateur de politique de certification

D'autres identificateur de politique de certificat sont appliqués si et seulement si les autres politiques identifiées sont conformes à la présente politique. Toutefois, en vue de promouvoir l'interopérabilité, suite à la RFC 2459, la présente politique suggère d'inclure uniquement un identificateur de politique dans un certificat.

7.1.7. Utilisation d'extensions de contraintes sur les politiques

A déterminer par les ANC.

7.1.8. Syntaxe et sémantique des qualificateurs de politique

A déterminer par les ANC.

7.1.9. Traitement de la sémantique de l'extension critique de la politique ce certification

A déterminer par les ANC.

7.2. Profil des LCR

7.2.1. Numéro de version

Le numéro de version est 2 (deux), comme défini dans la RCF 3280 « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ».

7.2.2. Publication

Les LCR doivent être émises et publiées périodiquement, même en l'absence de changement des informations sur le statut du certificat, ou plus fréquemment lorsque des certificats d'entité finale sont suspendus ou révoqués.

7.2.3. Profil des LCR

Les LCR doivent inclure, au moins, les options suivantes pour l'extension :

Champs
Version
Valide à partir de
Valide jusque
Algorithmes de signature
Série
Point de distribution de la LCR

8. Administration des spécifications

8.1. Procédures de modification de ces spécifications

Le CCBE peut modifier la présente politique. En cas de changements substantiels de cette politique, tous les ANC et utilisateurs doivent être avertis à l'avance. De plus, les ANC mettent à jour la politique conformément aux changements de celle-ci.

De même, les changements de politique qui impliquent uniquement des ajustements techniques mineurs doivent être notifiés à l'avance.

8.2. Politiques de publication et de notification

Une copie électronique de ce document, signée numériquement par un représentant habilité du CCBE, est disponible sous format électronique sur le site Internet.

Annexe 1 ACRONYMES

AC	*Autorité de certification*
CCBE	*Conseil des barreaux européens*
PC	*Politique de certification*
DPC	*Déclaration des pratiques de certification*
LRC	*Liste des certificats révoqués*
DSR	*Demande de signature de certificat*
DES	*Norme de cryptage des données*
DN	*Nom distinctif*
DSA	*Algorithme de signature numérique*
FIPS	*Federal information Processing Standard publication*
IETF	*Internet Engineering task force*
ISO	*Organisation internationale de normalisation*
ITU	*International Telecommunications Union*
LDAP	*Lightweight Directory Access Protocol.*
ANC	*Autorité nationale de certification*
OCSP	*On-line Certificate Status Protocol.*
OID	*Object identifier.*
PIN	*Numéro d'identification personnel*
PKI	*Infrastructure de clé publique*
AE	*Autorité d'enregistrement*
DDC	*Demande de commentaires*
RSA	*Rivest-Shimar-Adleman*
SHA-1	*Secure Hash Algorithm*
SSCD	*Dispositif sécurisé de création de signature*