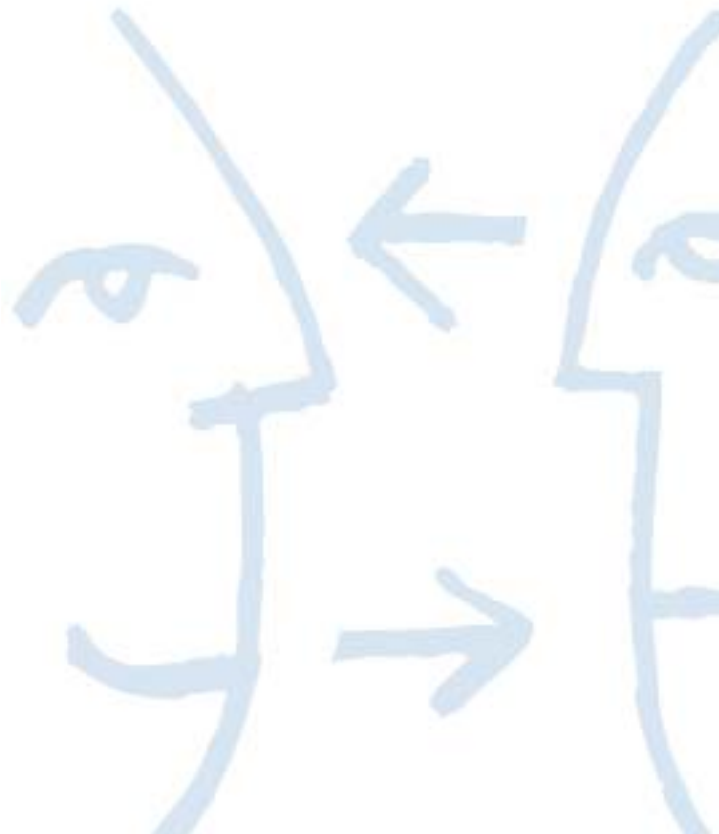


POLITIQUE DE CERTIFICATION DE L'AC

KEYNECTIS SSL RGS * (authentification serveur)

Date : 12/08/2011





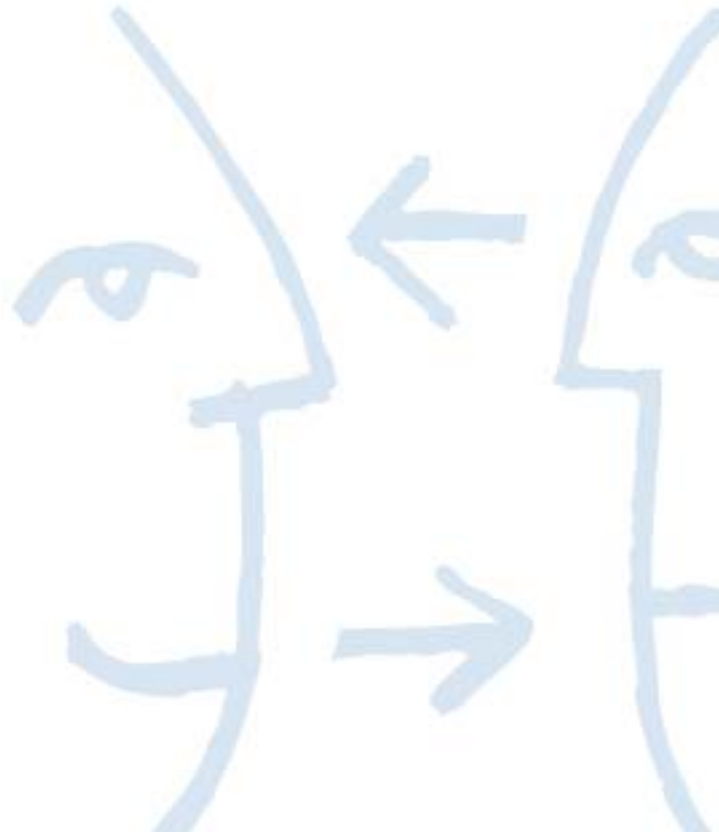
POLITIQUE DE CERTIFICATION : AC KEYNECTIS SSL RGS * (AUTHENTIFICATION SERVEUR)

Objet: Ce document consiste en la politique de certification de l'AC KEYNECTIS SSL RGS *

Numéro de version:	1.0	Nombre de pages:	53
Etat du document:	<input type="checkbox"/> Projet	<input checked="" type="checkbox"/> Version finale	
Rédacteur :	KEYNECTIS	KEYNECTIS	

Diffusion:	<input checked="" type="checkbox"/> Externe	<input checked="" type="checkbox"/> Interne KEYNECTIS	
	Public		KEYNECTIS

Historique:				
Date	Version	Rédacteur	Commentaires	Validé par
02/09/2011	1.0	EM	Passage en version 1.0	JYF



SOMMAIRE

AVERTISSEMENT	8
1 INTRODUCTION	9
1.1 Généralités	9
1.2 Nom du Document et Identification	9
1.3 Les composants de l'Infrastructure de Gestion de Clés	9
1.3.1 Autorité Administrative de KEYNECTIS (AAK)	10
1.3.2 Autorité de Certification (AC)	10
1.3.3 Autorité d'Enregistrement (AE)	10
1.3.4 Service de Publication (SP)	10
1.3.5 Opérateur de Service de Certification (OSC)	10
1.3.6 Propriétaire du Nom de Domaine	11
1.3.7 Contact Technique (CT)	11
1.3.8 Administrateur SSL	11
1.3.9 Autres participants	11
1.3.9.1 Utilisateur de certificat (UC)	11
1.4 Utilisation des certificats	11
1.4.1 Utilisation appropriée des certificats	11
1.4.1.1 Certificat de l'AC	11
1.4.1.2 Certificat SSL	12
1.4.2 Utilisation interdite des certificats	12
1.5 Application de la politique	12
1.5.1 Organisme responsable de la présente politique	12
1.5.2 Personne responsable	12
1.5.3 Personne déterminant la conformité de l'implémentation de la présente PC/DPC	12
1.5.4 Procédure d'approbation du présent document	12
1.6 Définitions et Acronymes	12
1.6.1 Définitions	12
1.6.2 Acronymes	15
2 ANNUAIRES ET SERVICES DE PUBLICATION	16
2.1 Service de publication	16
2.2 Informations publiées	16
2.3 Heure et fréquence de publication	16
2.4 Contrôle d'accès au service de publication	16
3 IDENTIFICATION ET AUTHENTIFICATION	17
3.1 Nommage	17
3.1.1 Types de noms	17
3.1.1.1 Certificat AC	17
3.1.1.2 Certificat SSL	17
3.1.2 Utilisation de noms explicites	18
3.1.3 Anonymat ou utilisation de pseudonyme	18
3.1.4 Règles d'interprétations des différentes formes de noms	18
3.1.5 Unicité des noms	18
3.1.6 Reconnaissance, vérification, et rôle des noms de marques déposées	18
3.2 Vérification initiale d'identité	18
3.2.1 Preuve de possession de la clé privée	18
3.2.2 Vérification de l'Identité d'une Entreprise ou d'une Administration cliente	19
3.2.3 Vérification de l'identité des personnes	19
3.2.4 Informations non vérifiées	19
3.2.5 Validation de l'autorité d'un demandeur	19
3.2.6 Critères de reconnaissance et certification croisée d'AC	19
3.3 Vérifications aux fins de renouvellement de clés	19
3.3.1 Vérifications aux fins de renouvellement de clés en situation normale	19
3.3.2 Vérifications aux fins de renouvellement de clés après révocation du certificat	19

3.4	Vérifications aux fins de révocation	20
4	EXIGENCES OPERATIONNELLES	21
4.1	Types de certificat	21
4.1.1	Origine de la demande de certificat	21
4.1.2	Procédure d'enregistrement et responsabilités	21
4.2	Traitement d'une demande de certificat	22
4.2.1	Identification et authentification	22
4.2.2	Approbation ou rejet d'une demande de certificat	22
4.2.3	Durée de traitement d'une demande de certificat	22
4.3	Emission d'un certificat	22
4.3.1	Actions effectuées par l'AC pendant l'émission d'un certificat	22
4.3.2	Notification de l'émission d'un certificat	22
4.4	Acceptation d'un certificat	22
4.4.1	Procédure d'acceptation d'un certificat	22
4.4.2	Publication d'un certificat par l'AC	22
4.4.3	Notification de l'émission d'un certificat par l'AC à d'autres entités	22
4.5	Utilisation des bi-clés et des certificats	22
4.5.1	Utilisation des bi-clés et des certificats	22
4.5.2	Utilisation des clés publiques et des certificats par les tierces parties	22
4.6	Demande d'un nouveau certificat	23
4.7	Changement de clés (ou certification d'une nouvelle clé publique)	23
4.8	Modification d'un certificat	23
4.9	Révocation d'un certificat	23
4.9.1	Motif de révocation d'un certificat	23
4.9.1.1	Certificat Composante IGC	23
4.9.1.2	Certificat SSL	23
4.9.2	Origine d'une demande de révocation	23
4.9.2.1	Certificat composante IGC	23
4.9.2.2	Certificat SSL	24
4.9.3	Procédure de demande de révocation	24
4.9.3.1	Certificat composante IGC	24
4.9.3.2	Certificat SSL	25
4.9.4	Délai accordé pour formuler la demande de révocation	25
4.9.5	Délai de traitement d'une révocation	25
4.9.5.1	Certificat Composantes IGC	25
4.9.5.2	Certificat SSL	25
4.9.6	Exigences de vérification de révocation pour les tierces parties	25
4.9.7	Fréquences de publication des LCR	26
4.9.8	Délai maximum de publication d'une CRL	26
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats	26
4.9.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	26
4.9.11	Autres moyens disponibles d'information sur les révocations	26
4.9.12	Exigences spécifiques en cas de compromission de la clé privée	26
4.9.13	Causes possibles d'une suspension	26
4.9.14	Origine d'une demande de suspension	26
4.9.15	Procédure de traitement d'une demande de suspension	26
4.9.16	Limites de la période de suspension d'un certificat	26
4.10	Service d'état des certificats	26
4.10.1	Caractéristiques opérationnelles	26
4.10.2	Disponibilité de la fonction	26
4.11	Fin de la relation avec l'AC	27
4.12	Séquestre et recouvrement de clés	27
5	MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN ŒUVRE	28
5.1	Sécurité physique	28
5.1.1	Situation géographique	28
5.1.2	Accès physique	28
5.1.3	Energie et air conditionné	28
5.1.4	Exposition aux liquides	28

5.1.5	Prévention et protection incendie.....	28
5.1.6	Mise hors service des supports	28
5.1.7	Sauvegardes hors site	28
5.2	Mesures de sécurité procédurales	28
5.2.1	Rôles de confiance	28
5.2.2	Nombre de personnes nécessaires à l'exécution de tâches sensibles	29
5.2.3	Identification et authentification des rôles.....	29
5.2.4	Rôles exigeant une séparation des attributions.....	29
5.3	Mesures de sécurité vis-à-vis du personnel.....	29
5.3.1	Qualifications, compétence et habilitations requises	29
5.3.2	Procédures de vérification des antécédents.....	29
5.3.3	Exigences en matière de formation initiale	29
5.3.4	Exigences et fréquence en matière de formation continue	29
5.3.5	Gestion des métiers	29
5.3.6	Sanctions en cas d'actions non autorisées.....	29
5.3.7	Exigences vis-à-vis du personnel des prestataires externes.....	30
5.3.8	Documentation fournie au personnel.....	30
5.4	Procédures de constitution des données d'audit.....	30
5.4.1	Type d'événements à enregistrer	30
5.4.2	Processus de journalisation	31
5.4.3	Protection des journaux d'événements.....	31
5.4.4	Procédures de sauvegarde des journaux d'événements	31
5.4.5	Système de collecte des journaux d'événements.....	31
5.4.6	Evaluation des vulnérabilités	31
5.5	Archivage des données	31
5.5.1	Type de données archivées.....	31
5.5.2	Période de conservation des archives.....	31
5.5.3	Protection des archives.....	32
5.5.4	Exigences d'horodatage des données.....	32
5.5.5	Système de collecte des archives.....	32
5.5.6	Procédures de récupération et de vérification des archives	32
5.6	Renouvellement de bi-clé	32
5.6.1	Certificat d'AC	32
5.6.2	Certificat SSL	32
5.7	Compromission et plan de reprise	33
5.7.1	Procédures en cas d'incident et de compromission	33
5.7.2	Corruption des ressources informatiques, des logiciels, et/ou des données	33
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.....	33
5.8.1	Transfert d'activité ou cessation d'activité affectant une composante de l'IGC	34
5.8.2	Cessation d'activité affectant l'AC.....	34
6	MESURES TECHNIQUES DE SECURITE	36
6.1	Génération et installation des bi-clés.....	36
6.1.1	Génération des bi-clés	36
6.1.1.1	Bi-clés d'AC	36
6.1.1.2	Bi-clés SSL	36
6.1.2	Fourniture de la clé privée	36
6.1.3	Fourniture de la clé publique à l'AC.....	36
6.1.4	Fourniture de la clé publique d'AC aux tierces parties	36
6.1.5	Taille de clés	36
6.1.6	Production des paramètres des clés publiques et contrôle de qualité	37
6.1.7	Utilisation de la clé (selon le champ "key usage" du certificat X 509 V3).....	37
6.2	Protection des clés privées et normes relatives au module cryptographique	37
6.2.1	Normes applicables aux ressources cryptographiques et contrôles	37
6.2.2	Contrôle de la clé privée par de multiples personnes.....	37
6.2.3	Séquestre de clé privée	37
6.2.4	Sauvegarde de clé privée	37
6.2.4.1	AC.....	37

6.2.4.2	Certificat SSL.....	37
6.2.5	Archivage de clé privée.....	38
6.2.6	Importation / exportation d'une clé privée.....	38
6.2.7	Stockage d'une clé privée dans un module cryptographique.....	38
6.2.8	Méthode d'activation d'une clé privée.....	38
6.2.8.1	AC.....	38
6.2.8.2	Certificat SSL.....	38
6.2.9	Méthode de désactivation d'une clé privée.....	38
6.2.9.1	AC.....	38
6.2.9.2	Certificat SSL.....	38
6.2.10	Méthode de destruction d'une clé privée.....	38
6.2.10.1	AC.....	38
6.2.10.2	Certificat SSL.....	38
6.2.11	Certification des ressources cryptographiques.....	38
6.3	Autres aspects de la gestion des bi-clés.....	39
6.3.1	Archivage des clés publiques.....	39
6.3.2	Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés.....	39
6.3.2.1	AC.....	39
6.3.2.2	Certificat SSL.....	39
6.4	Données d'activation.....	39
6.4.1	Génération et installation des données d'activation.....	39
6.4.1.1	AC.....	39
6.4.1.2	Certificat SSL.....	39
6.4.2	Protection des données d'activation.....	39
6.4.2.1	AC.....	39
6.4.2.2	Certificat SSL.....	39
6.4.3	Autres aspects touchant aux données d'activation.....	39
6.5	Mécanismes de sécurité des systèmes informatiques.....	39
6.5.1	Exigences techniques de sécurité des ressources informatiques.....	39
6.5.2	Indice de sécurité informatique.....	40
6.6	Contrôles techniques du système pendant son cycle de vie.....	40
6.6.1	Contrôle des développements des systèmes.....	40
6.6.2	Contrôles de gestion de la sécurité.....	40
6.6.3	Contrôle de sécurité du système pendant son cycle de vie.....	40
6.7	Mécanismes de sécurité du réseau.....	40
6.8	Horodatage/Système de datation.....	41
7	CERTIFICATS, CRL, ET PROFILS OCSP.....	42
7.1	Profil de Certificats.....	42
7.1.1	Extensions de Certificats.....	42
7.1.1.1	Certificat AC.....	42
7.1.1.2	Champs de base du certificat.....	42
7.1.1.3	Extension du certificat.....	42
7.1.1.4	Certificat SSL.....	42
7.1.1.5	Extension du certificat.....	42
7.1.2	Identifiant d'algorithmes.....	43
7.1.3	Formes de noms.....	43
7.1.4	Identifiant d'objet (OID) de la Politique de Certification.....	43
7.1.5	Extensions propres à l'usage de la Politique.....	43
7.1.6	Syntaxe et Sémantique des qualificateurs de politique.....	43
7.1.7	Interprétation sémantique de l'extension critique "Certificate Policies".....	43
7.2	Profil de LCR.....	43
7.2.1	LCR et champs d'extensions des LCR.....	43
7.3	Profil OCSP.....	43
8	CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS.....	44
8.1	Fréquence et motifs des audits.....	44
8.2	Identité / Qualification des auditeurs.....	44
8.3	Lien entre l'auditeur et l'entité contrôlée.....	44
8.4	Points couverts par l'évaluation.....	44

8.5	Mesures prises en cas de non-conformité	44
8.6	Communication des résultats	44
9	AUTRES DISPOSITIONS COMMERCIALES ET JURIDIQUES	45
9.1	Tarifs	45
9.1.1	Tarifs pour l'émission et le renouvellement de certificats	45
9.1.2	Tarifs pour l'accès aux certificats	45
9.1.3	Tarifs pour l'accès aux LCR et aux informations d'état des certificats	45
9.1.4	Tarifs pour d'autres services	45
9.1.5	Politique de remboursement	45
9.2	Responsabilité financière	45
9.2.1	Couverture par les assurances	45
9.2.2	Autres ressources	45
9.2.3	Couverture et garantie concernant les entités utilisatrices	45
9.3	Confidentialité des informations et des données professionnelles	45
9.3.1	Périmètre des informations confidentielles	45
9.3.2	Informations hors du périmètre des informations confidentielles	45
9.3.3	Obligations en terme de protection des informations confidentielles	46
9.4	Protection des données personnelles	46
9.4.1	Politique de protection des données personnelles	46
9.4.2	Informations considérées comme personnelles	46
9.4.3	Informations à caractère non personnel	46
9.4.4	Obligations en terme de protection des données personnelles	46
9.4.5	Consentement exprès et préalable à l'utilisation de données à caractère personnel	46
9.4.6	Divulgateion due à un processus judiciaire ou administratif	46
9.4.7	Autres motifs de divulgation de données à caractère personnel	47
9.5	Droits relatifs à la propriété intellectuelle	47
9.6	Obligations et garanties	47
9.6.1	Obligations communes	47
9.6.2	Obligations et garanties de l'AAK	47
9.6.3	Obligations et garanties de l'AC	47
9.6.4	Obligations de l'AE	48
9.6.5	Obligations et garanties du CT	48
9.6.6	Obligations et garanties de l'Administrateur	48
9.6.7	Obligations et garanties du SP	49
9.6.8	Obligations et garanties des autres participants	49
9.6.8.1	Obligations et garanties de l'UC	49
9.7	Limite de garantie	49
9.8	Limites de responsabilité	49
9.9	Indemnités	50
9.10	Durée et fin anticipée de validité de la PC	50
9.10.1	Durée	50
9.10.2	Résiliation	50
9.10.3	Effets de la résiliation et survie	50
9.11	Amendements	50
9.11.1	Procédure pour apporter un amendement	50
9.11.2	Mécanisme et délais des notifications	50
9.11.3	Motifs selon lesquels un OID doit être changé	51
9.12	Règlement des différends	51
9.13	Droit applicable	51
9.14	Conformité au droit applicable	51
9.15	Divers	51
9.15.1	Totalité de l'entente	51
9.15.2	Affectation	52
9.15.3	Divisibilité	52
9.15.4	Exonération des droits	52
9.15.5	Force majeure	52
9.16	Autres dispositions	52
10	REFERENCES	53

AVERTISSEMENT

La présente politique de certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de KEYNECTIS.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par KEYNECTIS ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'Article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (Article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les Articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

1 INTRODUCTION

1.1 Généralités

La dématérialisation, ou conversion au format électronique des transactions quotidiennes traditionnelles (contrats, courrier, factures, formulaires administratifs, etc.), permet avant tout d'accélérer les processus documentaires. En raison de l'aspect innovant et technique de ces processus, les entreprises doivent faire appel à des prestataires de services spécialisés à même d'assurer le rôle de tierce partie de confiance et de fait, de fournir une preuve de la transaction.

Les certificats électroniques se trouvent au cœur des technologies. Pour fournir leurs services, les tierces parties de confiance (Autorité de Certification, Autorité d'Horodatage, Autorité de Validation), les entreprises et organisations utilisant des certificats électroniques, s'appuient sur le centre de production et les autorités de KEYNECTIS (AC, AH et AV) pour les services de certification et d'horodatage, ainsi que pour les services de validation.

KEYNECTIS dispose d'une Autorité de Certification Racine (ACR) qui certifie l'AC KEYNECTIS SSL RGS *, laquelle délivre des certificats SSL conformément à la présente Politique de Certification (PC).

La présente politique de certification (PC) a pour objet de décrire la gestion du cycle de vie des certificats SSL délivrés par l'AC et des bi-clés associées, ainsi que la gestion du certificat de l'AC et de sa bi-clé.

L'AC « KEYNECTIS SSL RGS * » est une AC qualifiée selon les exigences prévues par le Référentiel Général de Sécurité (RGS) pour le service de certificat authentification au niveau *. L'AC permet d'émettre des certificats SSL RGS * avec un nom de domaine (FQDN contenu dans le CN). A ce nom de domaine peuvent être associé des noms de domaine alternatif qui sont contenus dans l'extension SAN du certificat SSL.

La présente Politique de Certification est élaborée conformément :

- Au RFC 3647 : « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;
- Au document : « Référentiel Général de Sécurité, Politique de Certification Type Authentification serveur, version 2.3, 11 février 2010, niveau *, OID : 1.2.250.1.137.2.2.1.2.2.5 » (certificat serveur seulement).

1.2 Nom du Document et Identification

La présente PC appelée : « KEYNECTIS SSL RGS * » est la propriété de KEYNECTIS. Cette PC est enregistrée par un numéro d'identifiant d'objet (OID) qui est : 1.3.6.1.4.1.22234.2.5.3.6.

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins le seul identifiant de la version applicable de la PC est l'OID.

1.3 Les composantes de l'Infrastructure de Gestion de Clés

Pour délivrer les certificats, l'AC s'appuie sur les services suivants :

- Service d'enregistrement : ce service collecte et vérifie les informations d'identification du CT ou de l'Administrateur SSL qui demande un certificat, avant de transmettre la demande de certificat au service de demande de certificat ;
- Service de demande de certificat : ce service crée une demande de certificat, à l'aide des informations fournies par le service d'enregistrement dans le but de créer et de transmettre une demande de certificat au service de génération de certificat ;
- Service de génération de certificat : ce service génère les certificats électroniques pour les CT ou les l'Administrateur SSL à partir des informations transmises par le service de demande de certificat ;
- Service de remise de certificat : ce service remet au CT ou à l'Administrateur SSL son certificat ;
- Service de révocation de certificats : ce service traite les demandes de révocation des certificats SSL et détermine les actions à mener, dont la génération des Liste de Certificats Révoqués (LCR) ;

- Service de Publication : ce service met à disposition des utilisateurs de certificat (UC) les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales d'utilisation, politique de certification publiée par l'AC, certificat d'AC, certificats SSL, ...), ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations (LCR, avis d'information, ...)
- Service de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audit consultables. Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus dans la délivrance des certificats par l'AC aux CT et aux Administrateurs SSL. La Déclaration des Pratiques de Certification (notée DPC) donnera les détails des pratiques de l'IGC dans cette même perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

1.3.1 Autorité Administrative de KEYNECTIS (AAK)

L'AAK est KEYNECTIS. L'AAK est responsable de l'AC dont elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité de l'AC est composé de la présente PC, de la DPC associée, des conditions générales d'utilisation et des procédures mises en œuvre par les composantes de l'IGC. L'AAK valide le référentiel de sécurité composé de la PC et de la DPC. Elle autorise et valide la création et l'utilisation des composantes de l'AC. Elle suit les audits et/ou contrôle de conformités effectués sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application. Elle valide que le Client possède des procédures spécifiques pour les services de l'AE qu'il met en œuvre.

1.3.2 Autorité de Certification (AC)

L'AC génère des certificats et révoque des certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. L'AC met en œuvre les services de génération de certificats, de révocation de certificats et de journalisation et d'audit.

KEYNECTIS s'appuie sur ses propres capacités d'Opérateur de Service de Certification (OSC) afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des certificats.

L'AC agit conformément à la présente PC et à la DPC associée qui sont établies par l'AAK.

KEYNECTIS est AC au sens de la responsabilité de gestion du cycle de vie des certificats.

1.3.3 Autorité d'Enregistrement (AE)

L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, de remise de certificats, de révocation de certificats et journalisation et d'audit. L'AE est chargée d'authentifier et d'identifier les CT et les Administrateurs SSL. L'AE est mise en œuvre par KEYNECTIS.

Toutefois, KEYNECTIS n'exclut pas de déléguer l'enregistrement de demandes de certificats à une entité tierce. Cette entité tierce est alors appelée Revendeur. En ce cas, un contrat entre le Revendeur et KEYNECTIS permet de définir précisément les obligations et les services mis en œuvre par cette AE déléguée. La DPC précise les délégations possibles et les procédures associées lorsqu'un revendeur est utilisé et agit en tant qu'AE déléguée.

Dans tous les cas, l'AE agit conformément à la PC et à la DPC associée qui sont établies par l'AAK.

1.3.4 Service de Publication (SP)

Le SP est utilisé pour la mise en œuvre du service de publication (Se reporter au § 2).

Le SP agit conformément à la PC et à la DPC associée.

1.3.5 Opérateur de Service de Certification (OSC)

L'OSC assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC. L'OSC est techniquement dépositaire de la clé privée de

l'AC utilisée pour la signature des certificats. Sa responsabilité se limite au respect des procédures que l'AC définit afin de répondre aux exigences de la présente PC.

Dans la présente PC, son rôle et ses obligations ne sont pas distingués de ceux de l'AC. Cette distinction sera précisée dans la DPC.

1.3.6 Propriétaire du Nom de Domaine

Le propriétaire du nom de domaine est l'entité légale qui détient le nom de domaine concerné par la délivrance d'un certificat. Le nom de domaine est géré par un administrateur de nom de domaine. Le propriétaire de nom de domaine fait appel à un contact technique ou un administrateur SSL pour gérer les certificats SSL associé aux noms de domaines dont il est propriétaire. C'est le représentant légal de l'entité légale à laquelle appartient le nom de domaine qui autorise la demande de certificat et le CT et/ou l'Administrateur SSL à gérer la bi-clé et les demande de certificat et de révocation de certificat.

1.3.7 Contact Technique (CT)

Un Contact Technique est une personne nommée et autorisé par le propriétaire du nom de domaine et qui est autorisée à :

- Agir en tant que demandeur SSL pour la génération de la CSR ;
- Générer les bi-clés dont les clés publiques seront associées à un certificat SSL ;
- Remplir les formulaires de demande de certificat SSL ;
- Retirer les certificats SSL ;
- Procéder le cas échéant aux demandes de révocation des certificats SSL.

Dans la terminologie du RGS, le CT est un RCAS (Responsable du certificat d'authentification serveur).

1.3.8 Administrateur SSL

Un administrateur SSL est un contact technique autorisé par le propriétaire du nom de domaine à agir comme contact technique pour enregistrer plusieurs noms de domaine à partir d'une racine de FQDN commune. Par exemple, l'administrateur SSL peut retirer plusieurs certificats SSL en faisant varier seulement le paramètre « variable » dans le FQDN suivant : www.variable.nomdedomaine.fr. Pour ce faire l'Administrateur SSL dispose d'un accès privilégié sur l'interface d'AE afin de retirer lui-même les certificats SSL. Au préalable, l'administrateur SSL est authentifié et enregistré par l'AE pour le nom de domaine commun (par exemple www.nomdedomaine.fr). L'AE fige cette partie du nom de domaine, dans les interfaces de l'AE utilisable par l'administrateur SSL, afin que l'administrateur SSL ne puisse pas créer n'importe quelle forme de nom de domaine.

L'administrateur SSL est ensuite chargé de gérer les demandes de pour créer les noms de domaines autorisé sous la racine commune de FQDN. L'AE contrôle régulièrement l'ensemble des sites crée par l'Administrateur SSL afin de détecter tout abus de la part de l'Administrateur SSL.

1.3.9 Autres participants

1.3.9.1 Utilisateur de certificat (UC)

L'UC est une personne ou une machine qui fait confiance aux certificats SSL, fait confiance au chemin de certification de l'AC, afin d'identifier et d'authentifier un nom de domaine et l'entité dont le nom de domaine est inclus dans le certificat SSL

1.4 Utilisation des certificats

1.4.1 Utilisation appropriée des certificats

1.4.1.1 Certificat de l'AC

Le certificat de l'AC sert à authentifier les certificats SSL. La clé privée associé au certificat d'AC sert pour :

- La signature de certificat SSL ;
- La signature de LCR.

1.4.1.2 Certificat SSL

Un certificat SSL délivré par l'AC est utilisé par les UC pour vérifier l'identité d'un nom de domaine sur un serveur donné.

Les certificats délivrés aux CT et aux administrateurs SSL sont exclusivement utilisés par les CT identifiés à l'article 1.3.7 et les Administrateurs SSL identifiés à l'article 1.3.8 ci-dessus pour mettre en œuvre des sessions SSL pour les FQDN pour lesquels ils sont autorisés par les propriétaires de nom de domaine.

Il est rappelé que l'utilisation de la clé privée, par les CT et les Administrateurs SSL, et du certificat associé doit rester strictement limitée au service de signature. Dans le cas contraire, leur responsabilité pourrait être engagée.

1.4.2 Utilisation interdite des certificats

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au § 1.4.1 ci-dessus ne sont pas autorisées. En pratique, cela signifie que l'AC ne peut être en aucun cas tenue pour responsable d'une utilisation des certificats qu'elle émet autre que celles prévues dans la présente PC.

Les certificats ne peuvent être utilisés que conformément aux lois applicables en vigueur, en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation et les lois, décrets, arrêtés et directives propres à la signature électronique.

Cette PC décrit la gestion du cycle de vie des certificats SSL et bi-clés associées indépendamment de leur support de génération et d'utilisation, elle n'a pas vocation de remplacer une politique de sécurité des serveurs SSL qui elle décrit la gestion des sessions SSL et la protection des bi-clés sur les serveurs

Il convient au CT et aux Administrateurs SSL d'élaborer leur propre politique de sécurité afin de définir notamment les engagements et les limites de responsabilités qu'un accès à un nom de domaine lors d'une session SSL confère au données, diffusées ou reçues, et aux fonctions ainsi accessible, ainsi que les moyens et conditions de protection des bi-clés.

1.5 Application de la politique

1.5.1 Organisme responsable de la présente politique

La présente PC est sous la responsabilité de l'AAK.

1.5.2 Personne responsable

Coordonnées de la personne ou de la direction responsable de l'élaboration de la PC :

- KEYNECTIS ;
- Contact : Responsable Qualité et Sécurité ;
- 11-13 rue René Jacques - 92131 Issy-les-Moulineaux Cedex ;
- Tél : +33 (0)1 55 64 22 80 ;
- Fax : +33 (0)1 55 64 22 01 ;
- info@keynectis.com.

1.5.3 Personne déterminant la conformité de l'implémentation de la présente PC/DPC

L'AAK procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour l'AC d'émettre des certificats.

1.5.4 Procédure d'approbation du présent document

L'AAK possède ses propres méthodes pour approuver le présent document. L'AAK approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet.

1.6 Définitions et Acronymes

1.6.1 Définitions

AAK : Se reporter au § 1.3.1.

Autorité de Certification : Se reporter au § 1.3.2.

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.

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) : Se reporter au § 1.3.2.

Autorité d'Enregistrement (AE) : Se reporter au § 1.3.3.

Client : organisation ayant besoin d'un certificat SSL pour sécuriser son site Web. Un client peut et est autorisé à utiliser la clé privée qui correspond à la clé publique contenue dans le certificat.

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettre en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

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 : 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].

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 (certificat auto signé).

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

Chemin de certification : (ou chaîne de confiance, ou chaîne de certification) chaîne constituée de multiples certificats nécessaires pour valider un certificat.

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

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

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].

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 PIN, une phrase secrète, ...).

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 de Gestion de Clés (IGC) : 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 ou critères communs), utilisé pour conserver et mettre en oeuvre la clé privée AC.

Nom de domaine : nom enregistré par l'organisation auprès d'organismes tels que l'AFNIC ou l'INTERNIC. Il est composé du nom précédant l'extension (telle que .fr ou .com) et complété par l'extension elle-même. Le nom de domaine doit toujours être enregistré au nom de l'organisation qui en fait la demande. Pendant le processus d'enregistrement, le nom de domaine est « associé » à un contact technique qui est juridiquement autorisé à utiliser ce nom de domaine.

OSC : Se reporter au § 1.3.5

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'IGC 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].

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].

Porteur de secret : personnes qui détiennent une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

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

Revendeur : Se reporter au § 1.3.4.

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

SP : Se reporter au § 1.3.4.

Utilisateur de Certificat : Se reporter au §.1.3.9.1

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaîne de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification.

1.6.2 Acronymes

- **AAK** : Autorité Administrative de KEYNECTIS;
- **AC** : Autorité de Certification ;
- **AE** : Autorité d'Enregistrement ;
- **CC** : Critères Communs ;
- **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 ;
- **HTTP**: Hypertext Transport Protocol ;
- **IGC** : Infrastructure de Gestion de Clés ;
- **IP**: Internet Protocol ;
- **ISO**: International Organization for Standardization ;
- **LCR** : liste de certificats révoqués ;
- **LDAP**: Lightweight Directory Access Protocol ;
- **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 ;
- **URL**: Uniform Resource Locator.

2 ANNUAIRES ET SERVICES DE PUBLICATION

2.1 Service de publication

Le SP est en charge de la publication des données identifiées au § 2.2 ci-dessous.

2.2 Informations publiées

L'AC, via le SP, rend disponibles les informations suivantes :

- La PC de l'AC : <https://www.keynectis.com/PC/> ;
- Le certificat de l'AC : <https://www.keynectis.com> ;
- Les certificats de la chaîne de confiance à laquelle l'AC est rattaché à savoir : le certificat racine de l'ACR Certplus « Class 2 Primary CA » : <https://www.keynectis.com> ;
- Le formulaire de demande de certificat (sur demande) : <https://www.keynectis.com> ;
- Le formulaire et/ou les modalités de révocation d'un certificat (sur demande) : <https://www.keynectis.com> ;
- Les conditions générales d'utilisation : <https://www.keynectis.com> ;
- La LCR : URL=http://trustcenter-crl.certificat2.com/keynectis/RGS/SSL1e.crl ;
- La LCR (LDAP) :
URL=ldap://ldap.keynectis.com/cn=KEYNECTIS%20SSL%20RGS,o=KEYNECTIS?certificateRevocationList;binary?base?objectclass=crlDistributionPoint.

La DPC n'est pas publiée mais consultable auprès de l'AAK sur demande justifiée et autorisée par l'AAK.

2.3 Heure et fréquence de publication

La PC de l'AC et le certificat de l'AC sont disponibles en permanence et mises à jour selon les besoins suivant un taux de disponibilité définie dans la DPC.

Une nouvelle LCR est publiée toutes les 24 heures suivant un taux de disponibilité définie dans la DPC.

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

L'ensemble des informations publiques et publiées (Se reporter au § 2.2) est libre d'accès en lecture et téléchargement sur Internet.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X.509, l'AC (Issuer) et propriétaire de nom de domaine (subject) sont identifiés par un Distinguished Name (DN).

Les attributs du DN sont encodés en « printableString » ou en « UTF8String » à l'exception des attributs emailAddress qui sont en « IA5String ».

3.1.1.1 Certificat AC

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	CN = Class 2 Primary CA O = Certplus C = FR
Subject	CN = KEYNECTIS SSL RGS OU = 0002 478217318 O = KEYNECTIS C = FR

3.1.1.2 Certificat SSL

L'identité dans le certificat est la suivante :

Champ de base	Valeur
Issuer	CN = KEYNECTIS SSL RGS OU = 0002 478217318 O = KEYNECTIS C = FR
Subject	C = Code ISO du Pays de l'autorité compétente auprès de laquelle l'organisation cliente de KEYNECTIS est officiellement enregistré (tribunal de commerce, ministère, ...). Ce code est inscrit en majuscules ; CN = FQDN ; O = Nom officiel complet de l'organisation cliente tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, ...) ; Pour les Clients de droit français : <ul style="list-style-type: none"> - ICD = 0002 ; - l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent : <ul style="list-style-type: none"> - soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres - soit l'attribut organizationalUnitName est présent mais avec

	<p>un numéro ICD différent de 0002</p> <ul style="list-style-type: none">- soit l'attribut <code>organizationalUnitName</code> est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. <p>D'autres instances de l'attribut <code>organizationalUnitName</code> peuvent être présentes mais ne doivent pas commencer par 4 chiffres.</p> <p>S = département de l'organisation Client (optionnel) L = Ville de l'organisation Client (optionnel)</p>
--	---

3.1.2 **Utilisation de noms explicites**

Les noms choisis pour désigner les serveurs dans les certificats doivent être explicites.

L'identification de l'entité à laquelle le serveur est rattaché est obligatoire.

Le DN du serveur contient son FQDN (« Fully Qualified Domain Name ») ou nom de domaine totalement qualifié. Exemple : www.nomdedomaine.fr auquel le serveur est rattaché.

Nota – Le certificat d'authentification serveur est associé au FQDN et pas au serveur physique sur lequel la bi-clé est déployée. Autrement dit, une bi-clé d'authentification serveur peut être déployée sur plusieurs machines physiques rattachées à ce FQDN (cas notamment d'architecture de répartition de charge).

3.1.3 **Anonymat ou utilisation de pseudonyme**

S'agissant de certificats de machines, les notions d'anonymisation ou de pseudonymisation sont sans objet.

3.1.4 **Règles d'interprétations des différentes formes de noms**

Les UC peuvent se servir de l'identité incluse dans les certificats (Se reporter au 3.1.1) afin d'authentifier des noms de domaine.

3.1.5 **Unicité des noms**

Les identités portées par l'AC dans les certificats (Se reporter au § 3.1.1) sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, une identité attribuée à un Client ne peut être attribuée à un autre Client.

A noter que l'unicité d'un certificat est basé sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC, mais que ce numéro est propre au certificat et ne permet donc pas d'assurer une continuité de l'identification dans les certificats SSL successifs d'un nom de domaine donné.

En cas de différent au sujet de l'utilisation d'un nom pour un certificat, l'AAK a la responsabilité de résoudre le différent en question.

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

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n° 92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par la communauté d'utilisateur et les Clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

3.2 **Vérification initiale d'identité**

3.2.1 **Preuve de possession de la clé privée**

La preuve de la possession de la clé privée par le CT ou l'Administrateur SSL est réalisée par les procédures de génération de la clé privée (se reporter au § 6.1.1.1 ci-dessous) correspondant à la clé publique à certifier et par le mode de transmission de la clé publique (se reporter au § 6.1.3 ci-dessous).

3.2.2 Vérification de l'Identité d'une Entreprise ou d'une Administration cliente

L'authentification des organisations (propriétaire de nom de domaine et CT et Administrateur SSL) repose sur la vérification des informations fournies par le CT ou l'Administrateur SSL dans le cadre de sa demande de certificat (Se reporter au § 4.1.2). Ces informations comprennent le nom et l'adresse de l'organisation ainsi que les documents ou les références de l'existence de celle-ci, ainsi que le nom de domaine qu'elle détient.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

Dans tous les cas, la vérification de l'appartenance d'un CT et d'un Administrateur SSL à l'organisation de « type » Administration et Entreprise dont il se réclame est effectuée.

En vue de la délivrance du certificat SSL, il est également nécessaire de vérifier que le nom de domaine présent dans la demande appartient à cette organisation (propriétaire de nom de domaine), et qu'elle est donc autorisée à l'utiliser. Les vérifications sont effectuées en consultant les bases de données officielles de noms de domaine de type AFNIC ou INTERNIC. L'AE vérifie que le CT et l'Administrateur SSL que le nom de domaine inclus dans le FQDN du serveur appartient bien à l'entité qu'il représente.

3.2.3 Vérification de l'identité des personnes

L'enregistrement d'un serveur auquel un certificat doit être délivré se fait via l'enregistrement du CT et de l'Administrateur SSL correspondant.

L'identification et l'authentification du CT, ou Administrateur SSL, et des signataires de la demande de certificat est effectuée par l'AE à partir des informations contenues dans le dossier de demande de certificat (Cf. § 4.1.2).

Un CT et un Administrateur SSL peut être amené à changer en cours de validité du certificat d'authentification serveur correspondant. Dans ce cas, tout nouveau CT et Administrateur SSL fait également l'objet d'une procédure d'enregistrement.

3.2.4 Informations non vérifiées

Les informations non vérifiées ne sont pas introduites dans les certificats.

3.2.5 Validation de l'autorité d'un demandeur

La validation de l'autorité d'un demandeur correspond à la validation de l'appartenance à une organisation (se reporter au § 3.2.2 ci-dessus) et son autorisation par un représentant légal de l'organisation.

3.2.6 Critères de reconnaissance et certification croisée d'AC

Un certificat SSL émis par l'AC à la garantie d'être authentifiable dans les navigateurs car l'AC émettrice est signée par une ACR dont le certificat est largement diffusé dans les principaux outils que sont les systèmes d'exploitation et les navigateurs internet.

3.3 Vérifications aux fins de renouvellement de clés

3.3.1 Vérifications aux fins de renouvellement de clés en situation normale

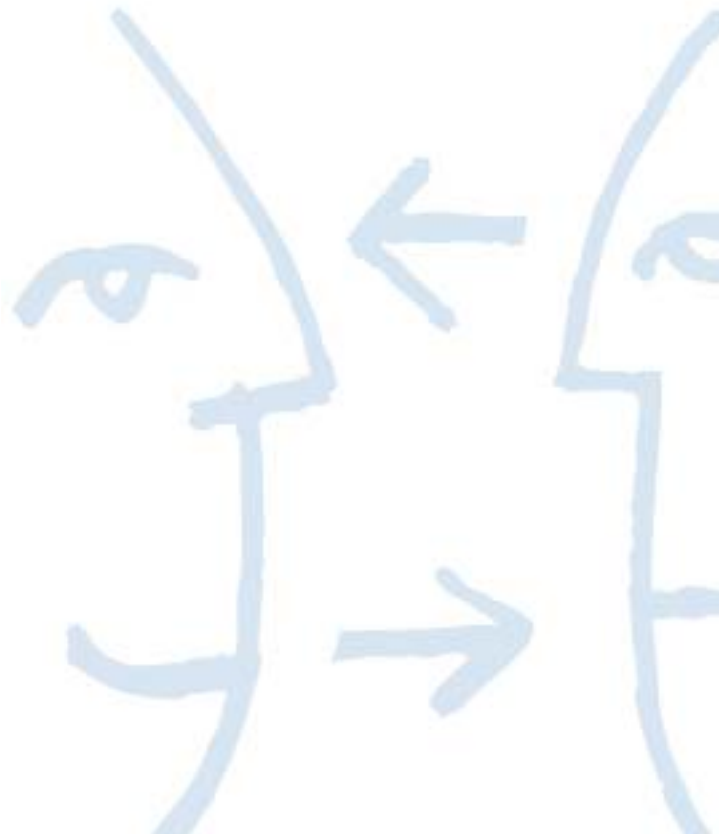
Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2 ci-dessus).

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

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2).

3.4 Vérifications aux fins de révocation

Les demandes de révocation sont authentifiées par l'AE à l'aide d'informations seulement connues du CT, ou de l'Administrateur SSL, et de l'AE. Lorsque le demandeur est une personne autre que le CT ou l'Administrateur SSL, l'authentification est réalisée suivant des procédures définies dans la DPC.



4 EXIGENCES OPERATIONNELLES

4.1 Types de certificat

4.1.1 Origine de la demande de certificat

Une demande de certificat est émise par un CT ou un Administrateur SSL auprès de l'AE (service d'enregistrement).

4.1.2 Procédure d'enregistrement et responsabilités

Les informations suivantes doivent figurer dans la demande de certificat SSL :

- CT et Administrateur SSL au sein d'une Entreprise :
 - o Un mandat, daté de moins de 3 mois, désignant le futur CT ou l'Administrateur SSL comme étant habilité à être CT ou l'Administrateur SSL pour le nom de domaine (FQDN). Ce mandat doit être signé par un représentant légal qui détient le nom de domaine de l'entité et co-signé, pour acceptation, par le CT ou l'Administrateur SSL ;
 - o La demande de certificat est signée par le CT, ou l'Administrateur SSL (en fonction de l'origine de la demande), et datée de moins de 3 mois. La demande et le mandat peuvent être réunis dans un seul et même document ;
 - o Un document officiel d'identité du CT, ou l'Administrateur SSL (en fonction de l'origine de la demande), avec signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original" (uniquement pour les dossiers papiers), en cours de validité, comportant une photographie d'identité, l'AE en conserve une copie ;
 - o Les Informations permettant à l'AE de contacter le CT, le propriétaire de nom de domaine et l'Administrateur SSL (numéro de téléphone, courriel, ...) ;
 - o Toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
 - o Tout document attestant de la qualité du signataire de la demande de certificat. La qualité du signataire est portée dans la demande de certificat et est ainsi garantie par l'entité ;
 - o Les conditions générales d'utilisation (CGU) signée par le CT ou l'Administrateur SSL ;
 - o La CSR pour la clé publique à certifier.

- CT et Administrateur SSL au sein d'une Administration :
 - o Un mandat, daté de moins de 3 mois, désignant le futur CT ou l'Administrateur SSL comme étant habilité à être CT ou l'Administrateur SSL pour le nom de domaine (FQDN). Ce mandat doit être signé par un représentant légal qui détient le nom de domaine de l'entité et co-signé, pour acceptation, par le CT ou l'Administrateur SSL ;
 - o Un document officiel d'identité du CT ou de l'Administrateur SSL avec signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original", en cours de validité, comportant une photographie d'identité, l'AE en conserve une copie ;
 - o La demande de certificat est signée par le CT, ou l'Administrateur SSL (en fonction de l'origine de la demande), et datée de moins de 3 mois. La demande et le mandat peuvent être réunis dans un seul et même document ;
 - o Les informations qui permettent de construire l'identité définies aux § 3.1.1.2 et § 3.1.2 ;
 - o Les Informations permettant à l'AE de contacter le CT, l'Administrateur SSL et le propriétaire de nom de domaine (numéro de téléphone, courriel, ...) ;
 - o Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
 - o Les conditions générales d'utilisation (CGU) signée par le CT ou l'Administrateur SSL ;
 - o La CSR pour la clé publique à certifier.

La demande de certificat contient le FQDN à certifier. Dans le cas du Club SSL, une seule demande de certificat vaut pour l'émission de plusieurs certificats à la seule initiative de l'Administrateur SSL.

4.2 Traitement d'une demande de certificat

4.2.1 Identification et authentification

L'AE authentifie le demandeur (se reporter aux § 3.2.2, 3.2.3 et le 3.2.5).

L'AE s'assure que le demandeur a pris connaissance des conditions générales d'utilisation.

L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.

4.2.2 Approbation ou rejet d'une demande de certificat

En cas d'approbation de la demande, l'AE (service de demande de certificat) transmet la demande à l'AC (service de génération de certificat).

En cas de rejet de la demande, l'AE en informe le demandeur en justifiant le rejet.

4.2.3 Durée de traitement d'une demande de certificat

La demande de certificat est traitée dès la réception de la demande par l'AE dans les meilleurs délais.

4.3 Emission d'un certificat

4.3.1 Actions effectuées par l'AC pendant l'émission d'un certificat

L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC génère le certificat SSL.

L'AC transmet le certificat au service de retrait de certificat de l'AE.

L'AE transmet le certificat au CT.

Lorsqu'il s'agit de Club SSL, c'est l'Administrateur SSL qui émet directement une demande technique auprès de l'AE. Cette transmission, ou l'Administration est authentifié lors d'une session SSL par l'AE, déclenche le processus de génération de certificat par de l'AC. L'Administrateur SSL récupère lui même son certificat.

Les communications, entre les différentes composantes de l'IGC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

4.3.2 Notification de l'émission d'un certificat

La remise du certificat au CT ou à l'Administrateur SSL (service de remise de certificat) s'effectue par l'AE par courrier électronique au CT ou directement auprès de l'AE par l'Administrateur SSL.

4.4 Acceptation d'un certificat

4.4.1 Procédure d'acceptation d'un certificat

Dès que le CT, ou l'Administrateur SSL, a récupéré son certificat, l'AC considère le certificat comme accepté. L'acceptation est tacite. En cas de contestation, le CT, ou l'Administrateur SSL, alerte l'AE et demande la révocation de son certificat.

4.4.2 Publication d'un certificat par l'AC

Le certificat de l'AC est publié par le SP.

Les certificats SSL ne sont pas publiés par le SP.

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

Le demandeur, le contact technique (CT) et l'Administrateur SSL sont informés de la délivrance d'un certificat SSL pour le ou les noms de domaine dont ils sont responsables.

Le service clients de l'AC est également informé de la délivrance d'un certificat SSL.

4.5 Utilisation des bi-clés et des certificats

4.5.1 Utilisation des bi-clés et des certificats

L'utilisation des bi-clés et des certificats est définie au § 1.4 ci-dessus. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (se reporter au § 6.1.7). La clé privée ne peut être utilisée que pour une opération de type sécurité d'accès type session SSL.

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

L'utilisation des certificats par les UC est décrites dans les paragraphes 1.4 et 3.1.4 ci-dessus.

4.6 Demande d'un nouveau certificat

Cette section concerne le processus de renouvellement du certificat, sans que les clés publiques ou toute autre information incluse dans les certificats soient modifiées. Seule la période de validité et le numéro de série changent.

Ce type d'opération n'est pas autorisé au titre de la présente PC.

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

Cette section concerne la génération d'un nouveau certificat avec changement de la clé publique associée.

Le changement de la clé publique d'un certificat implique la création d'un nouveau certificat. Dans ce cas la procédure à appliquer pour renouveler un certificat SSL est identique à celles décrites pour la délivrance du premier certificat (se reporter au § 4.1 ci-dessus).

4.8 Modification d'un certificat

Cette section concerne la génération d'un nouveau certificat avec conservation de la même clé. Cette opération est rendue possible uniquement si la clé publique réutilisée dans le certificat est toujours conforme aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé.

Ce type d'opération n'est pas autorisé au titre de la présente PC.

4.9 Révocation d'un certificat

4.9.1 Motif de révocation d'un certificat

4.9.1.1 Certificat Composante IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des
- Procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple,
- Suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.1.2 Certificat SSL

Un certificat est révoqué quand l'association la clé publique et l'identité qu'il certifie n'est plus considérée comme étant valide. Les motifs qui invalident cette association sont :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN ou du nom du serveur), ceci avant l'expiration normale du certificat ;
- Le demandeur, CT ou Administrateur SSL, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité de l'entité propriétaire du nom de domaine ou la fin d'activité du serveur qui met en œuvre site internet avec le FQDN certifié ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La révocation de l'AC ;
- La fin de vie de l'AC ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Quand l'une de ces occurrences se produit, le certificat en question doit être révoqué.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat composante IGC

L'AAK ou une autorité judiciaire via une décision de justice est à l'origine de la demande de révocation des certificats d'AC.

L'AC est à l'origine de la demande de révocation des certificats de composantes d'IGC.

4.9.2.2 Certificat SSL

Le CT ou l'Administrateur SSL peut faire une demande de révocation dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN ou du nom du serveur), ceci avant l'expiration normale du certificat ;
- Le demandeur, CT ou Administrateur SSL, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'organisation Client (se reporter au § 3.2.2), pour les Entreprise et les Administration, peut demander la révocation d'un certificat dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN ou du nom du serveur), ceci avant l'expiration normale du certificat ;
- Le demandeur, CT ou Administrateur SSL, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité de l'entité propriétaire du nom de domaine ou la fin d'activité du serveur qui met en œuvre site internet avec le FQDN certifié ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AC peut demander la révocation d'un certificat dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN ou du nom du serveur), ceci avant l'expiration normale du certificat ;
- Le demandeur, CT ou Administrateur SSL, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité de l'entité propriétaire du nom de domaine ou la fin d'activité du serveur qui met en œuvre site internet avec le FQDN certifié ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La révocation de l'AC ;
- La fin de vie de l'AC ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AE peut demander la révocation d'un certificat dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN ou du nom du serveur), ceci avant l'expiration normale du certificat ;
- Le demandeur, CT ou Administrateur SSL, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

4.9.3 Procédure de demande de révocation

4.9.3.1 Certificat composante IGC

La DPC précise les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des CT et Administrateur SSL concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE. Ces derniers devront informer les CT et les Administrateur SSL de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le point de contact identifié sur le site : <http://www.references.modernisation.gouv.fr> doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. La DGME et l'ANSSI se réservent le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

4.9.3.2 Certificat SSL

Une demande de révocation contient les informations suivantes :

- L'identité du demandeur du certificat utilisée dans le certificat (nom, prénom, ...) ;
- le FQDN du serveur utilisée dans le certificat
- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série du certificat,...).

La demande de révocation est conservée par l'AE dans ses journaux.

L'AE authentifie la demande de révocation qu'elle reçoit (se reporter au § 3.4).

L'AE transmet la demande de révocation à l'AC.

L'AC (service de révocation) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC (service de révocation) révoque le certificat en incluant le numéro de série du certificat dans la prochaine LCR qui sera émise par l'AC.

Le demandeur de la révocation est informé de la révocation effective du certificat. De plus, si le CT ou l'Administrateur SSL n'est pas le demandeur, alors le CT ou l'Administrateur SSL est également informé de la révocation effective du certificat.

L'organisation Client (propriétaire du nom de domaine), se reporter § 3.2.2, est informée de la révocation des certificats qui lui sont rattachés (au sens propriété du FQDN).

4.9.4 Délai accordé pour formuler la demande de révocation

Dès que le demandeur a connaissance qu'une des causes possibles de révocation de son ressort, est effective, il formule sa demande de révocation sans délai.

4.9.5 Délai de traitement d'une révocation

4.9.5.1 Certificat Composantes IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR et/ou de réponses OCSP) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.5.2 Certificat SSL

Le service de révocation est disponible 24 heures sur 24 et 7 jours sur 7 suivant un taux de disponibilité définie dans la DPC.

Une demande de révocation, authentifié et dûment établie par l'AE, de certificat SSL est traitée dans un délai inférieur à 24 heures.

4.9.6 Exigences de vérification de révocation pour les tierces parties

Il appartient aux UC de vérifier l'état de validité d'un certificat à l'aide de l'ensemble des LCR émises et/ou du service OCSP mise en œuvre par l'AC.

4.9.7 Fréquences de publication des LCR

La LCR est émise toute les 24 Heures.

4.9.8 Délai maximum de publication d'une CRL

Le délai maximum de publication d'une LCR suite à sa génération est de 30 minutes.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'AC met en œuvre un serveur OCSP dont l'URL est : <http://kvalid.keynectis.com/ssl-rgs-ocsp/>.

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre 4.9.6 ci-dessus.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats SSL, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC la révocation suite à une compromission de sa clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.). En cas de révocation de l'AC, l'ensemble des certificats SSL sont révoqués.

Les conditions générales d'utilisation du certificat mentionnent clairement qu'en cas de compromission de la clé privée d'un certificat SSL ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le CT ou l'Administrateur SSL s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13 Causes possibles d'une suspension

Sans objet.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Service d'état des certificats

4.10.1 Caractéristiques opérationnelles

Le service OCSP est mis à jour à partir des LCR émises par l'AC. Cependant le mécanisme principal de communication du statut des certificats est la LCR publiée par l'AC. Dans tous les cas, les utilisateurs de certificats peuvent utiliser un mécanisme de consultation libre de LCR et LAR. Ces LCR et LAR sont des LCR au format V2, publiées au moins dans un annuaire accessible en protocole LDAP V3.

4.10.2 Disponibilité de la fonction

Le service OCSP est mis à jour à partir des LCR émises par l'AC. Le service est disponible 24 heures sur 24 et 7 jours sur 7 suivant un taux de disponibilité préciser dans la DPC. Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue est fixé à un maximum donné dans la DPC.

4.11 Fin de la relation avec l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le CT ou l'Administrateur SSL avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat SSL est révoqué.

4.12 Séquestre et recouvrement de clés

Les bi-clés et les certificats SSL et d'AC émis conformément à la PC ne font pas l'objet de séquestre ni de recouvrement.



5 MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN ŒUVRE

5.1 Sécurité physique

5.1.1 Situation géographique

Le site d'exploitation de l'AC respecte les règlements et normes en vigueur et son installation tient compte des résultats de l'analyse de risques, du métier d'opérateur de certification selon la méthode EBIOS, par exemple certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...) réalisées par l'OSC.

5.1.2 Accès physique

Afin de limiter l'accès aux applications et aux informations de l'IGC et afin d'assurer la disponibilité du système d'exploitation de l'AC, l'OSC met en place un périmètre de sécurité opéré pour ses besoins. La mise en œuvre de ce périmètre permet de respecter les principes de séparation des rôles de confiance telle que prévus dans cette PC.

Les accès au site de l'OSC, qui met en œuvre les services d'IGC, sont limités aux seules personnes nécessaires à la réalisation des services et selon leur besoin d'en connaître. Les accès sont nominatifs et leur traçabilité est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion passifs et actifs. Tout évènement de sécurité fait l'objet d'un enregistrement et d'un traitement.

5.1.3 Energie et air conditionné

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre par l'OSC afin d'assurer la continuité des services délivrés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs.

5.1.4 Exposition aux liquides

Les systèmes de l'OSC sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions.

5.1.6 Mise hors service des supports

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation.

5.1.7 Sauvegardes hors site

L'OSC réalise des sauvegardes hors site permettant une reprise rapide des services d'IGC suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services.

Les précisions quant aux modalités des sauvegardes des informations sont fournies dans la DPC.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance de l'AC sont classés en 4 groupes :

- Les personnels d'exploitation, dont la responsabilité est le maintien de des systèmes qui supportent l'IGC en conditions opérationnelles de fonctionnement ;
- Les personnels d'administration, dont la responsabilité est l'administration technique des composantes de l'IGC ;
- Les personnels opérationnels dont la responsabilité est de mettre en œuvre les fonctions d'IGC ;
- Les personnels de « sécurité », dont la responsabilité est de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de la composante d'IGC ;
- Les personnels porteurs de données d'activation de clé.

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

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

5.2.3 Identification et authentification des rôles

L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel qui est amené à mettre en œuvre les services de l'IGC avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

Ces contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de l'AC. Chaque attribution d'un rôle à un membre du personnel de l'IGC lui est notifiée par écrit ou équivalent.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétence et habilitations requises

Chaque personne amenée à travailler au sein de l'AC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de certification de l'IGC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

L'AC met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante au sein de laquelle il opère.

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Gestion des métiers

Des précisions sont fournies dans la DPC.

5.3.6 Sanctions en cas d'actions non autorisées

Des précisions sont fournies dans la DPC.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Des précisions sont fournies dans la DPC.

5.3.8 Documentation fournie au personnel

Des précisions sont fournies dans la DPC.

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer les événements manuellement ou électroniquement par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier et / ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'événements à enregistrer

L'IGC journalise les événements concernant les systèmes liés aux fonctions qu'elles mettent en œuvre dans le cadre de l'IGC :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evénements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres événements sont également recueillis. Il s'agit d'événements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ayant des rôles de confiance ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'IGC, des événements spécifiques aux différentes fonctions de l'IGC sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Evénements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction,...) ;
- Génération des certificats ;
- Transmission des certificats et selon les cas, acceptations / rejets ;
- Publication et mise à jour des informations liées à l'AC ;
- Génération d'information de statut d'un certificat SSL.

Chaque enregistrement d'un événement dans un journal contient les champs suivants :

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement ;
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements.

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés:

- Destinataire de l'opération ;
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

5.4.2 Processus de journalisation

Les opérations de journalisation sont effectuées au cours du processus considéré. En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement. Des précisions sont fournies dans la DPC.

5.4.3 Protection des journaux d'évènements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.4 Procédures de sauvegarde des journaux d'évènements

L'IGC mettent en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risques de l'AC.

5.4.5 Système de collecte des journaux d'évènements

Des précisions sont fournies dans la DPC.

5.4.6 Evaluation des vulnérabilités

L'AC et l'AE doivent être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés au moins à une fréquence mensuelle. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

5.5.1 Type de données archivées

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- La politique de certification ;
- La déclaration des pratiques de certification ;
- Les certificats SSL et ceux des composantes de l'IGC (dont ceux de la hiérarchie d'AC) et les LCR des AC associées ;
- Les justificatifs d'identité des CT et des Administrateurs SSL et, le cas échéant, de leur entité de rattachement ;
- Les dossiers complets de demandes de certificats et de révocation ;
- Les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Certificats et LCR émis par l'AC

Les certificats SSL et d'AC sont archivés 5 ans après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 sont archivés pendant 5 ans après leur génération.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- Seront protégées en intégrité ;
- seront accessibles aux seules personnes autorisées ;
- pourront être consultées et exploitées.

5.5.4 Exigences d'horodatage des données

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

5.5.5 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (Se reporter au 5.5.3).

5.5.6 Procédures de récupération et de vérification des archives

Les archives papier sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées. Les sauvegardes électroniques archivées sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées.

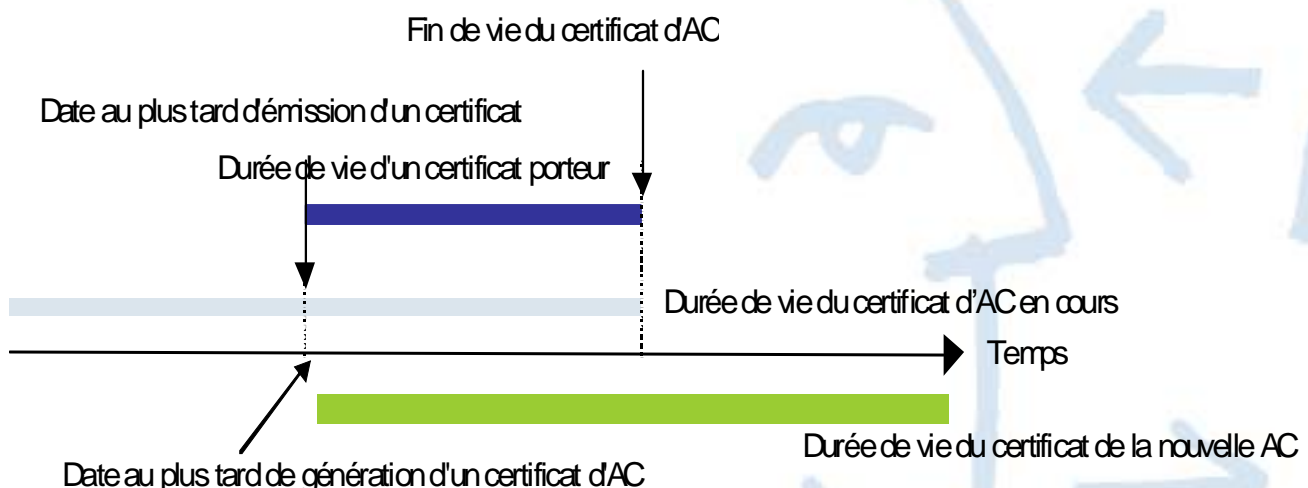
5.6 Renouvellement de bi-clé

5.6.1 Certificat d'AC

La durée de vie d'un certificat d'AC est 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 conformément aux recommandations des autorités nationale ou internationale compétentes en la matière. La DPC précise les standards utilisés.

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

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



Par ailleurs, l'AC change sa bi-clé et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

5.6.2 Certificat SSL

La durée de validité d'un certificat est de 3 ans maximum.

5.7 Compromission et plan de reprise

5.7.1 Procédures en cas d'incident et de compromission

L'AC 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.

L'AC 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 fait partie du périmètre audité, selon le paragraphe 8 ci-dessous.

Les personnels de l'AC 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 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 l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou les CT et les Administrateurs SSL devient insuffisant pour son utilisation prévue restante, alors l'AC :

- Informe tous les CT et les Administrateurs SSL et les UC avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats ;
- Révoque tout les certificats concernés.

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

L'AC doit également prévenir directement et sans délai le point de contact identifié sur le site : <http://www.references.modernisation.gouv.fr>.

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

Si le matériel de l'AC 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.

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

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

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

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

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 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

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC :

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats SSL et des informations relatives aux certificats) ;
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des CT ou des Administrateurs SSL ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire ;
- L'AC doit communiquer au point de contact identifié sur le site <http://www.referencessmodernisation.gouv.fr>, les principes du plan d'action mettant en oeuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à la DGME et à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les CT et les Administrateurs SSL et les utilisateurs de certificats ;
- L'AC doit tenir informées la DGME et l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

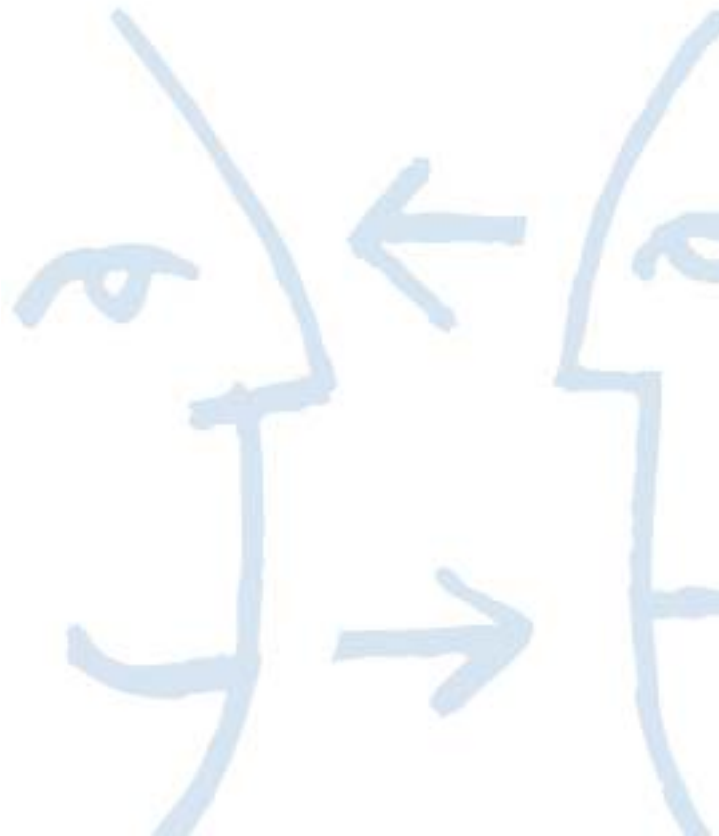
Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC procède aux actions suivantes :

- La notification des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- Révoque son certificat ;
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Informe (par exemple par récépissé) tous les des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.



6 MESURES TECHNIQUES DE SECURITE

6.1 Génération et installation des bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Bi-clés d'AC

Suite à l'accord de l'AAK pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle.

Les cérémonies de clés se déroulent sous le contrôle d'au moins 2 personnes dans des rôles de confiance (maître de cérémonie et témoins) et sont impartiaux. Elle se déroule dans les locaux de l'OSC. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Les rôles impliqués dans les cérémonies de clés sont précisés dans la DPC.

Suite à leur génération, les parts de secrets (données d'activation) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

6.1.1.2 Bi-clés SSL

La génération de la bi-clé est réalisée directement dans le support matériel de la bi-clé par le CT ou l'Administrateur SSL ou sous contrôle du CT ou de l'Administrateur SSL. Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité conformément aux exigences du RGS.

Le CT et l'Administrateur SSL s'engage, en signant la demande de certificat à l'AC, à respecter les exigences du RGS en la matière. L'AC n'est pas responsable du processus choisi par le CT et l'Administrateur SSL pour la génération, la protection et l'utilisation de la bi-clé certifiée.

6.1.2 Fourniture de la clé privée

Il n'y a pas de fourniture de clé privée au CT ou à l'Administrateur SSL car c'est le CT ou l'Administrateur SSL qui gère la génération de la bi-clé à certifier (cf. 6.1.1.2).

La clé reste donc constamment sous le contrôle et la responsabilité du CT et de l'Administrateur SSL.

6.1.3 Fourniture de la clé publique à l'AC

La clé publique est transmise à l'AE par le CT, lors de la demande de certificat, au format PKCS#10 et la transmission est authentifiée par l'AE.

La clé publique est transmise à l'AC par l'Administrateur SSL qui initie la demande de certificat auprès de l'AE, sous un format PKCS#10, et lors d'une connexion sécurisée (SSL) de manière à garantir l'intégrité et la confidentialité de la communication et l'authentification entre l'AC et l'AE.

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

Le certificat de l'AC est remis au CT ou à l'Administrateur SSL lors de la remise du certificat au CT ou à l'Administrateur SSL.

Le certificat de l'AC Racine dont dépend l'AC est contenu dans les principaux navigateurs internet.

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 et AC doivent ou ne doivent pas être modifiés.

L'utilisation de l'algorithme RSA avec la fonction de hachage SHA1 est utilisée pour l'AC. La taille de la bi-clé de l'AC est d'au moins 2048 bits.

La longueur des clés des certificats SSL est de 2048 bits minimum pour l'algorithme RSA avec la fonction de hachage SHA1.

6.1.6 Production des paramètres des clés publiques et contrôle de qualité

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles évaluées certifiées EAL 4+ et qualifié standard par l'ANSSI.

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

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 et certificat AC est la suivante :

- AC :
 - o Key CertSign ;
 - o Key CRL Sign ;
- Certificat SSL :
 - o Digital signature.

L'utilisation du champ « Extended key usage » dans le certificat SSL est la suivante :

- Certificat SSL :
 - o id-kp-serverAuth.

6.2 Protection des clés privées et normes relatives au module cryptographique

6.2.1 Normes applicables aux ressources cryptographiques et contrôles

La ressource cryptographique matérielle de l'AC utilise des générateurs d'aléas qui devront être conformes à l'état de l'art, aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés devront être conformes aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

6.2.2 Contrôle de la clé privée par de multiples personnes

L'activation de la clé privée d'AC est contrôlée par au moins 2 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 font l'objet d'une authentification forte. L'AC est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seuls rôles de confiance qui peuvent émettre des certificats.

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.2.3 Séquestre de clé privée

Les clés privées d'AC et des serveurs ne font jamais l'objet de séquestre.

6.2.4 Sauvegarde de clé privée

6.2.4.1 AC

La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées sont 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. Les sauvegardes de clés privées d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme de fichier chiffrée (AES ou 3DES).

6.2.4.2 Certificat SSL

Le CT ou l'Administrateur SSL peut procéder à une copie de sauvegarde de sa clé privée afin de pouvoir la déployer sur plusieurs serveurs en cas d'incident ou pour des raisons de performances des sites internet ainsi protégés.

Le CT et l'Administrateur SSL sont responsables de définir et de faire respecter les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.2.5 Archivage de clé privée

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

6.2.6 Importation / exportation d'une clé privée

Les clés d'AC 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 sont chiffrées au moyen de l'algorithme AES ou 3DES. Une clé privée d'AC 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 stockées dans des ressources cryptographique matérielle 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

6.2.8.1 AC

Les clés privées d'AC ne peuvent être activées qu'avec un minimum de 2 personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

6.2.8.2 Certificat SSL

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.2.9 Méthode de désactivation d'une clé privée

6.2.9.1 AC

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC 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 sont en ligne uniquement afin de signer des certificats SSL et des LCR après avoir authentifié la demande de certificat et la demande de révocation.

6.2.9.2 Certificat SSL

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.2.10 Méthode de destruction d'une clé privée

6.2.10.1 AC

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 retrouver.

6.2.10.2 Certificat SSL

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de destruction de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.2.11 Certification des ressources cryptographiques

Se reporter au § 6.2.1.

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 (Se reporter au § 5.5.2 ci-dessus).

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

6.3.2.1 AC

Comme une AC 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 moins la durée de vie des certificats SSL émis.

6.3.2.2 Certificat SSL

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 AC

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (Se reporter au § 6.1.1.1). 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 après génération pendant la cérémonie des clés. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Certificat SSL

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.4.2 Protection des données d'activation

6.4.2.1 AC

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'une même AC à un même instant.

6.4.2.2 Certificat SSL

Le CT et l'Administrateur SSL sont responsables de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.4.3 Autres aspects touchant aux données d'activation

Les données d'activation sont changées dans le cas où 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 IGC 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 ;
- Requier l'identification des utilisateurs ;
- Assure la séparation rigoureuse des tâches ;
- Fournit une autoprotection du système d'exploitation.

Quand un composant d'IGC 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'IGC sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

6.5.2 Indice de sécurité informatique

Les composants d'IGC utilisés pour supporter les services d'AC et qui sont hébergés par l'OSC 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'IGC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'IGC ;
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'IGC. Seules les applications nécessaires à l'exécution des activités IGC sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC 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 installés 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, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'IGC. Lors de son premier chargement, on vérifie que le logiciel de l'IGC 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 poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

6.7 Mécanismes de sécurité du réseau

L'AC est en ligne accessible par des postes informatiques sous contrôle. Les composantes accessibles de l'IGC 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).

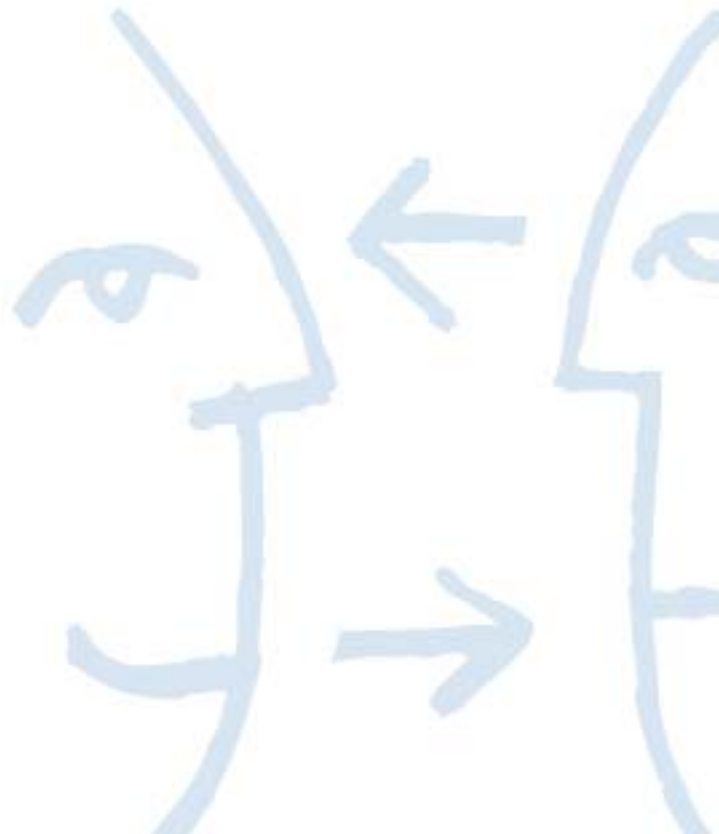
Les autres composantes de l'IGC de l'AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système IGC est hébergé refuse tout service, hormis ceux qui sont nécessaires au système IGC, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

6.8 Horodatage/Système de datation

Il n'y a pas d'horodatage utilisé par l'AC mais une datation sûre. Tous les composants de l'AC 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, CRL, ET PROFILS OCSP

7.1 Profil de Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats SSL et AC sont définis par le RFC 5280.

7.1.1 Extensions de Certificats

7.1.1.1 Certificat AC

7.1.1.2 Champs de base du certificat

Les informations principales contenues dans le certificat de l'AC sont :

Champ de base	Valeur
Issuer DN	CN = Class 2 Primary CA O = Certplus C = FR
Subject DN	CN = KEYNECTIS SSL RGS OU = 0002 478217318 O = KEYNECTIS C = FR
Longueur des clefs de l'AC :	2048

7.1.1.3 Extension du certificat

Les informations principales contenues dans le certificat de l'AC sont :

- Authority Key Identifier ;
- Basic Constraint (critique) ;
- Key Usage (critique) ;
- CRL distribution point ;
- Subject Key Identifier.

7.1.1.4 Certificat SSL

Les informations principales contenues dans le certificat SSL sont :

Champ de base	Valeur
Issuer DN	CN = KEYNECTIS SSL RGS OU = 0002 478217318 O = KEYNECTIS C = FR
Subject DN	Se reporter au 3.1.1.2
Longueur des clefs de l'AC :	2048

7.1.1.5 Extension du certificat

Les informations principales contenues dans le certificat sont :

- Authority Info Access
- Authority Key Identifier ;
- Basic Constraint (critique) ;
- Certificate Policies ;
- CRL Distribution Points ;
- Key Usage (critique) ;
- Extended key usage ;
- Subject Alternative Name ;
- Subject Key Identifier.

7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est Sha-1WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}.

7.1.3 Formes de noms

Les formes de noms respectent les exigences du § 3.1.1.2 pour l'identité des SSL et de l'AC qui est portée dans les certificats émis par l'AC.

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

Les certificats émis par l'AC contiennent l'OID de la PC qui est donné au § 1.2.

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.

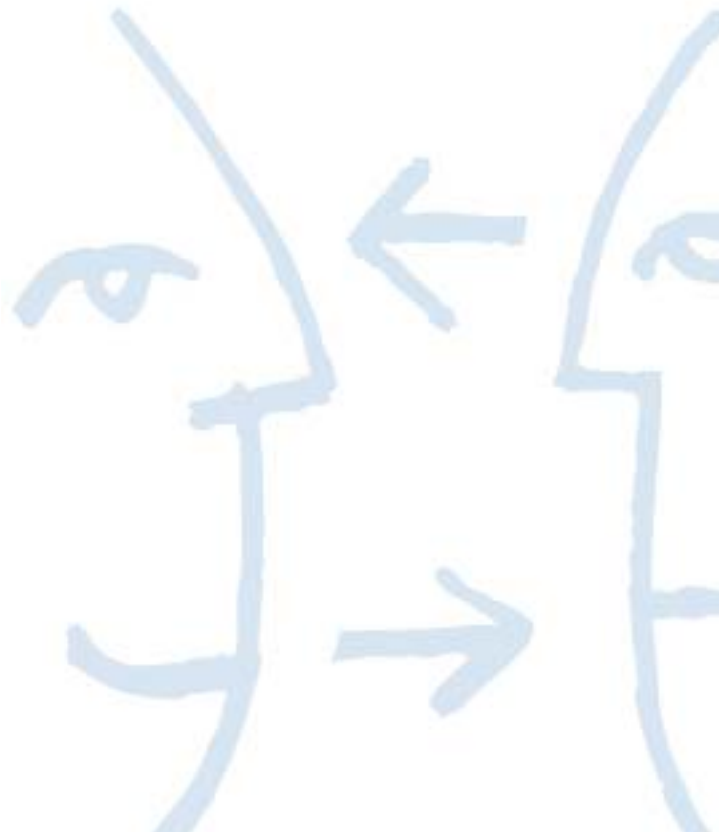
7.2 Profil de LCR

7.2.1 LCR et champs d'extensions des LCR

La DPC donne le détail.

7.3 Profil OCSP

La DPC donne le détail.



8 CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et motifs des audits

L'AC fait l'objet d'audit périodique de conformité au moins une fois par an, pour permettre à l'AAK d'autoriser l'AC d'émettre ou non (selon le résultat des audits) des certificats SSL au titre de la présente PC. Cet audit est réalisé dans le cadre de la qualification RGS de l'AC.

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par le COFRAC en France (Se reporter au [PROG_ACCRED]) conformément à [QPSCe] et au [décretRGS].

La démarche et les exigences liées aux audits de qualification sont définies dans [PROG_ACCRED] et ne sont donc pas reprises ici.

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. Les auditeurs en charge de l'audit de conformité doivent effectuer l'audit de conformité comme tâche principale. L'AAK apporte une attention particulière quand à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit. L'AAK 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 l'AAK, soit une entité de l'AAK suffisamment séparée de l'AC afin d'effectuer une évaluation juste et indépendante.

L'AAK 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

L'AAK peut décider que l'AC 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, l'AAK peut suspendre les opérations de la composante non conforme de l'IGC, ou peut donner l'ordre de cesser toute relation avec la composante en question, 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 l'AAK ;
- 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 de l'AAK.

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

Quand les actions correctives sont réalisées, l'AC en informe l'AAK 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 à l'AAK comme prévu au § 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 au § 8.5 ci-dessus. Le Rapport de Contrôle de Conformité n'est rendu disponible à des tiers utilisateurs sur Internet.

9 AUTRES DISPOSITIONS COMMERCIALES ET JURIDIQUES

9.1 Tarifs

9.1.1 Tarifs pour l'émission et le renouvellement de certificats

Conformément aux conditions tarifaires en vigueur de KEYNECTIS publiés sur le site internet www.keynectis.com ou convenu avec le Client dans le cadre d'un contrat de service.

9.1.2 Tarifs pour l'accès aux certificats

Conformément aux conditions tarifaires en vigueur de KEYNECTIS publiés sur le site internet www.keynectis.com ou convenu avec le Client dans le cadre d'un contrat de service.

9.1.3 Tarifs pour l'accès aux LCR et aux informations d'état des certificats

Le SP de l'AC KEYNECTIS SSL (qui contient la LCR pour le certificat de l'AC et de l'AC KEYNECTIS SSL) est accessible gratuitement sur Internet. Cette publication ne sera pas utilisée par les services OCSP ou autre service similaire, mais uniquement par les parties utilisatrices afin de vérifier si un certificat est ou non valide.

9.1.4 Tarifs pour d'autres services

Conformément aux conditions tarifaires en vigueur de KEYNECTIS publiés sur le site internet www.keynectis.com ou convenu avec le Client dans le cadre d'un contrat de service.

9.1.5 Politique de remboursement

Conformément aux conditions tarifaires en vigueur de KEYNECTIS publiés sur le site internet www.keynectis.com ou convenu avec le Client dans le cadre d'un contrat de service.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Keynectis atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations relatives au présent Contrat.

9.2.2 Autres ressources

L'AC dispose de ressources financières suffisantes à son bon fonctionnement et à l'accomplissement de sa mission.

9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité utilisatrice du fait d'un manquement par l'AC à ses obligations, l'AC pourra être amené à dédommager l'entité utilisatrice dans la limite de la responsabilité de l'AC définie dans les conditions générales d'utilisation et aux présentes.

9.3 Confidentialité des informations et des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- La partie non-publique de la DPC de l'AC,
- Les clés privées de l'AC, des composantes et des porteurs de données d'activation,
- Les données d'activation associées aux clés privées d'AC et des certificats SSL,
- Tous les secrets de l'IGC,
- Les journaux d'événements des composantes de l'IGC,
- Le dossier d'enregistrement du CT et de l'Administrateur SSL,
- Les causes de révocations ne sont jamais publiées,
- La politique de sécurité interne de l'AC
- Les parties de la DPC considérées comme confidentielles.

Par ailleurs, l'AC 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 et peuvent utiliser ces informations confidentielles.

9.3.2 Informations hors du périmètre des informations confidentielles

Les données figurant dans le certificat ne sont pas considérées comme confidentielles.

9.3.3 Obligations en terme de protection des informations confidentielles

L'AC a mis en place et respecte des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles au sens de l'article 9.3.1 ci-dessus.

A cet égard, l'AC respecte notamment la législation et la réglementation en vigueur sur le territoire français. En particulier, il est précisé qu'elle peut devoir mettre à disposition les dossiers d'enregistrement des CT et Administrateurs SSL à des tiers dans le cadre de procédures légales.

L'AC permet également l'accès à ces informations au CT et à l'Administrateur SSL.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

La collecte et l'usage de données personnelles par l'AC dans le cadre du traitement des demandes de certificats sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi CNIL.

9.4.2 Informations considérées comme personnelles

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

- Données d'identification contenues dans les dossiers d'enregistrement fournis par le CT et l'Administrateur SSL ;
- Demande (renseignée) d'émission de certificat ;
- Demande (renseignée) de révocation de certificat ;
- Motif de révocation des certificats SSL.

9.4.3 Informations à caractère non personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des serveurs (qui sont considérées comme confidentielles sauf accord explicite du CT ou de l'Administrateur SSL) ;
- Les dossiers d'enregistrement des CT et Administrateur SSL.

9.4.4 Obligations en terme de protection des données personnelles

L'AC a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles au sens de l'article 9.4.1 ci-dessus dans le cadre de la délivrance et la gestion d'un certificat SSL.

Chacune des Parties prendra toutes les mesures adéquates en matière de protection des données à caractère personnel et se conformera pour l'exécution des présentes, aux obligations découlant des textes nationaux européens et le cas échéant internationaux en matière de protection des données personnelles. Chacune des Parties veillera à se conformer aux dispositions légales en vigueur relatives à la protection des données personnelles et notamment à la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004, et procédera ou fera procéder aux formalités nécessaires.

En outre, le contact du Client ayant le pouvoir d'accomplir tout acte nécessaire à l'exécution des présentes (notamment les demandes de certificats) au nom du Client dispose sur ses données personnelles d'un droit d'accès, de rectification, et de suppression qu'il peut exercer en s'adressant au Correspondant Informatique et Liberté de KEYNECTIS à l'adresse e-mail suivante : sandrine.barilli@keynectis.com.

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

Aucune des données à caractère personnel communiquées, contenu dans les dossiers d'enregistrement, par un CT ou un Administrateur SSL ne peut être utilisée par l'AC, pour une autre utilisation autre que celle définie dans le cadre de la PC, sans consentement exprès et préalable de la part du CT ou de l'Administrateurs SSL. Le consentement du CT ou de l'Administrateur SSL pour l'utilisation desdites données pour celle définie dans le cadre de la PC est considéré comme obtenu lors de la soumission de la demande de certificat et du fait de l'acceptation par le CT ou l'Administrateur SSL du certificat émis par l'AC.

9.4.6 Divulgaration due à un processus judiciaire ou administratif

L'AC agit conformément aux réglementations européenne et française et dispose de procédures sécurisées pour permettre l'accès des autorités judiciaires sur décision judiciaire ou autre autorisation légale aux données à caractère personnel.

9.4.7 Autres motifs de divulgation de données à caractère personnel

L'AC obtient l'accord du CT ou de l'Administrateur SSL (Se reporter au § 9.4.5) de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8.

9.5 Droits relatifs à la propriété intellectuelle

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, ...etc.) est sanctionnée par le Code de la propriété intellectuelle.

L'AC détient tous les droits de propriété intellectuelle et elle est propriétaire de la PC et de la DPC associée, des certificats émis par l'AC.

Le propriétaire du nom de domaine détient tous les droits de propriété intellectuelle sur les informations d'identification contenues dans les certificats SSL émis par l'AC et dont il est propriétaire.

9.6 Obligations et garanties

Les composantes de l'IGC, les Clients et la communauté d'utilisateurs de certificats sont responsables pour tous dommages occasionnés en suite d'un manquement de leurs obligations respectives telles que définies aux termes de la PC.

9.6.1 Obligations communes

Les obligations communes des différentes composantes de l'IGC sont :

- Assurer l'intégrité et la confidentialité des clés privées dont elles sont depositaires, ainsi que des données d'activation desdites clés privées, le cas échéant ;
- N'utiliser les clés publiques et privées dont elles sont depositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- Mettre en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent ;
- Documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'IGC ;
- Respecter et appliquer les termes de la présente PC qu'elles reconnaissent ;
- Accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées ;
- Respecter les conventions qui les lient aux autres entités composantes de l'IGC.

9.6.2 Obligations et garanties de l'AAK

Les obligations de l'AAK sont les suivantes :

- L'élaboration de la PC et de la DPC ;
- L'audit de l'AC ;
- Le contrôle de la relation contractuelle avec le CT ou l'Administrateur SSL agissant en tant qu'AE ;
- Documente les schémas de certification qu'elle entretient avec des AC tierces.

9.6.3 Obligations et garanties de l'AC

L'AC 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 est responsable du maintien de la conformité aux procédures prescrites dans la présente PC. L'AC fournit tous les services de certification en accord avec sa DPC. Les obligations communes aux composantes de l'AC 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 toutes les informations utiles, conformément aux intentions de l'AAK de contrôler et vérifier la conformité avec la PC ;
- Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- Mettre en œuvre 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 ;
- Met à la disposition de l'AE l'ensemble des moyens techniques nécessaires à la réalisation de ses obligations ;
- Prendre toutes les mesures raisonnables pour s'assurer que les CT et les Administrateurs SSL sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

L'AC est responsable de la conformité de sa PC, avec les exigences émises dans la PC Type Authentification serveur du RGS pour le niveau de sécurité *. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la PC Type Authentification Serveur RGS *, par elle-même ou l'une de ses composantes. Elle prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles fournies dans les dossiers d'enregistrement à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée.

9.6.4 Obligations de l'AE

Les obligations de l'AE sont les suivantes :

- L'authentification du demandeur (CT et Administrateur SSL) ;
- L'authentification de la demande de certificat ;
- L'authentification de la demande de révocation ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de l'AAK de contrôler et vérifier la conformité avec la PC ;

9.6.5 Obligations et garanties du CT

Les obligations du CT sont :

- Protéger en confidentialité et intégrité les informations confidentielles qu'il détient (clé privée et donnée d'activation) ;
- Transmettre la clé publique, correspondante à la clé privée, à l'AE ;
- Se conformer à toutes les exigences de la PC et de la DPC associée ;
- Garantir que les informations qu'il fournit à l'AE sont complètes et correctes ;
- Prendre toutes les mesures raisonnables pour éviter l'utilisation non autorisée de sa clé privée et en protéger la confidentialité ;
- Aviser immédiatement l'AE en cas de besoin de révocation de son certificat.

9.6.6 Obligations et garanties de l'Administrateur

Les obligations de l'Administrateur SSL sont :

- Protéger en confidentialité et intégrité les informations confidentielles qu'il détient (clé privée et donnée d'activation) ;
- Transmettre la clé publique, correspondante à la clé privée, à l'AE ;

- Se conformer à toutes les exigences de la PC et de la DPC associée ;
- Garantir que les informations qu'il fournit à l'AE sont complètes et correctes ;
- Ne générer que des certificats SSL que pour des FQDN pour lesquels il est autorisé et dont le nom de domaine principale est validé et vérifié par l'AE ;
- Prendre toutes les mesures raisonnables pour éviter l'utilisation non autorisée de sa clé privée et en protéger la confidentialité ;
- Aviser immédiatement l'AE en cas de besoin de révocation de son certificat.

9.6.7 Obligations et garanties du SP

Les obligations du SP sont :

- De publier les LCR ;
- De publier les certificats d'AC ;
- De publier la PC et les CGU associées ;
- De garantir les taux de disponibilités des informations publiées ;
- De protéger les accès au SP.

9.6.8 Obligations et garanties des autres participants

9.6.8.1 Obligations et garanties de l'UC

Les obligations de l'UC sont :

- De valider un certificat SSL à l'aide de la LCR ou du service OCSP fournit par KEYNECTIS.

9.7 Limite de garantie

L'AC garantit au travers de ses services d'IGC :

- L'identification et l'authentification de l'AC avec son certificat auto signé ;
- L'identification et l'authentification des noms de domaine FQDN avec les certificats SSL générés par l'AC ;
- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Ces garanties sont exclusives de toute autre garantie de l'AC.

L'émission de Certificats, conformément à la PC, ne fait pas de l'une des composantes de l'IGC, un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du CT, de l'Administrateur SSL et du Client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

En conséquence de quoi, les CT, les Administrateurs SSL, les Clients et les utilisateurs de Certificat sont des personnes juridiquement et financièrement indépendantes de l'AC et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'AC ou de l'une des composantes de l'IGC. Les services de certification (Se reporter au § 1.3) ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre.

Le fait que le nom d'une organisation soit dans un certificat et utilisé à des fins d'authentification de nom de domaine ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur du Client.

9.8 Limites de responsabilité

KEYNECTIS n'est pas responsable quant à la forme, la suffisance, l'exactitude, l'authenticité la falsification ou l'effet juridique des documents et informations remis lors de la demande d'émission, de renouvellement ou de révocation d'un Certificat.

KEYNECTIS ne garantit pas l'exactitude des informations fournies par le Client à l'utilisateur de certificat, ni les conséquences d'une négligence ou d'un manque de précaution ou de sécurité imputable au Client.

KEYNECTIS ne garantit pas l'exactitude des informations fournies par le Client, ni les conséquences d'une négligence ou d'un manque de précaution ou de sécurité imputable au Client et à l'Administrateur SSL.

En outre, le Client demeure responsable à l'égard de KEYNECTIS de toute utilisation non autorisée :

- du Certificat Administrateur SSL et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée ;
- des Certificats SSL et des dommages qui pourraient en résulter.

En outre, le Client demeure responsable à l'égard de KEYNECTIS de toute utilisation non autorisée du Certificat SSL et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée.

KEYNECTIS n'assume aucun engagement ni responsabilité quant aux conséquences dues à tout retards, perte, altération, destruction, utilisation frauduleuse des données, transmission accidentelle de virus ou tout autre élément nuisible via toute télécommunication telle que Internet. En outre, KEYNECTIS n'est pas responsable de la qualité de la liaison internet du Client.

Dans le cas où la responsabilité de KEYNECTIS serait retenue au titre des présentes Conditions Générales d'Utilisation, il est expressément convenu que KEYNECTIS serait tenue à réparation des dommages directs certains et immédiats, dont le Client apportera la preuve, dans les limites maximums fixées par KEYNECTIS.

Keynectis exclut toute responsabilité en cas de non respect par le Client de ses obligations définies dans les présentes et dans la Politique de Certification.

KEYNECTIS ne sera pas responsable des préjudices indirects ou imprévisibles subis par le Client, tels que notamment les pertes de bénéfices, de vente, de contrats, de chiffre d'affaires, de revenus ou d'économies anticipées, perte de clientèle, préjudice d'exploitation, atteinte à l'image de marque, perte de données ou usage de celles-ci, inexactitude ou corruption de fichiers, en relation ou provenant de l'inexécution ou exécution fautive des présentes ou inhérents à l'utilisation des Certificats émis par KEYNECTIS.

Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure au sens de l'article 14 ci-après.

9.9 Indemnités

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'AC vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés lors de la procédure prévue à l'article 9.3 des présentes.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée

La PC devient effective une fois approuvée par l'AAK. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Résiliation

Selon l'importance des modifications apportées à la PC, l'AAK décidera soit de faire procéder à un audit de la PC/DPC des AC concernées, soit de donner instruction à l'AC de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

9.10.3 Effets de la résiliation et survie

La fin de validité de la PC entraîne la cessation de toutes les obligations et responsabilités de l'AC pour les certificats émis conformément à la PC.

9.11 Amendements

9.11.1 Procédure pour apporter un amendement

L'AAK révisé 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'AAK. 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.

9.11.2 Mécanisme et délais des notifications

L'AAK donne un préavis d'1 mois au moins aux composantes de l'IGC de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des

modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, ...) et non sur la forme de la PC et de la DPC.

9.11.3 Motifs selon lesquels un OID doit être changé

Si l'AAK 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

En cas de contestation ou de litige, les parties décident de soumettre cette difficulté à une procédure amiable, préalablement à toute procédure devant un tribunal. A ce titre, toute partie qui souhaite mettre en jeu ladite procédure doit notifier par lettre recommandée avec avis de réception une telle volonté, en laissant un délai de quinze (15) jours à l'autre partie.

Les parties désignent alors un expert amiable d'un commun accord dans ledit délai de quinze (15) jours.

A défaut d'accord, compétence expresse est attribuée à M. le Président du Tribunal de Grande Instance de Paris pour effectuer une telle désignation.

L'expert amiable doit tenter de concilier les parties dans un délai de 30 jours à compter de sa saisine. Il propose un rapport en vue de concilier chacune des parties. Ce rapport a un caractère confidentiel et ne peut servir que dans le cadre de la procédure d'expertise amiable.

En cas de conciliation, les parties s'engagent à signer un accord transactionnel et confidentiel. Cet accord transactionnel doit expressément préciser si les présentes continuent à s'appliquer.

A défaut d'accord écrit des parties, le conciliateur établit un Procès Verbal de non-Conciliation daté et signé en trois exemplaires, dont un destiné à chaque partie au présent contrat et qu'il conserve à titre probatoire.

Les parties conviennent qu'aucune action contentieuse ne peut être valablement introduite avant que ne se soit écoulé un jour franc à compter de la date figurant sur ce PV de non-Conciliation.

L'AAK s'assure que tous les accords qu'elle conclut prévoient des procédures adéquates pour le règlement des différends.

Entre autre, l'AC définit sa politique de nommage et propose, et s'autorise dans certains cas, 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.

Lorsque le différent porte sur une identité, alors il est du ressort du Client de gérer et de résoudre le litige. L'AAK s'assure que le Client a décrit et prévu ce type de litige dans ses procédures en qualité d'AE.

9.13 Droit applicable

Les dispositions de la politique de certification sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.

9.14 Conformité au droit applicable

La 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.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

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'AAK a le droit d'affecter et de déléguer la PC à une partie de son choix.

9.15.3 Divisibilité

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention de ladite Politique de Certification.

Les intitulés portés en tête de chaque Article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

9.15.4 Exonération des droits

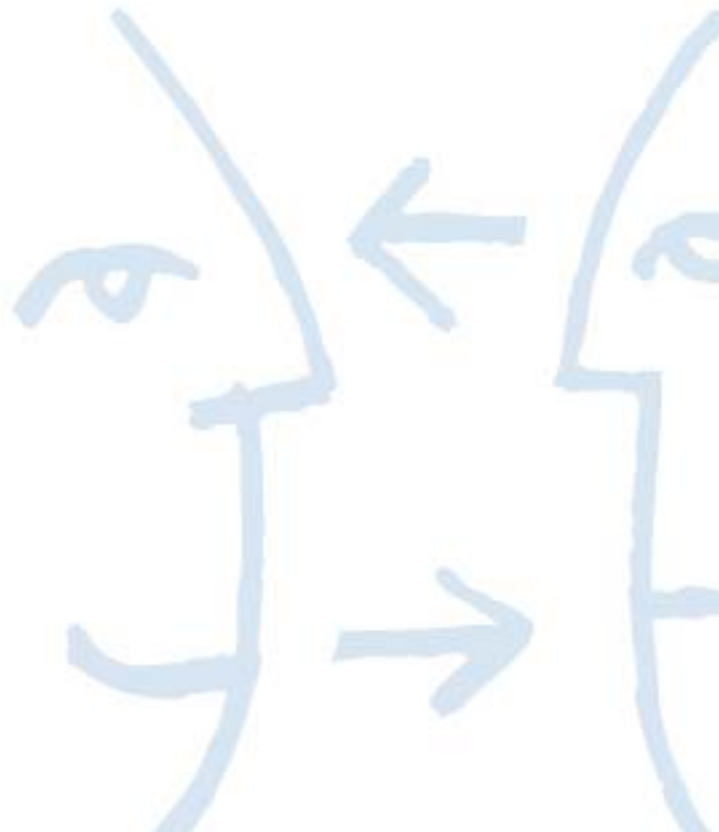
Les exigences définies dans la PC/DPC doivent être appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, soit possible.

9.15.5 Force majeure

L'AC 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, CT et Administrateurs SSL.

9.16 Autres dispositions

Le cas échéant, la DPC en fournira les détails.



10 REFERENCES

Les documents référencés sont les suivants :

- [CNIL] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;
- [ORDONNANCE] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives ;
- [DécretRGS] Décret relatif à l'Ordonnance n° 2005-1516 du 8 décembre 2005 ;
- [RGS] Référentiel Général de Sécurité – Arrêté ou version de travail publiée. ;
- [PROG_ACCRED] : COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf www.cofrac.fr.

