HISTORIQUE DU DOCUMENT

Référence	Version	Date	Rédaction	statut	Validé par
MET_PA/DM-0039-06 A	1	15/05/2006	JYF/EM EAC/PA.	Création	DM

Historique des modifications :	
Version 1	Création

SOMMAIRE

1 INTRODUCTION 7
1.1 Généralités 7
1.2 Nom du Document et Identification 7
1.3 Les composantes de l'Infrastructure à Clés Publiques (ICP) 7
1.3.1 Autorité de certification SSL CERTINOMIS (AC SSL CERTINOMIS) 8
1.3.2 Autorité d'Enregistrement (AE) 8
1.3.3 Service de Publication (SP) 8
1.3.4 Propriétaire de Nom de Domaine 8
1.3.5 Contact Technique (CT) 9
1.3.6 Autres participants 9
1.3.6.1 Autorité de Certification Racine (ACR) 9
1.3.6.2 Tiers utilisateur 9
1.4 Utilisation des certificats 9
1.4.1.1 Certificat d'AC SSL 9
1.4.1.2 Certificat SSL 9
1.4.2 Utilisation interdite des certificats 9
1.5 Application de la politique 10
1.5.1 Organisme responsable de la présente politique 10
1.5.2 Personne responsable 10
1.5.3 Personne déterminant la conformité de la présente politique avec la PC d'ACR 10
1.5.4 Procédure d'approbation de la DPC 10
1.6 Définitions et Acronymes 11
1.6.1 Définitions 11
1.6.2 Acronymes 13

2 ANNUAIRES ET SERVICES DE PUBLICATION 15
2.1 Service de publication 15
2.2 Informations publiées 15
2.3 Heure et fréquence de publication 15
2.4 Contrôle d'accès au service de publication 15

3 IDENTIFICATION ET AUTHENTIFICATION 16
3.1 Nommage 16
3.1.1 Types de noms 16
3.1.2 Utilisation de noms explicites 16
3.1.3 Anonymat ou utilisation de pseudonyme 16
3.1.4 Règles d'interprétations des différentes formes de noms 16
3.1.5 Unicité des noms 16
3.1.6 Reconnaissance, vérification, et rôle des noms de marques déposées 16
3.2 Vérification initiale d'identité 17
3.2.1 Preuve de possession de clé privée 17
3.2.2 Vérification de l'identité des organisations 17
3.2.3 Vérification de l'identité des personnes 17
3.2.4 Informations non vérifiées 17
3.2.5 Validation du représentant légal 17
3.2.6 Critères de reconnaissance 17
3.3 Vérifications aux fins de renouvellement de clés 17
3.3.1 Vérifications aux fins de renouvellement de clés en situation normale 17
3.3.2 Vérifications aux fins de renouvellement de clés après révocation du certificat 18
3.4 Vérifications aux fins de révocation 18

4 EXIGENCES OPERATIONNELLES 19
4.1 Types de certificat 19
4.1.1 Origine de la demande de certificat SSL 19
4.1.2 Procédure d'enregistrement et responsabilités 19

4.2 Traitement d'une demande de certificat 19
4.2.1 Identification et authentification 19
4.2.2 Approbation ou rejet d'une demande de certificat 19
4.2.3 Durée de traitement d'une demande de certificat 19
4.3 Emission d'un certificat 19
4.3.1 Actions effectuée par l'AC SSL CERTINOMIS pendant l'émission d'un certificat 19
4.3.2 Notification au client de l'émission d'un certificat 20
4.4 Acceptation d'un certificat 20
4.4.1 Procédure d'acceptation d'un certificat 20
4.4.2 Publication d'un certificat par l'AC SSL CERTINOMIS 20
4.4.3 Notification de l'émission d'un certificat par l'AC à d'autres entités 20
4.5 Utilisation des bi-clés et des certificats 20
4.5.1 Utilisation des bi-clés SSL et des certificats 20
4.5.2 Utilisation des clés publiques et des certificats par les tierces parties 20
4.6 Renouvellement du certificat 20
4.6.1 Motifs de renouvellement d'un certificat 20
4.6.2 Personne pouvant demander le renouvellement d'un certificat 21
4.6.3 Traitement des demandes de renouvellement d'un certificat 21
4.6.4 Notification au client de l'émission d'un nouveau certificat 21
4.6.5 Conduite constituant l'acceptation du renouvellement d'un certificat 21
4.6.6 Publication par l'AC du renouvellement d'un certificat 21
4.6.7 Notification de l'émission d'un certificat par l'AC à d'autres entités 21
4.7 Changement de clés (ou certification d'une nouvelle clé publique) 21
4.7.1 Motifs de changement de clés 21
4.7.2 Personne pouvant demander le changement de clés 21
4.7.3 Traitement des demandes de recertification 21
4.7.4 Notification au client de l'émission du nouveau certificat 21
4.7.5 Conduite constituant l'acceptation d'un certificat avec nouveau bi-clé 21
4.7.6 Publication du nouveau certificat par l'AC 21
4.7.7 Notification de l'émission d'un nouveau certificat par l'AC à d'autres entités 22
4.8 Modification d'un certificat 22
4.8.1 Motifs de modification d'un certificat 22
4.8.2 Personne pouvant demander la modification d'un certificat 22
4.8.3 Traitement des demandes de modification de certificat 22
4.8.4 Notification au client de l'émission d'un nouveau modifié 22
4.8.5 Conduite constituant l'acceptation d'un certificat modifié 22
4.8.6 Publication par l'AC d'un certificat modifié 22
4.8.7 Notification de l'émission d'un certificat par l'AC à d'autres entités 22
4.9 Révocation et suspension d'un certificat 22
4.9.1 Motif de révocation d'un certificat 22
4.9.2 Origine d'une demande de révocation 23
4.9.3 Procédure de demande de révocation 23
4.9.4 Période de grâce 23
4.9.5 Délai de traitement d'une révocation 23
4.9.6 Exigences de vérification de révocation pour les tierces parties 24
4.9.7 Fréquences de publication des LCR 24
4.9.8 Possibilité de vérifier l'état des certificats en ligne 24
4.9.9 Exigences de vérification en ligne de l'état des certificats 24
4.9.10 Autres formes de publication des révocations 24
4.9.11 Exigences spécifiques concernant la compromission des clés 24
4.9.12 Motifs de suspension d'un certificat 24
4.9.13 Personne pouvant demander la suspension d'un certificat 24
4.9.14 Procédure de demande de suspension d'un certificat 24
4.9.15 Limites de la période de suspension 24
4.10 Service d'état des certificats 24
4.10.1 Caractéristiques opérationnelles 24
4.10.2 Disponibilité du service 25
4.10.3 Options 25
4.11 Fin d'abonnement 25
4.12 Séquestre et recouvrement de clés 25

5 MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN OEUVRE 26
5.1 Sécurité physique 26
5.1.1 Emplacement des sites et construction 26
5.1.2 Accès physique 26
5.1.3 Alimentation et climatisation 26
5.1.4 Exposition à l'eau 26
5.1.5 Système de détection et d'extinction d'incendie 26
5.1.6 Supports 26
5.1.7 Mise au rebut 26
5.1.8 Sauvegardes hors site 27
5.2 Mesures procédurales 27
5.2.1 Rôles de confiance 27
5.2.2 Nombre de personnes exigées par tâche 27
5.2.3 Identification et vérification pour chacun des rôles de confiance 27
5.2.4 Rôles nécessitant une séparation des tâches 28
5.3 Mesures de contrôle du personnel 28
5.3.1 Exigence en matière de qualifications, d'expérience, et d'habilitation 28
5.3.2 Procédures de vérification des antécédents 28
5.3.3 Exigences en matière de formation professionnelle 28
5.3.4 Formation professionnelle – Fréquence et exigences 29
5.3.5 Rotation des emplois 29
5.3.6 Sanctions en cas d'actions non autorisées 29
5.3.7 Contrôle des personnels des entreprises cocontractantes 29
5.3.8 Documentation fournie au personnel 29
5.4 Procédures de journalisation 29
5.4.1 Evènements journalisés 29
5.4.2 Fréquence de journalisation 29
5.4.3 Période de rétention des journaux 30
5.4.4 Protection des journaux 30
5.4.5 Procédures de sauvegarde des journaux 30
5.4.6 Système de collecte des journaux (interne & externe) 30
5.4.7 Notification au responsable de l'évènement 30
5.4.8 Evaluation des vulnérabilités 30
5.5 Archivage des journaux 30
5.5.1 Journaux à archiver 30
5.5.2 Durée de rétention des archives 31
5.5.3 Protection des archives 31
5.5.4 Sauvegarde des archives 31
5.5.5 Exigences d'horodatage des enregistrements 31
5.5.6 Système de collecte des archives (interne or externe) 31
5.5.7 Procédure d'obtention et de vérification des données archivées 31
5.6 Renouvellement de clé 31
5.6.1 Certificat d'AC SSL 31
5.6.2 Certificat SSL 32
5.7 Compromission et plan de reprise 32
5.7.1 Procédures en cas d'incident et de compromission 32
5.7.2 Corruption des ressources informatiques, des logiciels, et/ou des données 32
5.7.3 Procédures en cas de compromission de la clé privée d'une entité 33
5.7.4 Capacités de reprise d'activité à la suite d'un sinistre 33
5.8 Fin de vie d'AC SSL 33

6 MESURES TECHNIQUES DE SECURITE 34
6.1 Génération et installation des bi-clés 34
6.1.1 Génération des bi-clés 34
6.1.2 Fourniture de la clé privée à l'abonné 34
6.1.3 Fourniture de la clé publique à l'AC 34
6.1.4 Fourniture de la clé publique d'AC SSL aux tierces parties 34
6.1.5 Taille de clés 34
6.1.6 Production des paramètres des clés publiques et contrôle de qualité 34
6.1.7 Utilisation de la clé (selon le champ "key usage" du certificat X 509 V3) 34
6.2 Protection des clés privées et normes relatives au module cryptographique 34

6.2.1 Normes applicables aux ressources cryptographiques et contrôles 34
6.2.2 Contrôle de la clé privée par de multiples personnes 35
6.2.3 Séquestre de clé privée 35
6.2.4 Sauvegarde de clé privée 35
6.2.5 Archivage de clé privée 35
6.2.6 Importation / exportation d'une clé privée 35
6.2.7 Stockage d'une clé privée dans un module cryptographique 35
6.2.8 Méthode d'activation d'une clé privée 35
6.2.9 Méthode de désactivation d'une clé privée 35
6.2.10 Méthode de destruction d'une clé privée 35
6.2.11 Certification des ressources cryptographiques 35
6.3 Autres aspects de la gestion des bi-clés 36
6.3.1 Archivage des clés publiques 36
6.3.2 Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés 36
6.4 Données d'activation 36
6.4.1 Génération et installation des données d'activation 36
6.4.2 Protection des données d'activation 36
6.4.3 Autres aspects touchant aux données d'activation 36
6.5 Mécanismes de sécurité des systèmes informatiques 36
6.5.1 Exigences techniques de sécurité des ressources informatiques 36
6.5.2 Indice de sécurité informatique 37
6.6 Contrôles techniques du système pendant son cycle de vie 37
6.6.1 Contrôle des développements des systèmes 37
6.6.2 Contrôles de gestion de la sécurité 37
6.6.3 Contrôle de sécurité du système pendant son cycle de vie 37
6.7 Mécanismes de sécurité du réseau 37
6.8 Horodatage 38

7 CERTIFICATS, LCR, ET PROFILS OCSP 39
7.1 Profil de Certificat SSL 39
7.1.1 Extensions de Certificats SSL 39
7.1.2 Identifiant d'algorithmes 39
7.1.3 Formes de noms 39
7.1.4 Identifiant d'objet (OID) de la Politique de Certification 39
7.1.5 Extensions propres à l'usage de la Politique 39
7.1.6 Syntaxe et Sémantique des qualificateurs de politique 39
7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies" 39
7.2 Profil de LCR 40
7.2.1 LCR et champs d'extensions des LCR 40
7.3 Profil OCSP 40
7.3.1 Numéro de version 40
7.3.2 Extensions OCSP 40

8 CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS 41
8.1 Fréquence et motifs des audits 41
8.2 Identité / Qualification des auditeurs 41
8.3 Lien entre l'auditeur et l'entité contrôlée 41
8.4 Points couverts par l'évaluation 41
8.5 Mesures prises en cas de non-conformité 41
8.6 Communication des résultats 42

9 AUTRES QUESTIONS COMMERCIALES ET JURIDIQUES 43
9.1.1 Frais d'émission et de renouvellement de certificats SSL 43
9.1.2 Frais d'accès aux certificats SSL 43
9.1.3 Frais d'accès aux LCR et aux informations d'état des certificats SSL 43
9.1.4 Frais pour d'autres services 43
9.1.5 Politique de remboursement 43
9.2 Confidentialité des informations 43
9.2.1 Informations confidentielles 43
9.2.2 Information considérées comme non confidentielles 43
9.2.3 Obligation de protection des informations confidentielles 43

9.3 Confidentialité des informations à caractère personnel 43
9.3.1 Plan de confidentialité 43
9.3.2 Information considérées comme personnelles 44
9.3.3 Information non considérées comme n'étant pas à caractère personnel 44
9.3.4 Obligation de protection des informations à caractère personnel 44
9.3.5 Consentement exprès et préalable à l'utilisation de données à caractère personnel 44
9.3.6 Divulgation due à un processus judiciaire ou administratif 44
9.3.7 Autres motifs de divulgation de données à caractère personnel 44
9.4 Droits relatifs à la propriété intellectuelle 44
9.5 Obligations et garanties 44
9.5.1 Obligations et garanties de l'AC SSL 44
9.5.2 Obligations et garanties du client SSL 45
9.5.3 Obligations et garanties des autres participants 45
9.6 Déni de garanties 45
9.7 Limites de responsabilité 45
9.8 Indemnités 46
9.9 Durée et résiliation 46
9.9.1 Durée 46
9.9.2 Résiliation 46
9.9.3 Effets de la résiliation et survie 46
9.10 Avis individuels et communication avec les participants 46
9.11 Amendements 46
9.11.1 Procédure pour apporter un amendement 46
9.11.2 Mécanisme et délais des notifications 46
9.11.3 Motifs selon lesquels un OID doit être changé 46
9.12 Règlement des différends 46
9.13 Droit applicable 47
9.14 Conformité au droit applicable 47
9.15 Divers 47
9.15.1 Totalité de l'entente 47
9.15.2 Affectation 47
9.15.3 Divisibilité 47
9.15.4 Exonération des droits 47
9.15.5 Force majeure 47
9.16 Autres dispositions 47

1 INTRODUCTION

1.1 Généralités

La dématérialisation, c'est-à-dire la transposition sous format électronique des échanges traditionnels réalisés au quotidien (contrats, courrier, factures, formulaires administratifs, etc.) constitue avant tout un moyen de fluidifier les processus métier. Les aspects novateurs et techniques de ces applications imposent la nécessité, pour l'entreprise, de faire appel à des prestataires de service spécialisés et capables de jouer le rôle de tiers de confiance – en vue, le cas échéant, de fournir la preuve de l'échange.

Le présent document constitue la PC de l'AC SSL CERTINOMIS. La présente PC définit toutes les exigences auxquelles l'AC SSL CERTINOMIS doit se conformer pour gérer des certificats SSL (enregistrement, émission, gestion d'état, renouvellement). La confiance et la qualité offertes par les certificats SSL émis par l'AC CERTINOMIS dépendent des exigences et des moyens définis dans la présente PC.

La présente PC est conforme aux Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy, et Certification Practise Statement Framework.

Afin d'être reconnue partout et à tout moment dans les relations sur l'Internet, avec le même niveau de confiance l'AC SSL CERTINOMIS est rattachée à l'AC Racine de KEYNECTIS. Son certificat d'AC SSL est donc signé par l'ACR de KEYNECTIS. L'AC SSL CERTINOMIS respecte la PC de l'ACR ainsi que les exigences de la "PC des services SSL".

La Politique de Certification (PC) de l'AC Racine définit les exigences suivies par l'ACR KEYNECTIS. La PC dite "PC des services d'AC SSL" édicte les engagements (commerciaux, juridiques et techniques) qu'une AC émettant des certificats SSL doit respecter pour être certifiée par l'ACR. Les certificats de l'ACR sont disponibles dans tous les logiciels de navigation et de messagerie afin de faciliter la reconnaissance de tous les certificats SSL émis sous dans sa hiérarchie d'AC.

KEYNECTIS opère une Autorité de Certification Racine (ACR) afin de certifier des Autorités de Certification (AC) désireuses d'émettre des certificats SSL, dites AC SSL. Un certificat SSL est un certificat électronique autorisant des connexions SSL entre un utilisateur et un site web.

Pionnier en la matière, KEYNECTIS est un Opérateur de Services de Certification; industriel, il se met au service d'une ou plusieurs entités désireuses d'offrir des services de confiance et laisse à celles-ci (devenues Autorités) un contrôle total sur les modes d'attribution, de diffusion et de gestion des certificats numériques.

1.2 Nom du Document et Identification

La présente PC est la propriété de CERTINOMIS. Cette PC est enregistrée par un numéro d'identifiant d'objet (OID) qui est : 1.2.250.1.86.2.2.2.1

Cet OID est inscrit dans tous les certificats SSL émis au titre de la présente PC.

Cet OID sera également inscrit dans les certificats de l'AC SSL CERTINOMIS émis par l'ACR.

1.3 Les composantes de l'Infrastructure à Clés Publiques (ICP)

Pour permettre à l'AC SSL CERTINOMIS de fonctionner, CERTINOMIS a mis en place une ICP hébergée au sein du centre de production de KEYNECTIS. Afin d'assurer l'activité SSL de l'AC SSL CERTINOMIS, cette ICP comporte les composantes qui assurent les services suivants:

- Génération de clés d'AC SSL : l'AC SSL CERTINOMIS génère son propre bi-clé d'AC SSL dans le centre de production de KEYNECTIS au cours d'une cérémonie de clés;
- Génération du certificat d'AC SSL : l'AC SSL CERTINOMIS demande un certificat à l'ACR conformément à la PC de l'AC SSL Racine;

- Génération des bi-clés pour les certificats SSL : le client SSL est responsable de la génération du bi-clé dont il demande la certification de la clé publique;
- Authentification du client SSL : avant d'émettre un certificat SSL, l'AE (Autorité d'Enregistrement) de l'AC, hébergée et gérée par l'AC SSL CERTINOMIS, recueille et vérifie les informations inscrites dans la demande de certificat SSL;
- Génération des certificats SSL : si la demande de certificat du client est correcte et validée par l'AE, l'AC SSL CERTINOMIS génère un certificat SSL;
- Révocation de certificats SSL : quand le lien entre le client SSL et la clé publique certifiée dans son certificat n'est plus considéré comme valide, l'AC SSL CERTINOMIS révoque le certificat SSL;
- Renouvellement de certificats SSL : lorsqu'il y a lieu de remplacer le certificat d'un client SSL, pour cause d'expiration de certificat, de changement de contenu ou de compromission, l'AC SSL CERTINOMIS génère un nouveau certificat;
- Service de Publication: le certificat d'ACR, les certificats d'AC SSL CERTINOMIS et les LCR correspondantes sont publiés par l'AC SSL CERTINOMIS. De plus, les certificats ACR et les certificats AC SSL sont fournis par KEYNECTIS aux principaux éditeurs de logiciels de navigation et de messagerie (Microsoft, Mozilla foundation…) pour intégration.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus. La Déclaration des Pratiques de Certification donnera plus de détails sur les pratiques de chaque entité.

Les composantes définies ci-après contribuent à la mise en œuvre et à l'utilisation des certificats SSL émis par l'AC SSL CERTINOMIS.

1.3.1 Autorité de certification SSL CERTINOMIS (AC SSL CERTINOMIS)

L'AC SSL CERTINOMIS est une AC qui génère des certificats SSL pour ses clients (sociétés, administrations publiques …), permettant ainsi l'établissement de communications sécurisées au sein d'une communauté ouverte. L'AC SSL CERTINOMIS utilise les services de son SP pour publier les certificats et les LCR, qu'ils soient générés par l'AC SSL CERTINOMIS ou reçus de l'ACR.

L'AC SSL CERTINOMIS met en oeuvre ses propres PC/DPC pour l'exploitation de son ICP et respecte les PC de l'ACR et la "PC des services d'AC SSL".

1.3.2 Autorité d'Enregistrement (AE)

Une Autorité d'Enregistrement est une entité qui fournit des services "d'authentification des clients" pour l'AC SSL CERTINOMIS conformément à la présente PC. L'AE est authentifiée et reconnue par l'AC SSL CERTINOMIS.

L'AC SSL CERTINOMIS dispose de sa propre AE, qu'elle héberge et qu'elle opère pour les besoins d'enregistrement de ses clients.

Dans le cas du service "Club SSL", les services de l'AE peuvent être fournis par un représentant du client qui effectue tous les services d'AE à la place de l'AE de l'AC SSL CERTINOMIS. Le représentant du client est en relation contractuelle avec l'AC SSL CERTINOMIS et est authentifié par l'AE de l'AC SSL CERTINOMIS. Le représentant du client agit sous la responsabilité du client pour générer les demandes de certificat SSL notamment. L'AC SSL CERTINOMIS s'assure que le représentant du client est bien authentifié et mandaté par le client.

1.3.3 Service de Publication (SP)

Le SP est une entité qui rend les certificats et les LCR disponibles sur l'Internet.

1.3.4 Propriétaire de Nom de Domaine

Le propriétaire du nom de domaine est l'entité qui possède légalement le nom de domaine à inscrire dans le certificat SSL émis par l'AC SSL CERTINOMIS. Le nom de domaine est géré par un administrateur de noms de domaine. Une étape "d'authentification" permet à l'AC SSL CERTINOMIS de s'assurer que:

- L'entité mentionnée dans la demande de certificat ou RSC (Requête de Signature de Certificat) existe et a légalement le droit exclusif d'usage de ce nom de domaine;
- Le nom de domaine inscrit dans la demande appartient à cette entité, qui a donc le droit de l'utiliser;

• Le contact technique a le droit de soumettre la demande puisqu'il représente l'entité ou appartient à une société mandatée par l'entité propriétaire du nom de domaine et qui l'autorise à envoyer la demande (par exemple une société en relation capitalistique ou un hébergeur).

1.3.5 Contact Technique (CT)

Le contact technique est une personne autorisée par le propriétaire d'un nom de domaine à soumettre une demande de certificat.

Dans le cas particulier du Club SSL, le CT joue le rôle d'AE, il en gère tous les services. L'organisation à laquelle il appartient s'engage alors auprès de l'AC SSL CERTINOMIS, à respecter les clauses suivantes :

• L'organisation est responsable de l'authentification interne et des vérifications préalables à l'émission des certificats SSL;
• L'organisation, agissant en tant qu'AE, doit respecter les éléments de la PC/DPC qu'il doit mettre en oeuvre;
• L'organisation ne sera pas nécessairement soumise à un contrôle de conformité par l'AC SSL CERTINOMIS;
• L'organisation doit informer, dans un délai de sécurité raisonnable, l'AC SSL CERTINOMIS de la cessation et/ou de toute modification concernant l'identité et l'autorisation du représentant du client;
• L'utilisation d'un certificat de classe 3 sur support (carte à puce ou token) fourni par CertiNomis pour communiquer avec l'AC SSL CERTINOMIS.

1.3.6 Autres participants

1.3.6.1 Autorité de Certification Racine (ACR)

L'ACR est l'AC Racine exploitée par KEYNECTIS. L'ACR signe et révoque les certificats de l'AC SSL CERTINOMIS. Dans la présente PC, quand le terme "ACR" est utilisé sans détailler de composante (AE, SP...), il couvre tous les aspects de l'ICP existante au regard des aspects juridique et commercial. L'ACR utilise les services de son AE pour identifier et authentifier l'AC SSL CERTINOMIS pour les demandes de certificat, demandes de révocation et demandes de renouvellement. L'ACR utilise son Service de Publication pour publier les certificats ainsi que les Listes de Révocation d'Autorités (LRA) qu'elle a générés. L'ACR exploite ses services conformément à la PC de l'AC SSL Racine et à la DPC associée. L'ACR ne peut fonctionner sans l'approbation préalable du Responsable de l'ACR, à savoir la personne désignée comme telle dans le cadre de la PC d'ACR.

1.3.6.2 Tiers utilisateur

Un tiers utilisateur est un individu ou une organisation qui agit en se fiant à un certificat et/ou une signature numérique. Dans ce contexte, les clients internautes qui se fient aux certificats SSL sont des tiers utilisateurs.

1.4 Utilisation des certificats

1.4.1 Utilisation appropriée des certificats

1.4.1.1 Certificat d'AC SSL

Le certificat d'AC SSL est utilisé par un client internaute pour vérifier l'identité d'un certificat SSL émis conformément à la PC d'AC SSL CERTINOMIS.

1.4.1.2 Certificat SSL

Le certificat SSL est utilisé par un tiers utilisateur sur l'Internet ou sur un intranet pour vérifier l'identité d'un nom de domaine hébergé par un serveur.

1.4.2 Utilisation interdite des certificats

Les utilisations de certificats SSL émis par l'AC SSL CERTINOMIS à d'autres fins que celles couvertes par la présente PC ne sont pas autorisées. Cela signifie que l'AC SSL CERTINOMIS ne peut être en aucun cas tenue pour responsable d'une utilisation des certificats SSL qu'elle émet autre que celles prévues dans la présente PC.

Les certificats ne devront être utilisés que conformément aux lois en vigueur et applicables, et en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation.

Les certificats AC de l'AC SSL CERTINOMIS ne sont utilisés pour d'autres fonctions que celles de délivrance de certificats SSL. KEYNECTIS décline toute responsabilité à l'égard d'un usage des certificats d'AC SSL autre que la fonction AC, qui consiste à émettre des certificats SSL aux clients conformément à la présente PC.

1.5 Application de la politique

1.5.1 Organisme responsable de la présente politique

La présente PC est sous la responsabilité de la société CERTINOMIS.

1.5.2 Personne responsable

Monsieur Daniel Martin
Directeur Général
CertiNomis
20-22 rue Louis Armand
75015 Paris

Téléphone : (33) (0)1.58.09.80.60
Télécopieur : (33) (0)1.58.09.80.67

1.5.3 Personne déterminant la conformité de la présente politique avec la PC d'ACR

L'AC SSL CERTINOMIS est responsable de l'élaboration, de l'approbation et du maintien des PC et DPC de l'AC SSL CERTINOMIS. La personne responsable de l'AC SSL CERTINOMIS devra approuver la présente PC conformément à la PC d'ACR et à la "PC des services d'AC SSL".

1.5.4 Procédure d'approbation de la DPC

Le terme DPC (CPS en anglais) est défini dans l'Internet RFC 3647, X.509 Public Key Infrastructure Certificate Policy et le Certificate Practices Framework comme suit: "*Une déclaration des pratiques utilisées par une Autorité de Certification pour émettre des certificats*". Il s'agit de la description complète de détails tels que l'exacte mise en oeuvre de la fourniture de services et les procédures détaillées de gestion du cycle de vie des certificats. La DPC doit être plus détaillée que la présente.

La DPC de l'AC SSL CERTINOMIS est publiée par l'AC SSL CERTINOMIS. Le responsable de l'AC SSL CERTINOMIS possède ses propres méthodes pour approuver la DPC et s'assurer qu'elle est conforme à la présente PC. Un minimum de travail de contrôle de conformité est exigé de l'AC SSL CERTINOMIS.

Le responsable de l'AC SSL CERTINOMIS approuve les résultats de la revue de conformité effectuée par les experts désignés par le responsable de l'ACR à propos de la DPC de l'AC SSL CERTINOMIS.

Les modifications devront être apportés soit sous la forme d'une nouvelle DPC (avec un résumé des modifications), soit par un avis de mise à jour contenant les modifications et leurs références dans la précédente version de la DPC. Le responsable de l'ACR peut suggérer l'élaboration d'une nouvelle DPC. Toute nouvelle version de la DPC remplace automatiquement la version précédente et devient opérationnelle dès que le responsable de l'ACR a émis son accord sur le résultat de la revue de conformité. La nouvelle version de la DPC doit continuer à être conforme à la présente PC, ceci afin de permettre à l'AC SSL CERTINOMIS de s'y référer et d'émettre des certificats SSL.

1.6 Définitions et Acronymes

1.6.1 Définitions

Accord d'utilisation de LCR: Un accord spécifiant les termes et conditions sous lesquels une Liste de Certificats Révoqués ou les informations qu'elle contient peuvent être utilisées.

Accréditation volontaire: Toute autorisation indiquant les droits et obligations spécifiques à la fourniture de services de certification, accordés, sur demande du prestataire de service de certification concerné, par l'organisme public ou privé chargé d'élaborer ces droits et obligations et d'en contrôler le respect, lorsque le prestataire de service de certification n'est pas habilité à exercer les droits découlant de l'autorisation aussi longtemps qu'il n'a pas obtenu la décision de cet organisme. [EC 1999/93] Note: Le terme "accréditation" est en général compris d'une autre manière, signifiant "l'accréditation des organismes de certification effectuant des évaluations de conformité de produits et/ou de services ".

AC SSL CERTINOMIS: voir § 1.3.1 ci-dessus.

Audit: Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures. [ISO/IEC POSIX Security].

Autorité de Certification (AC): autorité à qui un ou plusieurs utilisateurs se fient pour créer et attribuer des certificats. Facultativement, l'autorité de certification peut créer les clés d'utilisateur [ISO/IEC 9594-8; ITU-T X.509]. Dans la présente PC, le terme AC SSL CERTINOMIS est utilisé pour désigner l'AC rattachée à l'ACR et qui émet des certificats SSL.

Autorité de Certification Racine (ACR): voir § 1.3.6.1 ci-dessus.

Autorité d'Enregistrement (AE): voir § 1.3.2 ci-dessus.

Centre de production KEYNECTIS: l'objet initial du Centre de production KEYNECTIS et des moyens exploités par KEYNECTIS est la production de certificats électroniques. Ces services comprennent :
- La gestion du cycle de vie des autorités de certification;
- La gestion du cycle de vie des certificats électroniques,
- La publication des éléments associés à la gestion de ces cycles de vie,
- La production de jetons d'horodatage,
- La personnalisation des cartes à puce et autres clés USB,
- La vérification des signatures électroniques ou de la validité des certificats.

Cérémonie de clés: Une procédure par laquelle une bi-clé d'AC ou AE est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.

Certificat SSL: clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509]. Dans ce contexte, les certificats du client SSL sont des certificats utilisés par un serveur pour établir une connexion SSL au titre d'un nom de domaine (ND) certifié. Le certificat contient le nom de domaine pleinement qualifié (FQDN: Fully Qualified Domain Name).

Certificat d'AC: certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509]. Dans ce contexte, les certificats AC sont des certificats ACR (certificat auto signé) et des certificats d'AC SSL (signés par l'ACR).

Certificat auto signé: certificat d'AC signé par la clé privée de cette même AC.

Chaîne de certification: (ou chaîne de confiance) chaîne constituée de multiples certificats nécessaires pour valider un certificat. Dans le contexte de la présente PC, la chaîne de certification est composée d'un certificat d'ACR, du certificat d'AC SSL CERTINOMIS et des certificats SSL signés par l'AC SSL CERTINOMIS.

Clé privée: clé du bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique: clé du bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1]

Client SSL: entité demandant la génération un certificat SSL pour son compte. Un client SSL est en mesure d'utiliser - et est autorisé à le faire - la clé privée qui correspond à la clé publique contenue dans le certificat.

Compromission: violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité: La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

Contact technique: voir § 1.3.5 ci-dessus.

Déclaration des Pratiques de Certification (DPC): une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) utilise pour approuver ou rejeter des demandes de certificat (émission, gestion, renouvellement et révocation de certificats). [RFC 3647].

Demande de certificat: message transmis par l'AE à l'AC pour obtenir l'émission d'un certificat d'AC.

Disponibilité: La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Données d'activation: Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un NIP, une phrase secrète, une clé partagée manuelle).

Fonction de hachage: fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux deux propriétés suivantes:
- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1];
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Infrastructure à Clé Publique (ICP): également appelée IGC (Infrastructure de Gestion de Clés), c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR doivent être publiés. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Intégrité: fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Interopérabilité: implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste de Certificats Révoqués (LCR): liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Modules cryptographiques: Un ensemble de composants logiciels et matériels utilisés pour mettre en oeuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS or EAL), utilisé pour conserver et mettre en oeuvre la clé privée AC.

Nom de domaine: nom qui a été enregistré auprès des organismes officiels tels que AFNIC ou INTERNIC. Il se compose du nom précédant une extension (telle que .fr ou .com) complété par l'extension elle-même. Durant le processus d'enregistrement, le nom de domaine est "associé" à un contact technique qui est légalement autorisé à utiliser ce nom de domaine.

Période de validité d'un certificat: La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10: (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'ICP après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR*:* entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (PC): ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509]. Le présent document est la PC applicable à l'AC SSL CERTINOMIS.

Politique de sécurité: ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509]. Dans ce contexte, la politique de sécurité sera élaborée par KEYNECTIS qui héberge et exploite l'AC SSL CERTINOMIS.

Protocole de vérification de statut de certificat en ligne (OCSP) : protocole destiné à fournir aux tiers utilisateurs des informations en temps réel sur le l'état de validité des certificats.

Propriétaire de nom de domaine : voir § 1.3.4 ci-dessus.

Qualificateur de politique: Des informations concernant la politique qui accompagnent un identifiant de politique de certification dans un certificat X.509. [RFC 3647]

Revue de conformité : processus établi par l'ACR pour déterminer si l'AC SSL CERTINOMIS se conforme à la PC de l'ACR et à la "PC des services d'AC SSL". Pour réaliser ce processus, l'ACR ou tout auditeur choisi par l'ACR vérifie la conformité des engagements pris par CERTINOMIS dans sa PC d'AC SSL et les modalités de sa mise en œuvre par KEYNECTIS précisées dans sa DPC. L'AC SSL CERTINOMIS doit fournir un résultat d'audit du champ d'application défini dans la "PC de services d'AC SSL". Le résultat de l'audit peut être fourni au travers d'un processus de qualification par rapport aux exigences de la norme processus ETSI TS 101 456 (processus de qualification des prestataires de services de certification électronique) , d'audit d'AC type WebTrust, ou d'autres processus d'audit pertinents.

RSA: algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adelman.

Secure Socket Layer (SSL): méthode la plus communément utilisée dans l'industrie pour protéger les communications avec les sites web, mise au point par Netscape Communications Corporation. Le protocole de sécurité SSL assure le chiffrement des données, l'authentification du serveur, l'intégrité des messages et en option l'authentification du client pour une connexion Transmission Control Protocol/Internet Protocol.

Services d'horodatage: service qui fournit une attestation signée numériquement (contre marque de temps) attestant qu'un document ou un ensemble de données a existé à un moment donné. Le service d'horodatage est un service qui associe de manière sûre un évènement et une heure afin d'établir de manière fiable l'heure à laquelle cet évènement s'est réalisé.

Service de Publication (SP): voir § 1.3.3 ci-dessus.

Système de confiance: Des matériels, logiciels, et procédures sécurisés contre les intrusions et une mauvaise utilisation; qui fournissent un niveau de disponibilité, fiabilité, et de fonctionnement correct; qui sont adaptés à l'exécution des fonctions pour lesquelles ils sont prévus; et qui mettent en oeuvre la politique de sécurité applicable.

Tiers utilisateur: voir § 1.3.6.2 ci-dessus.
Token : dispositif matériel utilisé pour envoyer des clés à une entité et qui peut protéger ces clés pendant le transport [ISO/IEC 9798-1 (2nd édition): 1997].

1.6.2 Acronymes

AC : Autorité de Certification
AE : Autorité d'Enregistrement
ACR : Autorité de Certification Racine

CT : Contact Technique
DN: Distinguished Name
DPC : Déclaration des pratiques de certification
EAL: Evaluation assurance level, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité
FIPS: United State Federal Information Processing Standards, norme fédérale américaine pour l'évaluation de produits de sécurité
HTTP: Hypertext Transport Protocol
ICP : Infrastructure à Clés Publiques
IP: Internet Protocol
ISO: International Organization for Standardization
LCR : liste de certificats révoqués
LDAP: Lightweight Directory Access Protocol
LRA : Liste de Révocation d'Autorité (de certification)
OCSP: Online Certificate Status Protocol
OID: Object Identifier;
PC : Politique de Certification
PIN: Personal Identification Number
PKCS: Public-Key Cryptography Standard
RFC: Request for comment
RSA: Rivest, Shamir, Adleman
SHA: Secure Hash Algorithm (norme fédérale américaine)
SP : Service de Publication
SSL: Secure Socket Layer
URL: Uniform Resource Locator

2 ANNUAIRES ET SERVICES DE PUBLICATION

2.1 Service de publication

L'AC SSL CERTINOMIS met à la disposition des clients et des tiers utilisateurs les informations définies ci-dessous à l'aide d'un service de publication.

2.2 Informations publiées

L'AC SSL CERTINOMIS s'assure que les termes et conditions applicables à l'usage des certificats SSL qu'elle émet sont mis à la disposition des clients et tiers utilisateurs via son SP. L'AC SSL CERTINOMIS rend disponibles les informations suivantes:

- La PC de l'AC SSL CERTINOMIS;
- Les certificats d'AC Racine;
- Les certificats d'AC SSL CERTINOMIS;
- Les certificats SSL émis par l'AC SSL CERTINOMIS;
- Les conditions générales d'utilisation des certificats SSL;
- La documentation sur les demandes de certificat et les demandes de révocation;
- Les informations d'état de validité des certificats SSL qu'elle a émis.

Ces informations sont rendues disponibles en français sur le site web de l'AC SSL CERTINOMIS à l'adresse suivante : ***www.certinomis.com***
L'acceptation du certificat SSL par le client SSL vaut approbation pour publication de ce certificat (complet) sur le site de l'AC SSL CERTINOMIS.

2.3 Heure et fréquence de publication

Les informations citées ci-dessus sont disponibles 24 heures sur 24, 7 jours sur 7. En cas d'indisponibilité du système, du service, ou d'autres éléments qui échappent au contrôle de l'AC SSL CERTINOMIS, cette dernière fait de son mieux pour que l'indisponibilité de ce service d'information ne dépasse pas la durée maximum prévue dans la Déclaration des Pratiques de Certification.

Les certificats et le statut des certificats sont disponibles dès qu'ils sont générés.

2.4 Contrôle d'accès au service de publication

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées. Les informations sont disponibles publiquement et internationalement au moyen de l'Internet.

L'AC SSL CERTINOMIS s'assure que toute information conservée dans une base documentaire de son ICP et dont la diffusion publique ou la modification n'est pas prévue est protégée.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Un certificat SSL porte un nom distinctif et unique (DN) X.501 dans le champ Subject du certificat et conformément au RFC3280. Le nom distinctif se compose des éléments suivants:

Organisation	Entité pour laquelle le certificat est émis. Le terme 'Organisation' est un nom générique couvrant les différents types d'entités demandant des certificats SSL (entreprise, administration, collectivité locale, association …). Le nom de l'Organisation doit être le même que celui associé au numéro de SIREN (ou DUNS) présent dans la demande de certificat.
Common Name	Nom de domaine pleinement qualifié (FQDN: Fully Qualified Domain Name). Il s'agit du nom du site à sécuriser. Le Common Name ne peut jamais être une adresse IP.
Locality	Le client doit saisir dans ce champ le nom de la ville où le siège social de son organisation est situé.
State	Le client SSL saisit ici le nom de l'état, de la région ou du département où son organisation est située.
Country	Le client SSL saisit ici le code à deux lettres (normalisé ISO) du pays où son organisation est située

Si le client modifie l'une quelconque des informations contenues dans le DN, il doit informer l'AC SSL CERTINOMIS de cette modification. L'AC SSL CERTINOMIS procède à la vérification de la nouvelle identité.

Selon les modifications introduites, le client SSL peut se voir demander de recertifier sa clé publique.

3.1.2 Utilisation de noms explicites

Les certificats émis conformément à la présente PC ne sont explicites que si les noms qui y apparaissent peuvent être compris et utilisés par les tiers utilisateurs. Les noms utilisés dans le certificat doivent avoir un lien explicite avec l'entité (personne ou objet) au profit desquels ils sont utilisés.

3.1.3 Anonymat ou utilisation de pseudonyme

L'identité utilisée pour les certificats SSL n'est ni un pseudonyme, ni un nom anonyme.

3.1.4 Règles d'interprétations des différentes formes de noms

Les règles d'interprétation des formes de noms découlent des formes et contenus des certificats définis aux articles 3.1.1 et 7.1.

3.1.5 Unicité des noms

Les identités des certificats SSL (cf. article 3.1.1) sont uniques au sein de l'ensemble des certificats SSL émis par l'AC SSL CERTINOMIS. L'AE assure cette unicité au moyen de son processus d'enregistrement ;

Tout contact technique qui demande un certificat SSL à l'AC SSL CERTINOMIS doit démontrer qu'il a le droit d'utiliser le nom en question pour identité.

En cas de différend au sujet de l'utilisation d'un nom pour un certificat, l'AC SSL CERTINOMIS a la responsabilité de résoudre le différend en question.

3.1.6 Reconnaissance, vérification, et rôle des noms de marques déposées

Il n'est pas garanti aux clients SSL qu'ils pourront faire figurer un nom de marque déposée dans leur nom, même s'ils le demandent.

L'AC SSL CERTINOMIS n'est pas dans l'obligation de faire une recherche de noms de marques déposées ou de résoudre un différend portant sur un nom de marque déposée.

3.2 Vérification initiale d'identité

3.2.1 Preuve de possession de clé privée

Un client demandant un certificat SSL s'assure que la génération de sa bi-clé est réalisée de manière à ce que seule la personne autorisée à gérer et utiliser sa bi-clé au sein de son organisation, détiennent la clé privée correspondant à la clé publique à certifier.

L'AC SSL CERTINOMIS s'assure que le client SSL possède la clé privée associée à la clé publique transmise aux fins de certification en utilisant une demande de certificat au standard PKCS#10.

3.2.2 Vérification de l'identité des organisations

L'AE vérifie que l'organisation mentionnée dans la demande de certificat (nom de domaine et client SSL) existe et qu'elle a droit d'utilisation exclusive de son nom, ceci en croisant les informations fournies avec celles recueillies par l'AE dans les bases de données des organismes officiels concernés ou des autorités compétentes détenant la capacité de confirmer ou non l'existence de l'organisation.

3.2.3 Vérification de l'identité des personnes

L'AE vérifie au cours d'entretiens téléphoniques à son initiative, que l'identité des contacts techniques mentionnée dans les demandes de certificats est correcte. Au cours de ces entretiens, diverses informations fournies par les clients SSL sont vérifiées. Ces vérifications comprennent la vérification d'une information secrète transmise par le client SSL lors de la demande de certificat.

En complément, l'AE procède à l'enregistrement des étapes suivies pour l'émission de chaque certificat.

3.2.4 Informations non vérifiées

Aucune information non vérifiée n'est introduite dans les certificats.

3.2.5 Validation du représentant légal

Une demande de certificat contenant une affiliation explicite ou implicite à une organisation n'est émise qu'après avoir reçu l'assurance que le contact technique détient l'autorisation d'agir pour le compte de cette organisation. Quand la certification du contact technique requiert une autorisation (confirmation de l'emploi et autorisation de l'employeur, existence et identité du service cité, attribution d'une fonction …), alors l'AE authentifie cette autorisation et/ou le représentant légal au moyen des mêmes procédures que celles décrites aux articles 3.2.2 et 3.2.3.

L'AE vérifie aussi que le CT appartient bien à l'organisation identifiée, ceci en utilisant les informations fournies dans la demande de certificat et au moyen de la même procédure que celle décrite à l'article 3.2.2.

3.2.6 Critères de reconnaissance

Un client qui obtient un certificat SSL émis par l'AC SSL CERTINOMIS, est garanti que :
- Les PC/DPC selon lesquelles a été émis ce certificat SSL ont réussi leur contrôle de conformité réalisé par le Responsable de l'ACR vis-à-vis de la "PC des services d'AC SSL",
- L'ICP utilisée pour émettre ce certificat SSL a suivi avec succès un audit de conformité ;
- Les certificats et informations d'état de validité des certificats publiés sont conformes aux exigences de la "PC des services d'AC SSL".

3.3 Vérifications aux fins de renouvellement de clés

3.3.1 Vérifications aux fins de renouvellement de clés en situation normale

Une demande de renouvellement de clé ne peut être effectuée par un client qu'au titre du nom de domaine pour lequel la clé a été générée. Le client s'identifie en utilisant le processus initial de vérification d'identité décrit à l'article 3.2.

3.3.2 Vérifications aux fins de renouvellement de clés après révocation du certificat

Après qu'un certificat SSL ait été révoqué pour une raison autre qu'un renouvellement ou une mise à jour, le client SSL doit recommencer la procédure d'enregistrement initial prévue à l'article 3.2 pour obtenir un nouveau certificat.

Si le certificat SSL a été révoqué en raison d'une compromission de clé, le client SSL doit générer une nouvelle bi-clé avant d'effectuer une nouvelle demande de certificat.

3.4 Vérifications aux fins de révocation

Les demandes de révocation sont authentifiées par l'AE. La procédure de vérification exige le même niveau de confiance que celle utilisée pour l'enregistrement initial (voir articles 3.2.2 et 3.2.3) afin de s'assurer que le client certifié a effectivement fait une demande de révocation.

En conséquence, l'AE de l'AC SSL CERTINOMIS vérifiera les identités des organisation et personnes demandeuses d'une révocation selon les étapes applicables de l'enregistrement initial.

4 EXIGENCES OPERATIONNELLES

4.1 Types de certificat

4.1.1 Origine de la demande de certificat SSL

Une demande de certificat SSL ne peut être transmise à l'AE de l'AC SSL CERTINOMIS que par le contact technique du client SSL.

4.1.2 Procédure d'enregistrement et responsabilités

Les informations suivantes doivent figurer dans la demande de certificat SSL :
- Identification personnelle du CT, c'est-à-dire nom, prénoms, adresse de courrier électronique, fonction, adresse postale complète, numéros de téléphone (standard et ligne directe);
- Identification de l'organisation, c'est-à-dire nom, prénoms et statut du représentant légal, ainsi que toute autre information utile à l'enregistrement (par ex. N° SIREN de la société);
- Clé publique au standard PKCS#10;
- Identification du nom de domaine;
- Durée de validité du certificat SSL (1 ou 2 an(s));
- Données "secrètes" du client pour le processus d'authentification lors de la vérification d'identité, voir article 3.2.3 ci-dessus (fourniture d'un couple question / réponse).

Avant que d'entrer en relation contractuelle avec un client, l'AC SSL CERTINOMIS informe le client des termes et conditions contractuelles d'utilisation des certificats SSL.

4.2 Traitement d'une demande de certificat

4.2.1 Identification et authentification

Le CT du client SSL soumet le formulaire de demande de certificat à l'AE (cf. article 4.1.2).

Les communications entre le CT et l'AE sont protégées de manière à garantir l'intégrité et l'origine des données transmises. Il est de la responsabilité de l'AE de vérifier que les informations figurant dans la demande de certificat sont exactes et vérifier à la fois l'organisation et l'identité du CT. L'AE effectue les vérifications nécessaires à l'authentification telles qu'elles sont décrites à l'article 3.2 par une procédure sous le double contrôle de deux personnes dans des rôles de confiance au sein de l'AE.

L'AE enregistre toutes les informations utilisées pour vérifier l'identité du client telle qu'inscrite dans la demande de certificat et, selon le cas, tout attribut spécifique, y compris tout numéro de référence contenu dans la documentation utilisée pour les vérifications, et toute limitation de sa validité.

4.2.2 Approbation ou rejet d'une demande de certificat

La demande de certificat est approuvée par l'AE après vérification de l'identité et contact téléphonique (articles 3.2 et 3.3).

Si les vérifications sont positives et la procédure complète de validation est terminée, l'AE transmet la demande de certificat à l'AC SSL CERTINOMIS.

4.2.3 Durée de traitement d'une demande de certificat

La durée du traitement d'une demande de certificat SSL est de 24 heures (si toutes les vérifications ont été effectuées – c'est-à-dire si les personnes chargées des vérifications ont été en mesure de les effectuer).

4.3 Emission d'un certificat

4.3.1 Actions effectuée par l'AC SSL CERTINOMIS pendant l'émission d'un certificat

Avant de générer un certificat SSL, l'AE transmet la demande de certificat à l'AC SSL CERTINOMIS qui vérifie que tous les champs et champs d'extension du certificat à signer sont correctement remplis.

La transmission des informations de l'AE vers l'AC SSL CERTINOMIS est protégée par un lien sécurisé. L'ensemble des opérations d'émission d'un certificat est protégé de manière à garantir l'intégrité, la confidentialité (si nécessaire) et l'origine des données transmises et traitées.

4.3.2 Notification au client de l'émission d'un certificat

L'AC SSL CERTINOMIS avise le client de l'émission du certificat en lui envoyant un courrier électronique.

4.4 Acceptation d'un certificat

4.4.1 Procédure d'acceptation d'un certificat

Dès que le CT du client SSL a téléchargé son certificat, l'AC SSL CERTINOMIS considère que le certificat est accepté.

4.4.2 Publication d'un certificat par l'AC SSL CERTINOMIS

L'AC SSL CERTINOMIS transmet le certificat SSL au SP pour publication (voir article 2) après avoir obtenu l'autorisation du client SSL.

4.4.3 Notification de l'émission d'un certificat par l'AC à d'autres entités

La publication d'un certificat SSL par le SP vaut notification.

4.5 Utilisation des bi-clés et des certificats

4.5.1 Utilisation des bi-clés SSL et des certificats

Les bi-clés SSL et les certificats SSL servent à établir une connexion SSL.

4.5.2 Utilisation des clés publiques et des certificats par les tierces parties

Avant de reposer leur confiance sur un certificat SSL, les tierces parties doivent procéder à :
- L'identification et la vérification du chemin de certification qui supporte le certificat SSL,
- Vérifier toutes les signatures électroniques des certificats du chemin de certification,
- Vérifier le champ "key usage" du certificat et utiliser le certificat en conséquence,
- Vérifier l'information de l'état de validité du certificat SSL.

4.6 Renouvellement du certificat

Le renouvellement d'un certificat consiste en l'émission d'un nouveau certificat pour un même nom de domaine et en utilisant le même bi-clé, après expiration d'un précédent certificat SSL.

Le renouvellement d'un certificat n'est possible que lorsque la durée de vie restante de la bi-clé est conforme aux recommandations en la matière (notamment par rapport à la longueur des clés).

4.6.1 Motifs de renouvellement d'un certificat

Un certificat SSL peut être renouvelé si sa clé publique n'a pas atteint sa limite de durée de vie, la clé privée associée n'a pas été révoquée ou compromise et les noms de domaine et attributs n'ont pas changé.

La durée de vie du nouveau certificat ne doit pas dépasser la durée de vie restante de la clé privée utilisée.

L'AE contrôle l'existence et l'état de validité du certificat à renouveler, vérifie que les informations utilisées pour contrôler l'identité et les attributs du certificat RA sont toujours valables, selon les procédures définies aux articles 3.2.2 et 3.2.3 ci-dessus.

4.6.2 Personne pouvant demander le renouvellement d'un certificat

L'AC SSL CERTINOMIS envoie des messages d'information d'arrivée en période de renouvellement au contact technique du client SSL.

4.6.3 Traitement des demandes de renouvellement d'un certificat

Même procédure que celle définie aux articles 4.1.2, 4.2 et 4.3.1 conformément au processus de vérification défini à l'article 3.3.

4.6.4 Notification au client de l'émission d'un nouveau certificat

Même procédure que celle définie à l'article 4.3.2.

4.6.5 Conduite constituant l'acceptation du renouvellement d'un certificat

Même procédure que celle définie à l'article 4.4.1.

4.6.6 Publication par l'AC du renouvellement d'un certificat

Même procédure que celle définie à l'article 4.4.2.

4.6.7 Notification de l'émission d'un certificat par l'AC à d'autres entités

Même procédure que celle définie à l'article 4.4.3.

4.7 Changement de clés (ou certification d'une nouvelle clé publique)

Changement de clé signifie qu'un certificat est créé pour une organisation en utilisant une nouvelle bi-clé.

4.7.1 Motifs de changement de clés

Les motifs de changement de bi-clé sont :
- La compromission de clé;
- La fin de vie de clé;
- La révocation du certificat de l'organisation.

4.7.2 Personne pouvant demander le changement de clés

La même personne que celle définie à l'article 4.1.1.

4.7.3 Traitement des demandes de recertification

Même procédure que celle définie aux articles 4.1.2, 4.2 et 4.3.1 conformément au processus d'authentification défini à l'article 3.3.

4.7.4 Notification au client de l'émission du nouveau certificat

Même procédure que celle définie à l'article 4.3.2.

4.7.5 Conduite constituant l'acceptation d'un certificat avec nouveau bi-clé

Même procédure que celle définie à l'article 4.4.1.

4.7.6 Publication du nouveau certificat par l'AC

Même procédure que celle définie à l'article 4.4.2.

4.7.7 Notification de l'émission d'un nouveau certificat par l'AC à d'autres entités

Même procédure que celle définie à l'article 4.4.3.

4.8 Modification d'un certificat

La modification d'un certificat signifie qu'un nouveau certificat qui contient des informations différentes est créé avec la même clé publique.

Le renouvellement d'un certificat n'est possible que lorsque la durée de vie restante de la bi-clé est conforme aux recommandations en la matière (notamment par rapport à la longueur des clés).

4.8.1 Motifs de modification d'un certificat

Le changement d'identité contenue dans un certificat est un motif possible de modification d'un certificat. Pour autant le changement de certificat n'est pas obligatoire dans ce cas.

4.8.2 Personne pouvant demander la modification d'un certificat

Même procédure que celle définie à l'article 4.1.1.

4.8.3 Traitement des demandes de modification de certificat

Même procédure que celle définie aux articles 4.1.2, 4.2 et 4.3.1 conformément au processus d'authentification défini à l'article 3.3.

4.8.4 Notification au client de l'émission d'un nouveau modifié

Même procédure que celle définie à l'article 4.3.2.

4.8.5 Conduite constituant l'acceptation d'un certificat modifié

Même procédure que celle définie à l'article 4.4.1.

4.8.6 Publication par l'AC d'un certificat modifié

Même procédure que celle définie à l'article 4.4.2.

4.8.7 Notification de l'émission d'un certificat par l'AC à d'autres entités

Même procédure que celle définie à l'article 4.4.3.

4.9 Révocation et suspension d'un certificat

4.9.1 Motif de révocation d'un certificat

Un certificat SSL est révoqué quand l'association entre ce certificat et la clé publique qu'il certifie n'est plus considéré comme étant valide. Exemples de motifs qui invalident cette association:

- Le nom de domaine enregistré ou le nom de l'organisation change, et le contact technique n'est plus autorisé à utiliser le nom de domaine;
- L'information DN n'est pas renseignée correctement;
- Perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé;
- Le CT a utilisé un DN inexact dans sa demande initiale.
- Fin des services de l'AC SSL CETINOMIS;
- Preuve que l'AC SSL CERTINOMIS a violé les exigences stipulées dans son accord avec KEYNECTIS;
- Modification de la taille des clés imposée par des institutions nationale ou internationale compétentes;

- L'AC SSL CERTINOMIS est révoquée;

Quand l'une quelconque de ces occurrences se produit, le certificat en question devra être révoqué et inscrit sur la LCR.

4.9.2 Origine d'une demande de révocation

Le CT du client SSL peut faire une demande de révocation dans les cas suivants:

- Perte de clé privée, perte de contrôle de clé privée, suspicion de ou compromission de clé;
- Perte du certificat SSL;
- Changement demandé de longueur de clé ou d'algorithme (signature et ou hachage) recommandé par un organisme national ou international compétent;
- Changement de nom d'organisation ou de nom de domaine et le contact technique n'est plus autorisé à utiliser le nom de domaine.
- Le DN inclus dans le certificat est erroné;
- Le CT a utilisé un DN inexact dans sa demande initiale;
- Fin de la relation entre l'AC SSL CERTINOMIS et le client SSL.

L'AC SSL CERTINOMIS peut faire une demande de révocation pour les raisons suivantes:

- Fin des services de l'AC SSL;
- Preuve d'un manquement majeur non résolu après réponse écrite du responsable de l'ACR dans les 30 jours qui suivent sa saisine.;
- Fin de la relation entre l'AC SSL CERTINOMIS et le client SSL.

4.9.3 Procédure de demande de révocation

Le CT transmet à l'AE une demande de révocation contenant au minimum:

- Son identification personnelle;
- Les données "secrètes" qu'il a transmises lors de la demande du certificat dont il demande la révocation (voir article 4.1.2 ci-dessus).

L'AE authentifie la demande de révocation autorisée et la transmet à l'AC SSL CERTINOMIS.

L'AC SSL CERTINOMIS authentifie l'AE et révoque le certificat en activant sa clé privée de signature.

La transmission des informations de l'AE vers l'AC SSL CERTINOMIS est protégée par un lien sécurisé. L'ensemble des opérations de révocation d'un certificat est protégé de manière à garantir l'intégrité, la confidentialité (si nécessaire) et l'origine des données transmises et traitées.

Le CT du client SSL est avisé de la modification de l'état de validité de son certificat. Une fois révoqué, un certificat n'est pas recertifié.

4.9.4 Période de grâce

Il n'y a pas de période de grâce dans le cas d'une révocation. Les parties en question doivent demander la révocation d'un certificat dès lors qu'elles en identifient les conditions.

4.9.5 Délai de traitement d'une révocation

Le service de révocation est disponible pendant les heures ouvrées.

Dans le cas où le CT fait office d'AE, la disponibilité de ce service dépend des conditions opérationnelles de disponibilité de l'organisation (voir article 1.3.5 ci-dessus).

En cas d'indisponibilité du système, du service, ou d'autres éléments qui échappent au contrôle de l'AC SSL CERTINOMIS, cette dernière fait de son mieux pour que l'indisponibilité de ce service ne dépasse pas la durée maximum prévue dans la Déclaration des Pratiques de Certification. L'AC SSL CERTINOMIS devra traiter une demande de révocation dès que possible suivant sa réception et de préférence immédiatement.

4.9.6 Exigences de vérification de révocation pour les tierces parties

Conformément à l'article 4.5.2 ci-dessus, les tierces parties doivent vérifier l'état de validité d'un certificat SSL avant de baser leur confiance sur ce certificat.

La fréquence de contrôle des LCR par les tierces parties relève de leur responsabilité.

S'il est temporairement impossible d'obtenir des informations d'état d'un certificat, les tierces parties ne doivent pas baser leur confiance sur ce certificat, ou doivent en accepter les risques et prendre leur responsabilités quant aux conséquences encourues par l'utilisation de ce certificat.

4.9.7 Fréquences de publication des LCR

Les LCR sont publiées au moins toutes les 24 heures, même s'il n'y a pas de modification de leur contenu. L'AC SSL CERTINOMIS s'assure que l'ancienne LCR est retirée de la publication dès lors que la nouvelle LCR est publiée.

Les LCR sont disponibles 24 heures sur 24 et 7 jours sur 7. En cas d'indisponibilité du système, du service, ou d'autres éléments qui échappent au contrôle de l'AC SSL CERTINOMIS, cette dernière fait de son mieux pour que l'indisponibilité de ce service ne dépasse pas la durée maximum prévue dans la Déclaration des Pratiques de Certification.

Le délai de publication de la révocation d'un certificat au profit des tierces parties est pratiquement immédiat et ne dépasse jamais 24 heures.

4.9.8 Possibilité de vérifier l'état des certificats en ligne

Sans objet.

4.9.9 Exigences de vérification en ligne de l'état des certificats

Sans objet.

4.9.10 Autres formes de publication des révocations

Sans objet.

4.9.11 Exigences spécifiques concernant la compromission des clés

Il n'y a pas d'exigences autres que celle de l'article 4.9.3 ci-dessus.

4.9.12 Motifs de suspension d'un certificat

Non applicable.

4.9.13 Personne pouvant demander la suspension d'un certificat

Non applicable.

4.9.14 Procédure de demande de suspension d'un certificat

Non applicable.

4.9.15 Limites de la période de suspension

Non applicable.

4.10 Service d'état des certificats

4.10.1 Caractéristiques opérationnelles

L'information d'état des certificats est disponible au travers du service de publication de l'AC SSL CERTINOMIS conformément à l'article 2 ci-dessus.

4.10.2 Disponibilité du service

Le service de publication est disponible conformément à l'article 2.3 ci-dessus.

4.10.3 Options

Sans objet.

4.11 Fin d'abonnement

Les certificats SSL qui ne sont pas expirés avant la fin de l'abonnement sont révoqués.

Quand un client met fin à son abonnement à l'AC SSL CERTINOMIS, toutes les garanties dont bénéficie le certificat SSL conformément à la présente PC cessent d'être applicables et sont révoquées.

4.12 Séquestre et recouvrement de clés

Les clés des certificats SSL ne font pas l'objet de séquestre de la part de l'AC SSL CERTINOMIS.

5 MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN OEUVRE

5.1 Sécurité physique

La politique de sécurité physique et environnementale applicable à la gestion du cycle de vie des certificats SSL et des éléments cryptographiques traite du contrôle d'accès physique, de la protection contre les désastres naturels, l'incendie, les pannes de servitudes (alimentation électrique, télécommunications), l'effondrement des structures, les dégâts des eaux, la protection contre le vol, l'intrusion, la reprise d'activité etc. Des contrôles sont mis en œuvre afin d'éviter le vol, la dégradation, la compromission de biens et l'interruption des activités des activités commerciales et le vol d'information ou de moyens de traitement de l'information.

Toutes les mesures mises en œuvre, installations et moyens sont conformes aux lois et règlements applicables localement.

Lesdites mesures sont assurées par KEYNECTIS en sa qualité d'opérateur de certification de CERTINOMIS pour les services qui la concerne, conformément au contrat qui les lie. Lesdites mesures s'appliquent également à CERTINOMIS en sa qualité de composante d'AC pour les services qui la concerne, en particulier pour les services d'enregistrement.

5.1.1 Emplacement des sites et construction

Les installations sensibles et critiques de traitement de l'information mises en œuvre au profit de l'AC SSL sont hébergées dans des zones sécurisées, protégées par des périmètres de sécurité présentant des barrières et des contrôles d'accès. Elles sont physiquement protégées des accès non autorisés, des dégradations et des interférences. Les moyens de protection mise en œuvre sont le résultat de l'analyse de risque conduite par l'AC SSL CERTINOMIS.

5.1.2 Accès physique

Les locaux utilisés dans le cadre de la gestion du cycle de vie des certificats SSL (incluant le service de révocation) et des éléments cryptographiques sont mis en œuvre dans un environnement qui protège physiquement les services des compromissions dues aux accès non autorisés aux systèmes ou données. Toutes personne qui pénètre physiquement ces zones ne doit pas rester sans surveillance par une personne autorisée pendant une période significative. Toutes le barrières physiques et tous les moyens de contrôle sont placés sous le contrôle de l'AC SSL CERTINOMIS.

5.1.3 Alimentation et climatisation

L'AC SSL s'assure que les moyens d'alimentation électrique et de climatisation sont dimensionnés pour supporter la mise en œuvre des moyens de gestion du cycle de vie des certificats SSL selon les engagements de service, par mise en œuvre d'installations redondantes.

5.1.4 Exposition à l'eau

L'AC SSL s'assure que les systèmes de gestion du cycle de vie des certificats SSL sont protégés contre les dégâts des eaux.

5.1.5 Système de détection et d'extinction d'incendie

L'AC SSL s'assure que les systèmes de gestion du cycle de vie des certificats SSL sont protégés par un système de détection et d'extinction d'incendie.

5.1.6 Supports

Les supports utilisés par l'AC SSL CERTINOMIS sont manipulés de manière à les protéger des dommages, du vol et des accès non autorisés. Les procédures de gestion des supports les protègent contre l'obsolescence et la détérioration pendant la période durant laquelle les archives doivent être conservées. Tous les supports sont manipulés de manière sécurisée conformément aux exigences du plan de classification des informations et les supports contenant des informations sensibles sont mis au rebut de manière sécurisée quand ils ne sont plus d'aucune utilité.

5.1.7 Mise au rebut

Tous les supports utilisés pour la conservation des informations, tels que clés, données d'activation, ou dossiers de l'AC SSL CERTINOMIS seront déclassifiés ou détruits avant d'être mis au rebut.

5.1.8 Sauvegardes hors site

Des sauvegardes complètes des systèmes de l'AC SSL CERTINOMIS, suffisantes pour permettre la reprise suite à une panne système, sont effectuées périodiquement comme décrit dans la DPC. Des copies de sauvegarde des informations commerciales et des logiciels sensibles sont effectuées régulièrement. Des installations de sauvegarde adéquates, pour s'assurer que toutes les informations commerciales et les logiciels essentiels peuvent être récupérés suite à un sinistre ou à une défaillance de support, sont utilisées. Les équipements de sauvegarde des systèmes individuels sont régulièrement testés pour s'assurer qu'ils répondent aux exigences des plans de reprise d'activité. Au moins une copie de sauvegarde complète est stockée à l'extérieur des locaux (en un lieu différent de celui où se trouvent les matériels de l'AC SSL CERTINOMIS). Les sauvegardes sont conservées dans un site où les contrôles physiques et de procédure sont équivalents à ceux mis en œuvre au site opérationnel de l'AC SSL CERTINOMIS.

5.2 Mesures procédurales

5.2.1 Rôles de confiance

Un rôle de confiance est un rôle qui peut avoir des conséquences en termes de sécurité s'il n'est pas tenu correctement, que ce soit par malveillance ou accidentellement. Les fonctions exécutées dans ces rôles constituent le fondement de la confiance dans l'exploitation de l'AC SSL CERTINOMIS.

Les rôles de confiance comprennent des rôles avec les responsabilités suivantes:

- Officier de sécurité: Responsabilité générale pour la mise en oeuvre des procédures de sécurité;
- Administrateur: Approuve la production/révocation/suspension des certificats;
- Ingénieur systèmes: Autorisé à installer, configurer et maintenir les systèmes de confiance de l'AC SSL CERTINOMIS pour l'enregistrement, la production de certificats, l'exploitation des modules cryptographiques et la gestion des révocations;
- Opérateur: Responsable de l'utilisation quotidienne des systèmes de confiance de l'AC SSL CERTINOMIS. Autorisé à effectuer la sauvegarde et la récupération des systèmes;
- Contrôleur: Autorisé à examiner les archives et les journaux d'audit des systèmes de confiance de l'AC SSL CERTINOMIS;
- Détenteur des données d'activation de l'AC SSL CERTINOMIS: une personne autorisée à détenir les données d'activation de l'AC SSL CERTINOMIS nécessaires à l'exploitation des modules cryptographiques.

Tous les personnels de l'AC SSL CERTINOMIS sont formellement affectés à des rôles de confiance par des personnes responsables de l'AC SSL CERTINOMIS.

5.2.2 Nombre de personnes exigées par tâche

Le nombre de personnes requises pour fournir les services de l'AC SSL CERTINOMIS est détaillé dans la DPC. Il s'agit d'organiser la confiance dans tous les services de l'AC SSL CERTINOMIS (production de clés, production de certificats, révocation) de manière à ce que toute activité malveillante nécessite une collusion. Quand un contrôle par plusieurs personnes est nécessaire, au moins l'un des participants devra être un Administrateur. Tous les participants devront avoir un rôle de confiance tel qu'il est défini à l'article 5.2.1.

Les opérations d'enregistrement effectuées pour le compte de l'AC SSL CERTINOMIS nécessitent l'intervention de deux personnes dans des rôles de confiance.

5.2.3 Identification et vérification pour chacun des rôles de confiance

Avant de se voir affecter un rôle dans l'AC SSL CERTINOMIS, toute personne fait l'objet de contrôles préalables.

Chaque personne jouant un rôle tel qu'il est défini dans la présente PC est identifiée et authentifiée de manière à garantir que la bonne personne est assignée au bon rôle afin d'exécuter ses tâches au profit de l'AC SSL. La DPC décrit les mécanismes utilisés pour identifier et authentifier la personne.

5.2.4 Rôles nécessitant une séparation des tâches

La séparation des tâches est réalisée soit par utilisation de matériels, soit procéduralement, soit par la combinaison des deux moyens. Les membres du personnel de l'AC SSL CERTINOMIS se voient assignés individuellement l'un des rôles définis à l'article 5.2.1 ci-dessus. Il est interdit d'avoir, en même temps, les rôles suivants:

- Officier de sécurité et Ingénieur système ou Opérateur;
- Contrôleur et Officier de sécurité ou Opérateur ou Administrateur ou Ingénieur système;
- Ingénieur système et Opérateur.

Aucune personne ne se verra affecter plus d'une seule identité.

5.3 Mesures de contrôle du personnel

5.3.1 Exigence en matière de qualifications, d'expérience, et d'habilitation

L'AC SSL CERTINOMIS emploie en nombre suffisant des personnels possédant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services. Le personnel de l'AC SSL CERTINOMIS satisfait aux exigences en matière de "connaissances spécifiques, expérience et qualifications" suite à leur formation et selon les diplômes associés, leurs antécédents professionnels, ou une combinaison des deux. Les rôles de confiance et les responsabilités telles qu'ils sont décrits dans la DPC de l'AC SSL CERTINOMIS, sont documentés dans les fiches de poste et clairement identifiés. Les membres du personnel de l'AC SSL CERTINOMIS (temporaires et permanents) ont des fiches de poste fondées sur le principe de la séparation des tâches et le besoin d'en connaître, la détermination de la sensibilité des postes étant fondée sur les tâches et le niveau d'accès, la vérification des antécédents, la formation et la sensibilisation des employés. Le personnel de l'AC SSL CERTINOMIS devra être formellement assigné aux rôles de confiance par le membre de la Direction responsable de la sécurité.

Les fiches de poste comprennent des exigences en matière de compétence et d'expérience. Les membres du personnel de la Direction de l'AC SSL ont une expérience ou une formation en matière de technologie de signature électronique. Les membres du personnel exerçant des responsabilités en matière de sécurité ont une bonne pratique des procédures de sécurité, ainsi qu'une expérience en matière de sécurité de l'information et d'évaluation des risques suffisante.

5.3.2 Procédures de vérification des antécédents

Aucun des membres du personnel de l'AC SSL CERTINOMIS dans un rôle de confiance ne devra avoir d'engagement ou de lien qui risque de causer un conflit d'intérêt avec les tâches qui lui incombent et porter ainsi préjudice à l'impartialité de l'exploitation de l'AC. L'AC SSL CERTINOMIS ne devra pas affecter à des rôles de confiance ou à sa Direction des personnes ayant été condamnées pour crime grave ou autre délit affectant sa qualification pour ce poste. Les membres du personnel ne devront pas avoir accès à des fonctions de confiance tant que les vérifications nécessaires n'auront pas été effectuées. L'AC SSL CERTINOMIS demande aux candidats de fournir leur extrait de casier judiciaire au préalable de leur embauche et rejette leur candidature en cas de refus. Toute personne assumant un rôle de confiance sera sélectionnée sur des critères de loyauté, fidélité, intégrité et fera l'objet de vérifications d'antécédents.

5.3.3 Exigences en matière de formation professionnelle

L'AC SSL CERTINOMIS s'assure que tous les membres du personnel qui accomplissent des tâches touchant à l'exploitation de l'AC SSL CERTINOMIS ont reçu une formation complète concernant:

- Les principes de sécurité et les mécanismes de fonctionnement de l'AC ou de l'AE;
- Les versions des logiciels utilisées dans le système ICP de l'AC;
- Les tâches qu'ils devront accomplir;
- Les procédures de reprise d'activité après sinistre.

Les membres du personnel de l'AC SSL et de l'AE de CERTINOMIS devront suivre une formation complémentaire quand des modifications auront été apportées aux systèmes de l'AC SSL ou de l'AE de CERTINOMIS. Des cours de mise à jour seront dispensés en fonction des besoins. L'AC SSL CERTINOMIS devra revoir ces besoins au moins une fois par an.

5.3.4 Formation professionnelle – Fréquence et exigences

Les personnes assumant des rôles de confiance devront être au courant des modifications apportées à l'exploitation de l'AC SSL CERTINOMIS, en fonction des besoins. Toute modification significative apportée à cette exploitation devra entraîner un plan de formation (sensibilisation), l'exécution de ce plan devra être documentée.

5.3.5 Rotation des emplois

L'AC SSL CERTINOMIS s'assure que tout changement en matière de personnel n'affectera pas l'efficacité opérationnelle du service ou la sécurité des systèmes.

5.3.6 Sanctions en cas d'actions non autorisées

Des sanctions disciplinaires adéquates sont prises à l'encontre des membres du personnel violant la PC ou la DPC.

5.3.7 Contrôle des personnels des entreprises cocontractantes

Les exigences relatives aux personnels des entreprises sous-traitantes ayant à réaliser des fonctions d'exploitation de l'AC SSL CERTINOMIS sont identiques à celles relatives aux personnels de l'AC SSL CERTINOMIS, en particulier à celles décrites à l'article 3 ci-dessus.

5.3.8 Documentation fournie au personnel

L'AC SSL CERTINOMIS met à la disposition des membres de son personnel la présente Politique de Certification (PC) et la Déclaration des Pratiques de Certification (DPC) associée, ainsi que le texte de toute loi, toute politique ou tout contrat qui s'appliquent aux postes qu'ils occupent. Tout autre document technique, d'exploitation, ou administratif (par ex. le Manuel de l'Administrateur, le Manuel de l'Utilisateur, etc..) est fourni aux membres du personnel de confiance pour leur permettre d'exécuter les tâches qui leur incombent.
Un suivi nominatif des membres du personnel ayant reçu une formation et mentionnant le niveau de cette formation sera tenu à jour.

5.4 Procédures de journalisation

5.4.1 Evènements journalisés

Tous les événements ayant trait à la sécurité et aux services des composantes de l'AC SSL CERTINOMIS sont consignés dans des registres ou journaux de vérification (audit). Dans la mesure du possible, les informations sur la sécurité seront recueillies automatiquement. Si ce n'est pas possible, un registre journal, un formulaire, ou tout autre dispositif physique sera utilisé. Tous les registres de vérification de sécurité, électroniques ou non électroniques, seront conservés et présentés à l'occasion des contrôles de conformité. L'AC SSL CERTINOMIS s'assure que tous les événements relatifs au cycle de vie des certificats sont consignés de manière à en assurer l'imputabilité.

Les détails concernant ce qui doit être consigné sont précisés dans la DPC. Au minimum, chaque registre de vérification doit inclure les éléments suivants (recueillis soit automatiquement soit manuellement pour tout événement à vérifier):

- Le type d'événement,
- La date et l'heure de son occurrence,
- Son succès ou son échec selon le cas,
- L'identité de l'entité et/ou de l'opérateur qui a provoqué l'événement,
- L'identité du destinataire de l'événement ;
- La cause de l'événement.

5.4.2 Fréquence de journalisation

Les journaux sont revus mensuellement pour rechercher toute preuve d'activité malveillante, ainsi qu'à la suite de chaque opération importante.

5.4.3 Période de rétention des journaux

Les registres concernant l'AC SSL CERTINOMIS et les certificats de l'AC SSL sont conservés sur site pendant au moins un mois avant archivage.

5.4.4 Protection des journaux

Les événements sont consignés de manière à s'assurer que seuls les personnels autorisés puissent y avoir accès.
Les événements sont consignés de manière à ce qu'ils ne puissent pas être aisément effacés ou détruits (sauf pour leur transfert vers un support durable) pendant la période durant laquelle ils doivent être conservés.
Les événements sont protégés de manière à ce qu'ils soient lisibles pendant toute la durée de leur conservation.

5.4.5 Procédures de sauvegarde des journaux

Les journaux d'audit et les résumés des audits sont sauvegardés en lieu sûr, sous le contrôle d'un personnel dans un rôle de confiance et séparés de leur source de génération. Les sauvegardes des journaux de vérification sont protégées avec le même niveau de confiance que le journal original.

5.4.6 Système de collecte des journaux (interne & externe)

Le système de collecte des journaux de vérification peut ou non être extérieur à l'AC SSL CERTINOMIS.
Le processus de collecte sera lancé au démarrage du système, et interrompu seulement à l'arrêt du système. Le système de collecte des journaux de vérification doit préserver l'intégrité et la disponibilité des données recueillies. Si nécessaire, le système de collecte des journaux protége la confidentialité des données. Si un problème survient durant la collecte des journaux, l'AC SSL CERTINOMIS décide de suspendre ou non l'exploitation de l'AC SSL CERTINOMIS jusqu'à ce que le problème soit résolu et en informe les composantes concernées.

5.4.7 Notification au responsable de l'évènement

Sans objet.

5.4.8 Evaluation des vulnérabilités

Le contrôleur explique tous les événements significatifs dans un résumé d'audit. Le processus de vérification inclut de vérifier que le journal n'a pas subi de modification non autorisée, qu'il ne comporte pas de discontinuité ou autre perte de données de vérification, puis de vérifier rapidement toutes les saisies, enfin d'effectuer une enquête plus approfondie sur toute alerte ou irrégularité relevée dans les journaux. Les mesures prises suite à ces vérifications sont documentées.

5.5 Archivage des journaux

5.5.1 Journaux à archiver

Les journaux archivés devront être assez détaillés pour établir la validité d'une signature et de l'exploitation correcte de l'ICP. Au minimum, les données suivantes devront être archivées:

- Enregistrement des événements de l'AC SSL CERTINOMIS;
- Documentation des audits de l'AC SSL CERTINOMIS;
- Documents PC de l'AC SSL CERTINOMIS;
- Documents DPC de l'AC SSL CERTINOMIS;
- Tout accord contractuel entre un client et l'AC SSL CERTINOMIS;
- Configuration matérielle du système;
- Certificats et LCR (ou autres informations de révocation);
- Autres données ou applications suffisantes pour vérifier le contenu des archives;
- Tous les échanges entre l'AC SSL CERTINOMIS et les auditeurs de conformité au regard de l'audit de conformité de l'AC SSL CERTINOMIS vis-à-vis des exigences du RESPONSABLE DE L'ACR.

5.5.2 Durée de rétention des archives

La durée minimale de rétention des données archivées est de 10 ans.

5.5.3 Protection des archives

Les archives sont créées de manière à ne pas pouvoir être aisément effacées ou détruites (sauf pour leur transfert vers un support durable) pendant la période durant laquelle elles doivent être conservées.
Les événements sont consignés de manière à s'assurer que seuls les personnels autorisés puissent y avoir accès.
Si le support original ne peut pas conserver les données pendant la période exigée, un mécanisme destiné à les transférer périodiquement vers un nouveau support sera mis en place.

5.5.4 Sauvegarde des archives

Sans objet.

5.5.5 Exigences d'horodatage des enregistrements

Si un service d'horodatage est utilisé pour dater les enregistrements, il doit répondre aux exigences formulées à l'article 6.8.

5.5.6 Système de collecte des archives (interne or externe)

Le système de collecte des archives respecte les exigences de sécurité définies à l'article 5.3 ci-dessus.

5.5.7 Procédure d'obtention et de vérification des données archivées

Les supports servant à archiver les informations de l'AC SSL CERTINOMIS sont vérifiés lors de leur création. Périodiquement, des échantillons statistiques des informations archivées sont testés pour en vérifier l'intégrité et la lisibilité des informations.
Seuls des matériels, des rôles de confiance et autres personnes autorisées (autorité judiciaire) par l'AC SSL CERTINOMIS peuvent accéder aux archives.

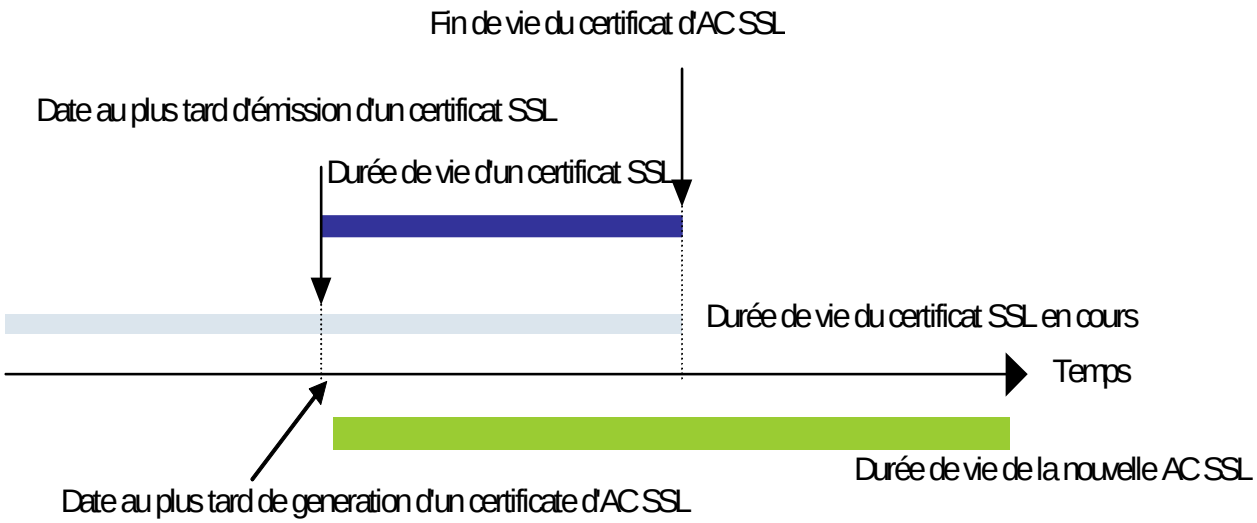
5.6 Renouvellement de clé

5.6.1 Certificat d'AC SSL

La durée de vie d'un certificat d'AC SSL est précisée dans la DPC et déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés notamment.

Une AC SSL ne peut pas générer de certificats SSL dont la durée de vie dépasse la période de validité du certificat d'AC SSL. C'est pourquoi, la bi-clé d'une AC SSL est renouvelée au plus tard à la date d'expiration du certificat d'AC SSL moins la durée de vie des certificats SSL émis.

Dès qu'une nouvelle clé privée est générée pour l'AC SSL, seule celle-ci est utilisée pour générer de nouveaux certificats SSL et les LCR associées. Le précédent certificat d'AC SSL reste valable pour valider le chemin de certification des anciens certificats SSL émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats SSL émis à l'aide de cette clé. Cette clé privée peut également être utilisée pour signer les LCR associées aux anciens certificats SSL émis.



Par ailleurs, l'AC SSL CERTINOMIS change sa clé et le certificat correspondant quand elle cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si elle est compromise. Le RESPONSABLE DE L'ACR se réserve le droit de prendre la décision de demander à l'AC SSL de changer sa clé à tout moment, et dans ce cas l'AC SSL CERTINOMIS procédera au changement demandé.

5.6.2 Certificat SSL

La durée de validité d'un certificat SSL est de 1 ou 2 ans, selon la longueur des clés utilisées et selon les recommandations des autorités nationales ou internationales compétentes.

5.7 Compromission et plan de reprise

5.7.1 Procédures en cas d'incident et de compromission

L'AC SSL a établi un plan de continuité de service qui met en évidence les différentes étapes à exécuter dans l'éventualité de la corruption ou de la perte des ressources système, des logiciels et ou des données et qui pourraient perturber ou compromettre le bon déroulement des services d'AC SSL.

L'AC SSL CERTINOMIS a conduit une analyse de risque pour évaluer les risques métier et déterminer les exigences de sécurité et procédures opérationnelles afin de rédiger un plan de reprise d'activité. Les risques pris en compte sont régulièrement revus et le plan est révisé en conséquence. Le plan de continuité de l'AC SSL fait partie du périmètre audité, selon l'article 8 ci-dessous.

Les personnels de l'AC SSL dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas où l'AC SSL CERTINOMIS détecte une tentative de piratage ou une autre forme de compromission, elle mène une analyse afin de déterminer la nature des conséquences et leur niveau.

Si nécessaire, l'ampleur des conséquences est évalué par la société CERTINOMIS afin de déterminer : si les services de l'AC SSL doivent être rétablis, si certains certificats SSL doivent être révoqués, si l'AC SSL doit être déclarée compromise, si certains services peuvent être maintenus (en priorité les services de révocation et de publication d'état des certificats SSL) et, le cas échéant, par quels moyens, selon le plan de reprise d'activité.

5.7.2 Corruption des ressources informatiques, des logiciels, et/ou des données

Si le matériel de l'AC SSL est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des service de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC SSL.

5.7.3 Procédures en cas de compromission de la clé privée d'une entité

Si la clé de signature de l'AC SSL est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- L'AC SSL CERTINOMIS, après enquête sur l'évènement décide de révoquer le certificat de l'AC SSL;
- Tous les clients dont les certificats ont été émis par l'AC SSL compromise, sont avisés dans les plus brefs délais que le certificat d'AC SSL a été révoqué;
- L'AC SSL décide ou non de générer un nouveau certificat d'AC SSL;
- Une nouvelle bi-clé AC SSL est générée et un nouveau certificat d'AC SSL est demandé à l'ACR;
- Les clients SSL sont informés de la capacité retrouvée de l'AC SSL de générer des certificats SSL.

5.7.4 Capacités de reprise d'activité à la suite d'un sinistre

Le plan de récupération après sinistre traite de la continuité d'activité telle qu'elle est décrite à l'article 5.7.1. Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

5.8 Fin de vie d'AC SSL

En cas de fin de vie ou de fin d'activité, l'AC SSL doit :

- Arrêter d'émettre des certificats SSL;
- Archiver tous les journaux de vérification et autres enregistrements avant la fin de l'activité;
- Détruire toutes ses clés privées à la fin de l'activité;
- Obtenir l'approbation des contacts techniques avant de transmettre toute information appartient au client SSL;
- Transférer tous les enregistrements à une autorité appropriée.

6 MESURES TECHNIQUES DE SECURITE

Dans le cadre du présent document, il convient de rappeler que lesdites mesures sont assurées par KEYNECTIS en sa qualité d'opérateur de certification de CERTINOMIS, conformément au contrat qui les lie.

6.1 Génération et installation des bi-clés

6.1.1 Génération des bi-clés

La génération des clés d'AC SSL est réalisée dans un environnement physique sécurisé par au moins deux personnes dans des rôles de confiance et en présence de témoins. Les données d'activation de la clé privée sont distribuées à des porteurs qui sont des personnes habilitées. La génération des clés d'AC SSL est réalisée à l'aide de ressources cryptographiques matérielles.

6.1.2 Fourniture de la clé privée à l'abonné

Le client SSL génère lui-même sa bi-clé.

6.1.3 Fourniture de la clé publique à l'AC

La clé publique est transmise à l'AC via l'AE, sous un format PKCS#10 et lors d'une connexion sécurisée par protocole SSL.

6.1.4 Fourniture de la clé publique d'AC SSL aux tierces parties

Les certificats SSL sont mis à disposition des tierces parties au travers du service de publication.

6.1.5 Taille de clés

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats SSL doivent ou ne doivent pas être modifiés.

L'utilisation de l'algorithme RSA avec fonctions de hachage SHA-1 ou SHA-{224, 384, 256, 512} est recommandé par l'AC SSL CERTINOMIS.

La longueur des clés des certificats SSL est d'au moins 1024 bits pour l'algorithme RSA.

6.1.6 Production des paramètres des clés publiques et contrôle de qualité

Les clients SSL génèrent eux-mêmes leurs propres clés selon les exigences techniques de la présente PC et de manière à s'assurer qu'il n'y a pas de traces ou d'informations existantes qui pourraient permettre de recouvrer les clés privées générées.

6.1.7 Utilisation de la clé (selon le champ "key usage" du certificat X 509 V3)

L'utilisation du champ "key usage" dans le certificat SSL est définie à l'article 7 ci-dessous. Le champ "key usage" est fixé de manière à ne permettre à la clé privée et au certificat SSL associé que l'ouverture de sessions sécurisées SSL. Cette restriction est mise en œuvre par utilisation combinée des champs "key usage" et "extended key usage".

6.2 Protection des clés privées et normes relatives au module cryptographique

6.2.1 Normes applicables aux ressources cryptographiques et contrôles

Les ressources cryptographiques de l'AC SSL sont certifiées au niveau EAL 4+ selon les critères communs.

Les clients SSL sont responsables du choix des moyens cryptographiques (matériels, logiciels) utilisés au profit du propriétaire du nom de domaine.

6.2.2 Contrôle de la clé privée par de multiples personnes

L'activation de la clé privée d'AC SSL est contrôlée par au moins 3 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée d'AC SSL font l'objet d'une authentification forte.

Les clients SSL sont responsables de la protection et du contrôle de leurs clés privées, de manière à ce que seules les utilisations autorisées sont possibles.

6.2.3 Séquestre de clé privée

Les clés privées d'AC SSL ne font jamais l'objet de séquestre.

6.2.4 Sauvegarde de clé privée

Les clés d'AC SSL sont sauvegardées sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées ont été réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC SSL. Les sauvegardes de clés privées d'AC SSL sont stockées dans des ressources cryptographiques matérielles ou sous forme chiffrée.

6.2.5 Archivage de clé privée

Les clés privées d'AC SSL ne font jamais l'objet d'archives.

6.2.6 Importation / exportation d'une clé privée

Les clés d'AC SSL sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC SSL sont chiffrées au moyen de l'algorithme AES (FIPS 197) ou 3DES. Une clé privée d'AC SSL chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

6.2.7 Stockage d'une clé privée dans un module cryptographique

Les clés privées d'AC SSL stockées dans des ressources cryptographique matérielles sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées.

6.2.8 Méthode d'activation d'une clé privée

Les clés privées d'AC SSL ne peuvent être activées qu'avec un minimum de trois personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC SSL en question.

6.2.9 Méthode de désactivation d'une clé privée

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC SSL ont été activées ne sont pas laissées sans surveillance ou accessible à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

Les ressources cryptographiques de signature de l'AC SSL sont en ligne uniquement afin de signer des certificats SSL après avoir authentifié l'AE.

6.2.10 Méthode de destruction d'une clé privée

Les clés privées d'AC sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

6.2.11 Certification des ressources cryptographiques

Les ressources cryptographiques matérielles utilisées par l'AC SSL CERTINOMIS sont certifiées au niveau EAL4+ selon les critères communs (norme ISO 15408), ou plus.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (voir article 5.5.2 ci-dessus).

6.3.2 Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés

La durée de vie opérationnelle d'un certificat est limitée par son expiration ou sa révocation. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond.

Comme une AC SSL ne peut émettre de certificats SSL d'une durée de vie supérieure à celle de son propre certificat, la bi-clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC SSL moins la durée de vie des certificats SSL émis.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation des clés privées d'AC SSL sont générées durant les cérémonies de clés (voir article 6.1.1). Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

Les clients SSL ont la responsabilité de faire en sorte que les clés privées qu'ils gèrent sont protégées par des données d'activation "fortes". Des informations complémentaires sont données dans la DPC.

6.4.2 Protection des données d'activation

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation sont responsables de leur gestion et de leur protection. Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'un même AC SSL à un même instant.

Le RESPONSABLE DE L'ACR recommande que les données d'activation soient stockées dans des coffres personnels dont l'accès est contrôlé par le porteur lui-même et une autre personne dans un rôle de confiance.

Les clients SSL s'assurent que les données d'activation de leur clés privées ne peuvent être activées que par une entité autorisée (personne et ou machine).

6.4.3 Autres aspects touchant aux données d'activation

Les données d'activation sont changées dans le cas ou les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance. Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

6.5 Mécanismes de sécurité des systèmes informatiques

6.5.1 Exigences techniques de sécurité des ressources informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une AC SSL comprend les fonctions suivantes :

- Authentification des rôles de confiance;
- Contrôle d'accès discrétionnaire;
- Interdiction de la réutilisation d'objets;

- Exige l'utilisation de la cryptographie lors des communications et pour la sécurité des bases de données;
- Requiert l'identification des utilisateurs;
- Assure la séparation rigoureuse des tâches;
- Fournit une autoprotection du système d'exploitation.

Quand un composant d'ICP est hébergé sur une plate forme évaluée au regard d'exigences d'assurance de sécurité, il doit être utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'ICP sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC SSL.

6.5.2 Indice de sécurité informatique

Les composants d'ICP utilisés pour supporter les services d'AC SSL de CERTINOMIS et qui sont hébergés par KEYNECTIS ont été conçus en suivant les recommandations du document du CEN CWA 14167-1 "Security requirement for trustworthy system managing digital certificates for electronic signatures".

6.6 Contrôles techniques du système pendant son cycle de vie

6.6.1 Contrôle des développements des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :
- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce;
- Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation;
- Les matériels et logiciels sont dédiés aux activités d'ICP. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'ICP.
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'ICP. Seules les applications nécessaires à l'exécution des activités ICP sont acquises auprès de sources autorisées par politique applicable de l'AC SSL. Les matériels et logiciels de l'AC SSL font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite;
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installées par des personnels de confiance et formés selon les procédures en vigueur.

6.6.2 Contrôles de gestion de la sécurité

La configuration du système d'AC SSL, ainsi que toute modification ou évolution, est documentée et contrôlée par la Direction de l'AC SSL CERTINOMIS. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC SSL. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'ICP. Lors de son premier chargement, on vérifie que le logiciel de l'ICP est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

6.6.3 Contrôle de sécurité du système pendant son cycle de vie

En ce qui concerne les logiciels et matériels évalués, l'AC SSL CERTINOMIS poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

6.7 Mécanismes de sécurité du réseau

L'AC SSL est en ligne. Les composantes accessibles de l'ICP sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

Les autres composantes ICP de l'AC SSL utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-

feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système ICP est hébergé refuse tout service, hormis ceux qui sont nécessaires au système ICP, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

6.8 Horodatage

Tous les composants de l'AC SSL sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP). Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

- Du début de validité d'un certificat de l'AC;
- De la révocation d'un certificat de l'AC;
- De l'affichage de mises à jour de LCR.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

7 CERTIFICATS, LCR, ET PROFILS OCSP

7.1 Profil de Certificat SSL

Les certificats SSL émis par l'AC SSL CERTINOMIS sont des certificats au format X.509 v3 (populate version field with integer "2").
Les champs des certificats SSL sont définis par le RFC 3280.

Les certificats SSL comprennent au moins les champs suivants:

Organization	Nom du propriétaire de nom de domaine
Common Name	Nom de domaine pleinement qualifié
Country	Pays dans lequel l'organisation est installée
Longueur de clé	Taille des clés utilisées
Durée de validité	Durée de validité du certificat (selon longueur de clés : 1 ou 2 ans)

7.1.1 Extensions de Certificats SSL

Pour un certificat SSL, les extensions suivantes, au moins, sont utilisées :
- Authority Key Identifier (champ marqué non critique);
- Key usage (champ marqué critique);
- Subject Key Identifier (champ marqué non critique);
- CRL Distribution Points (champ marqué non critique);
- Basic Constraints (champ marqué critique)
- Extended key usage (champ marqué critique).

La DPC précise les éventuelles autres extensions utilisées.

7.1.2 Identifiant d'algorithmes

Sha-1WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}.
Sha-256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}.
Sha-384WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}.
Sha-512WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}.
Sha-224WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 14}.

7.1.3 Formes de noms

Les formes de noms respectent les exigences de l'article 3.1 ci-dessus.

7.1.4 Identifiant d'objet (OID) de la Politique de Certification

Le certificat SSL contient l'OID de la PC qui supporte son émission.

7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies"

Pas d'exigence formulée.

7.2 Profil de LCR

L'AC SSL émet des LCR X.509 version deux (v2).
Les champs de la LCR sont ceux définis dans le RFC 3280.

La LCR de l'AC SSL contient les champs suivants :
- Version de la LCR
- Emetteur de la LCR
- Date de validité
- Date de prochaine mise à jour
- Algorithmes utilisés pour le hachage et la signature

7.2.1 LCR et champs d'extensions des LCR

La DPC donne les détails relatifs aux champs d'extension des LCR.

7.3 Profil OCSP

Si un service OCSP est mis à dispostion, il sera conforme au RFC2560.

7.3.1 Numéro de version

Si un service OCSP est mis à disposition, la DPC préciser quelle version est utilisée.

7.3.2 Extensions OCSP

Si un service OCSP est mis à disposition, la DPC précisera les extensions utilisées.

8 CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et motifs des audits

L'AC SSL fait l'objet d'audit périodique de conformité au mois une fois par an, pour permettre à la société CERTINOMIS d'autoriser l'AC SSL d'émettre ou non (selon le résultat des audits) des certificats SSL au titre de la présente PC.

La société CERTINOMIS a le droit de demander la réalisation d'audits de conformité supplémentaires à l'AC SSL qui opère au titre de la présente PC. La société CERTINOMIS doit alors informer de la raison de cette demande.

L'AC SSL CERTINOMIS doit fournir au RESPONSABLE DE L'ACR un rapport d'audit qui démontre la conformité de ses PC et DPC avec la PC de l'ACR et la "PC des services d'AC SSL". Le RESPONSABLE DE L'ACR a le droit de demander la réalisation ou de réaliser un audit de conformité de l'AC SSL CERTINOMIS.

8.2 Identité / Qualification des auditeurs

Les auditeurs doivent démontrer leurs compétences dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la "PC des services d'AC SSL". Les auditeurs en charge de l'audit de conformité doivent effectuer l'audit de conformité comme tâche principale. La société CERTINOMIS apporte une attention particulière quand à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit. La société CERTINOMIS effectue elle-même le choix des auditeurs.

8.3 Lien entre l'auditeur et l'entité contrôlée

Les auditeurs en charge de l'audit de conformité sont soit une entreprise privée indépendante de la société CERTINOMIS, soit une entité suffisamment séparée de l'AC SSL CERTINOMIS afin d'effectuer une évaluation juste et indépendante.

La société CERTINOMIS détermine si un auditeur remplit cette condition.

8.4 Points couverts par l'évaluation

L'objectif de l'audit de conformité est de vérifier qu'une composante de l'AC opère ses services en conformité avec la présente PC et sa DPC.

8.5 Mesures prises en cas de non-conformité

La société CERTINOMIS peut décider que l'AC SSL CERTINOMIS ou l'une de ses composantes n'agit pas en conformité avec les obligations définies dans la présente PC. Quand une telle décision est prise, elle peut suspendre les opérations de la composante non conforme de l'AC SSL, ou peut donner l'ordre de cesser toute relation avec la composante SSL en question (par ex. en révoquant le certificat que l'AC SSL a émis), ou peut décider que des actions correctives sont à prendre.

Quand l'auditeur en charge de l'audit de conformité trouve une divergence avec les exigences de la présente PC, les mesures suivantes doivent être prises:

- L'auditeur note la divergence;
- L'auditeur avise l'entité en question de la divergence. L'entité en avise rapidement le RESPONSABLE DE L'ACR;
- La partie responsable de la correction de la divergence détermine quelles sont les mesures à prendre en fonction des exigences de la présente PC, et les effectue sans délai avec l'approbation du RESPONSABLE DE L'ACR.

Suivant la nature et la gravité de la divergence, et la rapidité avec laquelle elle peut être corrigée, le RESPONSABLE DE L'ACR peut décider de suspendre temporairement le fonctionnement de l'AC SSL, de révoquer le certificat émis par l'ACR, ou de prendre toute autre mesure qu'il juge opportune.

Quand les actions correctives sont réalisées, l'AC SSL en informe le RESPONSABLE DE L'ACR et lui fournit un rapport de mise à hauteur, pour évaluation.

8.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant la mention des mesures correctives déjà prises ou en cours par la composante, est remis au RESPONSABLE DE L'ACR et à la société CERTINOMIS comme prévu à l'article 8.1 ci-dessus. Ce rapport cite les versions des PC et DPC utilisées pour cette évaluation. Quand nécessaire, le rapport de contrôle peut être diffusé comme prévu à l'article 8.5 ci-dessus.

Le Rapport de Contrôle de Conformité n'est rendu pas disponible à des tiers utilisateurs sur Internet.

9 AUTRES QUESTIONS COMMERCIALES ET JURIDIQUES

9.1.1 Frais d'émission et de renouvellement de certificats SSL

Des frais d'émission de certificat seront facturés selon une échelle de tarifs diffusés par l'AC sur son site WEB, ou négociés dans le cadre d'un contrat commercial.

9.1.2 Frais d'accès aux certificats SSL

Des frais d'accès au certificat peuvent être facturés par l'AC selon une échelle de tarifs diffusés ou négociés avec l'AC.

9.1.3 Frais d'accès aux LCR et aux informations d'état des certificats SSL

L'accès par l'Internet au service de publication contenant les LCR des AC SSL et des certificats SSL émis est fourni à titre gracieux. Ce service n'est pas fourni à l'attention de services OCSP ou autres services similaires, mais à l'attention de tierces parties pour vérifier l'état de validité des certificats.

9.1.4 Frais pour d'autres services

Aucun frais ne sera facturé pour l'accès en direct à cette Politique de Certification ou aux éléments publiés de la DPC. Cependant, des frais peuvent être facturés pour des copies sur support papier ou par voie électronique.

9.1.5 Politique de remboursement

Aucune exigence particulière.

9.2 Confidentialité des informations

9.2.1 Informations confidentielles

L'AC SSL garantit que seuls ses personnels dans des rôles de confiance autorisés, les personnels contrôleurs dans la réalisation des audits de conformité, ou d'autres personnes détenant le besoin d'en connaître, ont accès aux informations confidentielles suivantes et peuvent les utiliser :

- Registres et archives;
- Données d'identité personnelle;
- Clés privées ICP détenues;
- Données d'activation de l'AC SSL;
- Résultats et rapports de contrôle de conformité;
- Plans de reprise après sinistre;
- Accords contractuels ou non avec l'AC SSL;
- Politique de sécurité interne de l'AC SSL;
- Parties de la DPC considérées comme confidentielles.

9.2.2 Information considérées comme non confidentielles

Aucune des informations publiées dans la présente PC n'est considérée comme confidentielle. Néanmoins, celles-ci peuvent être visées par la loi sur la propriété intellectuelle.

9.2.3 Obligation de protection des informations confidentielles

L'AC SSL CERTINOMIS doit respecter les exigences définies par les lois européennes et françaises concernant la protection des données personnelles (données confidentielles et personnelles).

9.3 Confidentialité des informations à caractère personnel

9.3.1 Plan de confidentialité

L'AC SSL CERTINOMIS recueille, stocke, traite, divulgue de données à caractère personnel dans le respect des principes fondamentaux en matière de protection des données consacrés dans les lois européennes sur la protection des données à caractère personnel.

CERTINOMIS respecte rigoureusement toutes les prescriptions des lois européennes et françaises concernant la gestion et la protection des données à caractère personnel et dispose d'un contact permanent pour s'assurer que l'AC SSL toutes les exigences législatives sur la protection des données à caractère personnel.
L'AC SSL a été auditée sur ces dispositions dans le cadre de l'audit de conformité.

9.3.2 Information considérées comme personnelles

L'AC SSL CERTINOMIS considère que les informations suivantes sont des informations à caractère personnel :

- Formulaire (renseigné) de demande de certificat;
- Formulaire (renseigné) de demande de révocation;
- Motif de révocation.

9.3.3 Information non considérées comme n'étant pas à caractère personnel

Sans objet.

9.3.4 Obligation de protection des informations à caractère personnel

Les composantes ICP de l'AC SSL traitent et protègent toutes les données à caractère personnel de manière à ce que seuls des personnels dans des rôles de confiance (internes ou autorités judiciaires) y aient accès, selon la présente PC.

9.3.5 Consentement exprès et préalable à l'utilisation de données à caractère personnel

Aucune des données à caractère personnel fournies par un client SSL ne peut être utilisée, pour l'exécution des services SSL, sans consentement exprès et préalable de la part de ce client. Ce consentement est considéré comme obtenu lors de la soumission de la demande de certificat et du fait de l'acceptation par le client du certificat d'AC SSL émis par l'AC SSL (en accord avec la présente PC).

9.3.6 Divulgation due à un processus judiciaire ou administratif

L'AC SSL CERTINOMIS agit conformément aux réglementations européenne et française et dispose de procédures sécurisées pour permettre l'accès des autorités judiciaires aux données à caractère personnel.

9.3.7 Autres motifs de divulgation de données à caractère personnel

L'AC SSL obtient l'accord du CT de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit à l'article 5.8.

9.4 Droits relatifs à la propriété intellectuelle

L'AC SSL CERTINOMIS détient tous les droits de propriété intellectuelle et elle est propriétaire de la présente PC et de la DPC associée, du certificat d'AC SSL CERTINOMIS et des informations de révocation correspondantes qu'elle émet.

Les clients SSL détiennent tous les droits de propriété intellectuelle sur les informations contenues dans les certificats SSL émis par l'AC SSL et dont il sont propriétaires.

9.5 Obligations et garanties

9.5.1 Obligations et garanties de l'AC SSL

L'AC SSL s'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de certificats SSL.

L'AC SSL est responsable du maintien de la conformité aux procédures prescrites dans la présente PC, même si les fonctions de l'AC SSL sont déléguées à des sous-traitants. L'AC SSL fournit tous les services de certification en accord avec sa Déclaration des Pratiques de Certification.

Les obligations communes aux composantes de l'ICP AC SSL sont:
- Protéger les clés privées et leurs données d'activation en intégrité et confidentialité;
- N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC;
- Respecter et appliquer les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC doit être transmise à la composante concernée);
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toute information utile, conformément aux intentions du RESPONSABLE DE L'ACR de contrôler et vérifier la conformité avec la "PC des services d'AC SSL" et avec les PC et DPC applicables;
- Respecter totalement ou en partie les conventions qui la lient à l'ACR;
- Respecter totalement ou en partie les conventions qui la lient au client SSL;
- Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale;
- Mettre en oeuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC.

9.5.2 Obligations et garanties du client SSL

L'AC SSL s'engage, suite à la convention passée avec le client SSL, à se conformer aux exigences suivantes de la présente PC. L'AC SSL :

- Doit protéger la confidentialité des informations secrètes utilisées dans le processus d'authentification;
- Doit se conformer à toutes les exigences de la présente PC et de la DPC associée;
- Doit garantir que les informations qu'il fournit à l'AE sont complètes et correctes;
- Doit prendre toutes les mesures raisonnables pour éviter l'utilisation non autorisée de sa clé privée et en protéger la confidentialité;
- Doit aviser immédiatement l'AC SSL d'une demande de révocation.

9.5.3 Obligations et garanties des autres participants

Pas d'exigences.

9.6 Déni de garanties

L'AC SSL CERTINOMIS garantit au travers de ses services :

- L'identification et l'authentification de l'ACR avec son certificat auto signé;
- L'identification et l'authentification de l'AC SSL, avec son certificat généré par l'ACR;
- La gestion des certificats correspondant et des informations de validité des certificats selon la présente PC.

Aucune autre garantie ne peut-être mise en avant par l'AC SSL, les utilisateurs tiers et ou les clients SSL dans leurs accords contractuels (s'il en est).

9.7 Limites de responsabilité

En ce qui concerne les certificats SSL, l'AC SSL est seulement responsable des exigences et des principes édictés dans la présente PC. L'AC SSL est responsable de tout dommage causé à un client SSL ou à un tiers utilisateur en raison d'une exécution incorrecte des procédures définies dans sa PC/DPC.

L'AC SSL CERTINOMIS décline toute responsabilité à l'égard de l'usage qui est fait de certificats ACR, certificats AC SSL et certificats SSL ou des bi-clés publiques/privées associées dans des conditions et à des fins autres que celles prévues dans la présente PC.

9.8 Indemnités

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de CERTINOMIS vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge, toutes causes confondues, ne sauraient en aucun cas dépasser les limites contractuellement prévues dans les conditions générales d'utilisation du Certificat SSL.

9.9 Durée et résiliation

9.9.1 Durée

La présente PC devient effective une fois :
- Approuvée par la société CERTINOMIS;
- Publiée par le SP de l'AC SSL CERTINOMIS.

9.9.2 Résiliation

Une nouvelle version de la présente PC publiée par le SP peut obliger les composantes de l'AC SSL à modifier leurs propres DPC pour demeurer conformes à la nouvelle version de la PC. Les changements possibles devront être notifiés aux composantes en question avec un préavis fixé.

Selon l'importance des modifications apportées à sa PC, la société CERTINOMIS devra décider soit de faire procéder à un audit de la PC/DPC de l'AC SSL concernée, soit de donner instruction à l'AC SSL CERTINOMIS de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé. Suivant l'importance des modifications apportées à la PC, le certificat AC SSL n'est pas obligatoirement recertifiée par anticipation.

9.9.3 Effets de la résiliation et survie

La fin de validité de la présente PC entraîne la cessation de toutes les obligations et responsabilités de l'AC SSL.

9.10 Avis individuels et communication avec les participants

L'AC SSL CERTINOMIS fournit la nouvelle version de la PC au SP dès qu'elle est validée. Les clients SSL doivent être informés de tous les changements envisagés avant la mise en application de la nouvelle PC.

9.11 Amendements

9.11.1 Procédure pour apporter un amendement

L'AC SSL CERTINOMIS révise sa PC et sa DPC au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de l'AC SSL CERTINOMIS. Les corrections de fautes d'orthographe ou de frappe qui ne modifient pas le sens de la PC sont autorisées sans avoir à être notifiées. L'AC SSL CERTINOMIS se doit d'aviser les CT des conséquences et des modifications en cours d'approbation.

9.11.2 Mécanisme et délais des notifications

L'AC SSL CERTINOMIS donne un préavis de 2 mois au moins aux composantes de l'ICP de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification.

9.11.3 Motifs selon lesquels un OID doit être changé

Si l'AC SSL CERTINOMIS estime qu'une modification de la PC modifie le niveau de confiance assuré par les exigences de la PC ou par le contenu de la DPC, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).

9.12 Règlement des différends

L'AC SSL CERTINOMIS propose de régler les différends concernant l'identité à inscrire dans un certificat et dans le cas où les parties ne parviendraient pas à un accord amiable, le différend sera réglé par un tribunal français.

Les contrats entre les clients SSL et l'AC SSL CERTINOMIS contiennent une clause de résolution des différends.

9.13 Droit applicable

Les PC et DPC sont appliquées et interprétées selon les lois et règlements français ainsi que toutes les directives européennes concernées qui pourraient s'appliquer, afin d'assurer des procédures et une interprétation uniforme pour tous les clients SSL quelle que soit leur localisation.

9.14 Conformité au droit applicable

La présente PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux, d'état, locaux et étrangers concernant les, mais non limités aux, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

9.15 Divers

9.15.1 Totalité de l'entente

Le cas échéant, la DPC précisera les exigences spécifiques.

9.15.2 Affectation

Sauf si spécifié dans d'autres contrats, seule l'AC SSL CERTINOMIS a le droit d'affecter et de déléguer la présente PC à une partie de son choix.

9.15.3 Divisibilité

Le caractère inapplicable d'une disposition de la DPC, suite à une décision de justice, n'affecte en rien la validité des autres dispositions de cette DPC.

9.15.4 Exonération des droits

Les exigences définies dans la PC/DPC doivent être appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, soit possible.

9.15.5 Force majeure

L'AC SSL CERTINOMIS ne saurait être tenue pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs aux clients SSL ou aux tiers utilisateurs.

9.16 Autres dispositions

Le cas échéant, la DPC en fournira les détails.