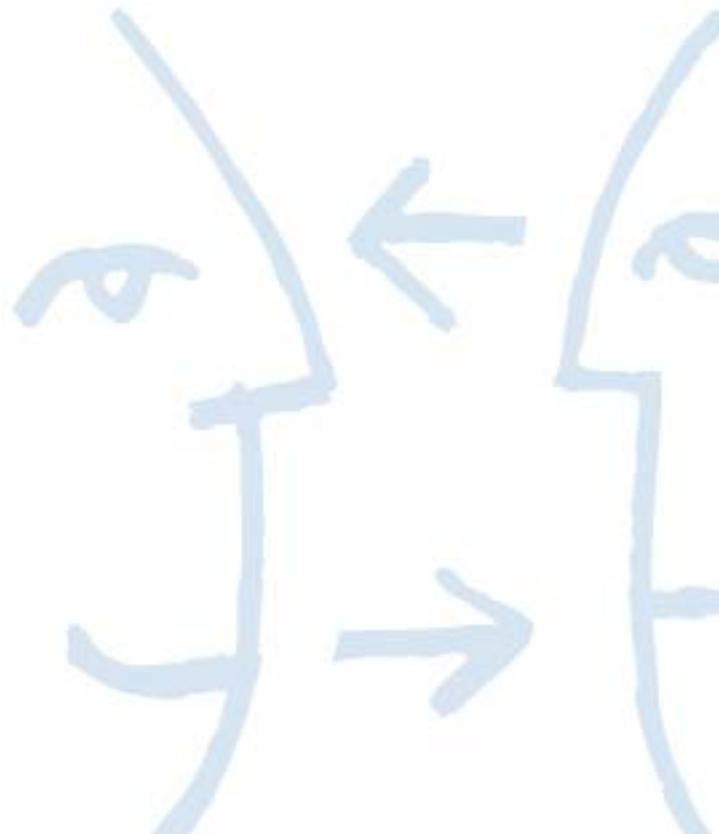




KEYNECTIS

■ POLITIQUE DE CERTIFICATION DE L'AC KEYNECTIS SSL

Date : 30/10/08



POLITIQUE DE CERTIFICATION DE L'AC KEYNECTIS SSL

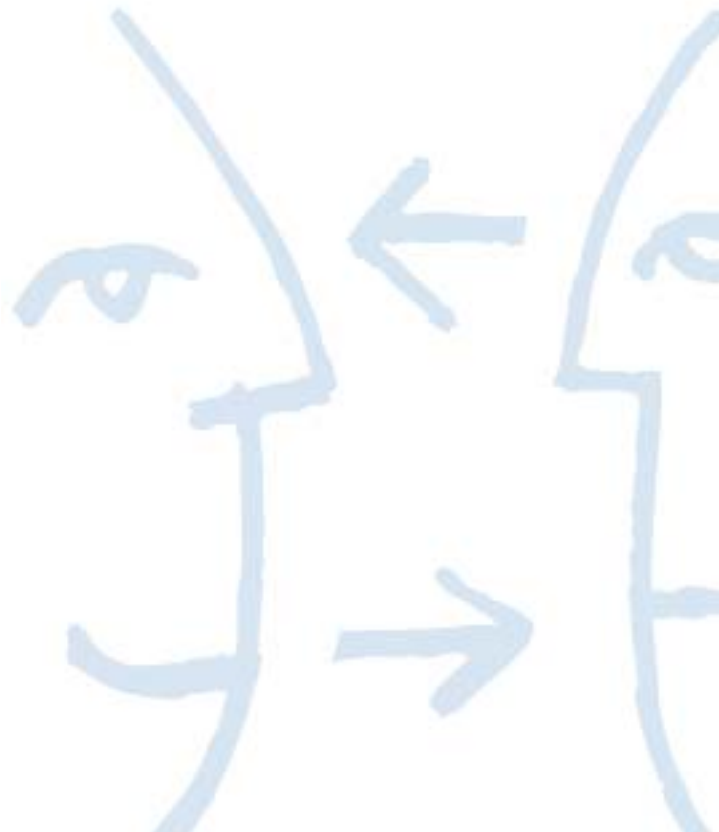
Sujet : Politique de Certification de l'AC KEYNECTIS SSL

Numéro de version : 1.2 **Nombre de pages :** 53
Statut du document : Projet Version finale
Auteur : Emmanuel MONTACUTELLI KEYNECTIS

Liste de diffusion : Externe Interne KEYNECTIS
 KEYNECTIS

Historique :

Date	Version	Auteur	Commentaires	Validé par
12/12/07	0.1	EM	Création du document	JYF
03/01/08	0.2	EM	Réponse aux commentaires	JYF
08/01/08	0.3	CDR	Révision	JYF
23/01/08	0.4	CDR	Révision	JYF
18/02/08	1.0	CDR	Version à publier	JYF
30/10/08	1.1	EM/MQ	Intégration d'un commentaire, modification des limites de responsabilité	
05/02/09	1.2	JYF	Mise à jour relative à l'offre Silver	TdV – BG - MQ



SOMMAIRE

1	INTRODUCTION	8
1.1	Vue d'ensemble	8
1.2	Nom du document et identification	9
1.3	Composantes de l'ICP	9
1.3.1	Autorité de Certification SSL de KEYNECTIS (AC KEYNECTIS SSL)	10
1.3.2	Autorité d'Enregistrement (AE)	10
1.3.3	Service de Publication	10
1.3.4	Propriétaire du Nom de Domaine	10
1.3.5	Contact Technique (CT)	10
1.3.6	Administrateur SSL	10
1.3.7	Autres composantes	11
1.4	Utilisation du certificat	12
1.4.1	Utilisation appropriée du certificat	12
1.4.2	Utilisation interdite du certificat	12
1.5	Administration de la politique	12
1.5.1	Organisation régissant le document	12
1.5.2	Contact	12
1.5.3	Responsable de la conformité de la PC	12
1.5.4	Procédure d'Approbation de la DPC	13
1.6	Définitions et acronymes	13
1.6.1	Définition	13
1.6.2	Acronymes	16
2	RESPONSABILITÉS EN TERMES D'ANNUAIRE ET DE PUBLICATION	18
2.1	Annuaire	18
2.2	Publication des informations de certification	18
2.3	Date et fréquence de publication	18
2.4	Contrôles d'accès à l'annuaire	18
3	IDENTIFICATION ET AUTHENTIFICATION	19
3.1	Dénomination	19
3.1.1	Conventions de noms	19
3.1.2	Utilisation de noms explicites	19
3.1.3	Anonymat ou pseudonyme des clients	19
3.1.4	Règles d'interprétation des différentes formes de noms	19
3.1.5	Unicité des noms	19
3.1.6	Reconnaissance, authentification et rôle des marques de commerce	20
3.2	Validation initiale de l'identité	20
3.2.1	Méthode permettant de prouver la possession d'une clé privée	20
3.2.2	Vérification de l'identité d'une organisation	20
3.2.3	Vérification de l'identité d'une personne	20
3.2.4	Informations non vérifiées	20
3.2.5	Validation de l'Autorité	20
3.2.6	Critères d'interfonctionnement	21
3.3	Identification et authentification des demandes de renouvellement de clés	21
3.3.1	Identification et authentification pour le renouvellement des clés après leur expiration	21
3.3.2	Identification et authentification pour le renouvellement des clés après leur révocation	21
3.4	Identification et authentification des demandes de révocation	21
4	EXIGENCES OPÉRATIONNELLES LIÉES AU CYCLE DE VIE DES CERTIFICATS	22
4.1	Demande de certificat	22
4.1.1	Origine d'une demande de certificat	22
4.1.2	Processus et responsabilités d'inscription	22



4.2	Traitement d'une demande de certificat	23
4.2.1	Fonctions d'identification et d'authentification	23
4.2.2	Approbation ou rejet des demandes de certificat	24
4.2.3	Durée de traitement des demandes de certificats	24
4.3	Délivrance du certificat	25
4.3.1	Actions de l'AC concernant la délivrance d'un certificat K.SSL Silver	25
4.3.2	Actions de l'AC concernant la délivrance d'un certificat (offres K.SSL Gold et K.SSL Silver, offres Club SSL et ISP SSL)	25
4.3.3	Notification par l'AC de la délivrance du certificat au porteur	25
4.4	Acceptation du certificat	25
4.4.1	Démarche d'acceptation du certificat	25
4.4.2	Publication du certificat par l'AC	25
4.4.3	Notification par l'AC aux autres entités de la délivrance du certificat	25
4.5	Utilisation du certificat et de la paire de clés	26
4.5.1	Utilisation du certificat et de la clé privée SSL	26
4.5.2	Utilisation du certificat et de la clé publique par la partie utilisatrice	26
4.6	Renouvellement du certificat	26
4.6.1	Motifs de renouvellement du certificat	26
4.7	Renouvellement de la clé du certificat	26
4.8	Modification du certificat	26
4.9	Suspension et révocation du certificat	26
4.9.1	Motifs de révocation	27
4.9.2	Procédure de traitement d'une demande de révocation	27
4.9.3	Délai accordé pour formuler la demande de révocation	28
4.9.4	Délai de traitement par l'AC d'une demande de révocation	28
4.9.5	Exigences de vérification de la révocation pour les parties utilisatrices	28
4.9.6	Fréquence d'établissement des LCR	28
4.9.7	Délai maximum de publication d'une LCR	28
4.9.8	Disponibilité d'un service de vérification en ligne de la révocation et de l'état des certificats	29
4.9.9	Exigences de vérification en ligne des révocations	29
4.9.10	Autres moyens disponibles d'information sur les révocations	29
4.9.11	Exigences spécifiques en cas de compromission de la clé	29
4.9.12	Motifs de suspension	29
4.9.13	Origine d'une demande de suspension	29
4.9.14	Procédure de traitement d'une demande de suspension	29
4.9.15	Limites relatives à la période de suspension	29
4.10	Services de vérification de l'état des certificats	29
4.10.1	Caractéristiques opérationnelles	29
4.10.2	Disponibilité du service	29
4.10.3	Dispositifs optionnels	29
4.11	Expiration de l'abonnement	29
4.12	Séquestre et recouvrement de clé	30
5	CONTRÔLES D'INSTALLATION, D'EXPLOITATION ET DE GESTION	31
5.1	Mesures de sécurité physiques	31
5.1.1	Situation géographique et construction de sites	31
5.1.2	Accès physique	31
5.1.3	Alimentation électrique et climatisation	31
5.1.4	Expositions à l'eau	31
5.1.5	Prévention et protection contre les incendies	31
5.1.6	Stockage des supports	31
5.1.7	Traitement des déchets	31
5.1.8	Sauvegarde hors site	31
5.2	Mesures de sécurité en termes de procédures	32
5.2.1	Rôles de confiance	32
5.2.2	Nombre de personnes requises par tâche	32
5.2.3	Identification et authentification de chaque rôle	32
5.2.4	Rôles nécessitant la séparation des attributions	32

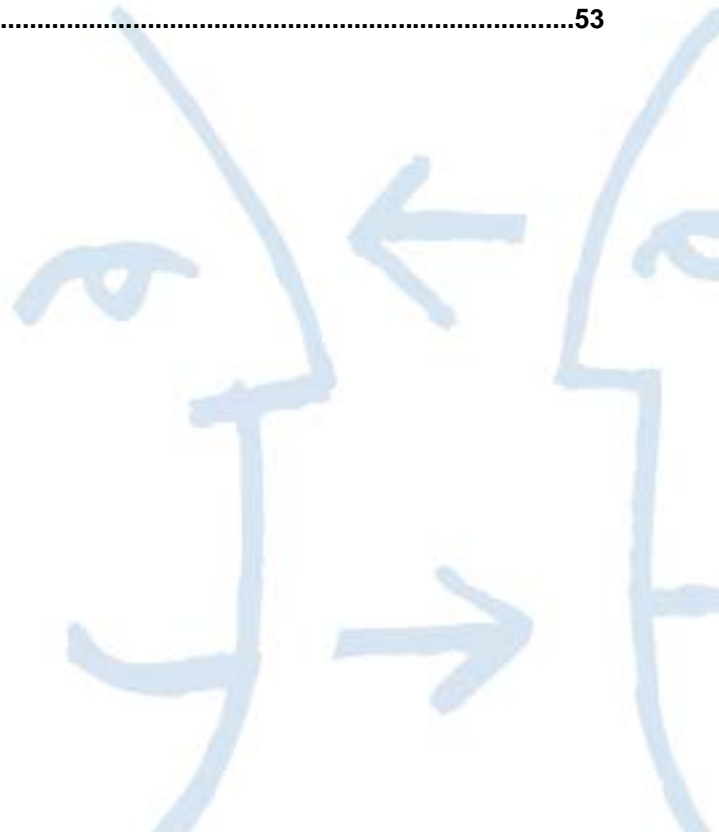


5.3	Mesures de sécurité en termes de personnel	33
5.3.1	Qualifications, expérience et habilitations requises	33
5.3.2	Procédures de vérification des antécédents	33
5.3.3	Exigences en matière de formation	33
5.3.4	Exigences et fréquence des formations	33
5.3.5	Séquence et fréquence de rotation des emplois	33
5.3.6	Sanctions en cas d'actions non autorisées	33
5.3.7	Exigences vis-à-vis des entrepreneurs indépendants	34
5.3.8	Documentation fournie au personnel	34
5.4	Procédures de journalisation	34
5.4.1	Types d'événements enregistrés	34
5.4.2	Fréquence de traitement des journaux d'audit	34
5.4.3	Période de conservation des journaux d'audit	34
5.4.4	Protection des journaux d'audit	34
5.4.5	Procédures de sauvegarde des journaux d'audit	35
5.4.6	Système de collecte des journaux d'audit (interne ou externe)	35
5.4.7	Notification au responsable d'un événement	35
5.4.8	Analyse des vulnérabilités	35
5.5	Archivage des enregistrements	35
5.5.1	Types d'enregistrements archivés	35
5.5.2	Période de conservation des archives	35
5.5.3	Protection des archives	35
5.5.4	Procédures de sauvegarde des archives	36
5.5.5	Exigences en matière d'horodatage des enregistrements	36
5.5.6	Système de collecte des archives (interne ou externe)	36
5.5.7	Procédures de récupération et de vérification des archives	36
5.6	Changement de clé d'une composante	36
5.6.1	Certificat SSL	36
5.6.2	Certificat de l'AC KEYNECTIS SSL	36
5.7	Compromission et reprise après sinistre	37
5.7.1	Procédures de gestion des incidents et des compromissions	37
5.7.2	En cas de compromission des ressources informatiques, logicielles et/ou des données	37
5.7.3	En cas de compromission de la clé privée d'une composante	37
5.7.4	Capacité de continuité des activités après un sinistre	37
5.8	Fin de vie d'une composante AC SSL	38
6	MESURES DE SÉCURITÉ TECHNIQUES	39
6.1	Génération et installation d'une paire de clés	39
6.1.1	Génération d'une paire de clés	39
6.1.2	Délivrance de la clé privée au client	39
6.1.3	Délivrance de la clé publique à l'émetteur de certificats	39
6.1.4	Délivrance de la clé publique d'une AC aux parties utilisatrices	39
6.1.5	Taille des clés des certificats SSL	39
6.1.6	Génération et contrôle de la qualité des paramètres de clé publique	39
6.1.7	Utilisation de la clé (selon le champ d'utilisation des clés du certificat X.509 v3)	39
6.2	Protection des clés privées et fonctionnement du module cryptographique	39
6.2.1	Contrôles et normes du module cryptographique	40
6.2.2	Contrôle des clés privées (m sur n) par plusieurs personnes	40
6.2.3	Séquestre des clés privées	40
6.2.4	Sauvegarde des clés privées	40
6.2.5	Archivage des clés privées	40
6.2.6	Transfert des clés privées vers ou à partir d'un module cryptographique	40
6.2.7	Stockage des clés privées sur un module cryptographique	40
6.2.8	Méthode d'activation des clés privées	40
6.2.9	Méthode de désactivation des clés privées	40
6.2.10	Méthode de destruction des clés privées	40
6.2.11	Certification du module cryptographique	41
6.3	Autres aspects de la gestion des paires de clés	41

6.3.1	Archivage des clés publiques	41
6.3.2	Périodes de validité des certificats et périodes d'utilisation des paires de clés.....	41
6.4	Données d'activation.....	41
6.4.1	Génération et installation des données d'activation	41
6.4.2	Protection des données d'activation	41
6.4.3	Autres aspects des données d'activation.....	41
6.5	Mesures de sécurité des systèmes informatiques	41
6.5.1	Exigences de sécurité technique spécifiques aux systèmes informatiques	41
6.5.2	Évaluation de la sécurité des systèmes informatiques	42
6.6	Mesures de sécurité techniques du cycle de vie	42
6.6.1	Mesures de sécurité liées au développement des systèmes	42
6.6.2	Mesures liées à la gestion de la sécurité.....	42
6.6.3	Mesures de sécurité liées au cycle de vie	42
6.7	Mesures de sécurité réseau	43
6.8	Horodatage.....	43
7	PROFILS DES CERTIFICATS, LCR ET OCSP	44
7.1	Profil des certificats	44
7.1.1	Extensions de certificats	44
7.1.2	Identifiants objet d'algorithme	44
7.1.3	Structure des noms.....	44
7.1.4	Identifiant d'objet de politique de certification	44
7.1.5	Utilisation d'extensions de contraintes sur les politiques.....	44
7.1.6	Règles de traitement de l'extension critique des politiques de certification.....	44
7.2	Profil des LCR.....	44
7.2.1	LCR et extensions des entrées des LCR.....	44
7.3	Profil OCSP	44
7.3.1	Numéro(s) de version	44
7.3.2	Extensions OCSP	45
8	AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS	46
8.1	Fréquence et circonstances des évaluations.....	46
8.2	Identité et compétences de l'auditeur	46
8.3	Relation entre l'auditeur et l'entité évaluée	46
8.4	Domaines abordés par l'évaluation.....	46
8.5	Mesures prises suite au constat de lacunes	46
8.6	Communications des résultats	46
9	AUTRES QUESTIONS JURIDIQUES ET COMMERCIALES	47
9.1	Tarifification	47
9.1.1	Frais de délivrance des certificats.....	47
9.1.2	Frais d'accès à un certificat	47
9.1.3	Frais de révocation ou d'accès aux informations d'état.....	47
9.1.4	Frais découlant d'autres services	47
9.1.5	Politique de remboursement.....	47
9.2	Responsabilité financière	48
9.2.1	Couverture d'assurance.....	48
9.2.2	Autres actifs	48
9.2.3	Couverture d'assurance ou de garantie pour les entités finales.....	48
9.3	Confidentialité des informations de l'entreprise.....	48
9.3.1	Étendue des informations confidentielles	48
9.3.2	Informations non confidentielles	48
9.3.3	Protection des informations confidentielles	48
9.4	Confidentialité des informations personnelles	49
9.4.1	Programme de confidentialité	49
9.4.2	Informations jugées confidentielles.....	49
9.4.3	Informations non jugées confidentielles.....	49
9.4.4	Protection des informations privées.....	49



9.4.5	Avis et autorisation d'utilisation des informations privées.....	49
9.4.6	Divulgarion conformément au processus judiciaire ou administratif.....	49
9.4.7	Autres circonstances de divulgations des informations.....	49
9.5	Droits de propriété intellectuelle	49
9.6	Déclarations et garanties.....	49
9.6.1	Déclarations et garanties de l'AC KEYNECTIS SSL	50
9.6.2	Déclarations et garanties du demandeur.....	50
9.6.3	Déclarations et garanties de l'AE.....	50
9.6.4	Déclarations et garanties du CT	50
9.6.5	Déclarations et garanties des autres composantes.....	50
9.7	Exonération de garanties.....	51
9.8	Limitations de responsabilité.....	51
9.9	Indemnisation	51
9.10	Durée et résiliation	51
9.10.1	Durée	51
9.10.2	Résiliation.....	51
9.10.3	Effet de la résiliation et survie	52
9.11	Avis individuels et communications avec les composantes.....	52
9.12	Amendements.....	52
9.12.1	Procédure d'amendement.....	52
9.12.2	Période et mécanisme de notification.....	52
9.12.3	Circonstances dans lesquelles l'OID doit être modifié.....	52
9.13	Dispositions relatives à la résolution des conflits.....	52
9.14	Législation applicable	52
9.15	Conformité avec la législation applicable.....	52
9.16	Dispositions diverses	52
9.16.1	Accord complet	52
9.16.2	Cession	53
9.16.3	Divisibilité	53
9.16.4	Renonciation de droits	53
9.16.5	Catastrophe naturelle.....	53
9.17	Autres dispositions	53



1 INTRODUCTION

1.1 Vue d'ensemble

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, 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, laquelle délivre des certificats SSL conformément à la présente Politique de Certification (PC).



Un certificat SSL est un certificat électronique autorisant des connexions SSL entre les serveurs et les sites Web.

Un certificat SSL autorise les opérations suivantes :

- Mise en place d'une liaison entre une page Web hébergée sur un serveur et son propriétaire ;
- Authentification du serveur hébergeant la page Web ;
- Initialisation d'une communication sécurisée entre le serveur hébergeant la page Web et les individus ou les serveurs qui se connectent à cette page Web.

L'AC KEYNECTIS SSL propose à ses clients plusieurs offres distinctes de délivrance de certificats SSL :

K.SSL Gold et Silver :

Les offres K.SSL Gold et Silver sont fournies aux clients sur une base unitaire. Chaque fois qu'un client achète un certificat SSL, il ou elle doit remplir un formulaire auprès de l'Autorité d'Enregistrement SSL de KEYNECTIS. Les vérifications des certificats K.SSL Gold effectuées par l'Autorité d'Enregistrement SSL de KEYNECTIS sont plus strictes que celles effectuées pour les certificats K.SSL Silver (voir la section 4 ci-dessous).

Club SSL :

L'offre Club SSL permet aux clients d'acquérir des certificats SSL sur une base quantitative (Club SSL 10 pour 10 certificats SSL, Club SSL 100 pour 100 certificats SSL), certificats qui doivent être utilisés dans l'année. Les clients sont de petites et moyennes organisations qui ont besoin d'un certain nombre de certificats pour répondre aux exigences de leurs noms de domaine. L'identité de l'organisation et de ses représentants est vérifiée par l'Autorité d'Enregistrement SSL de KEYNECTIS avant l'ouverture de l'interface d'enregistrement Club SSL.

ISP SSL :



Les certificats K.SSL Gold sont achetés sur une base quantitative par les Fournisseurs d'Accès à Internet (ISP, Internet Service Provider en anglais) au nom de leurs clients hébergés. L'identité du FAI et de ses représentants est vérifiée par l'Autorité d'Enregistrement SSL de KEYNECTIS avant l'ouverture de l'interface d'enregistrement ISP SSL.

Certificats K.SSL de test :

Ces certificats SSL sont uniquement délivrés à des fins de test par une AC auto signée. KEYNECTIS, en tant qu'émetteur de certificats K.SSL de test, ne sera pas tenu pour responsable de leur utilisation. Ces certificats sont automatiquement transmis par KEYNECTIS au demandeur lors de sa demande en ligne, sans aucune vérification. La validité du certificat K.SSL de test est de 14 jours. L'AC KEYNECTIS SSL ne gère pas l'état du certificat K.SSL de test.

La fiabilité et la qualité d'un certificat SSL dépendent des exigences de l'AC SSL et des moyens définis dans sa Politique de Certification (PC) et dans sa Déclaration des Pratiques de Certification (DPC). La présente PC définit les objectifs et exigences en matière de pratiques (commerciales, juridiques et techniques) employées par l'ACR et l'AC KEYNECTIS SSL pour fournir des services de certification comprenant l'enregistrement, la délivrance, le renouvellement et la révocation des certificats SSL.

Les certificats ACR et AC KEYNECTIS SSL sont compatibles avec tous les navigateurs Internet et programmes de messagerie afin de simplifier la reconnaissance des certificats SSL émis par KEYNECTIS.

La présente PC est conforme au document RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework, rédigé par l'Internet Engineering Task Force (IETF – Détachement d'ingénierie d'Internet).

1.2 Nom du document et identification

Cette PC est la propriété de KEYNECTIS.

Les identifiants d'objets (OID) suivants ont été attribués à cette PC :

1.3.6.1.4.1.22234.2.5.3.1 pour les certificats SSL signés par l'AC KEYNECTIS SSL

1.3.6.4.1.22234.2.7.1.1 pour les certificats de test signés par l'AC TEST de KEYNECTIS

Cet OID est présent dans les certificats SSL délivrés par l'AC KEYNECTIS SSL.

1.3 Composantes de l'ICP

Pour héberger et faire fonctionner ses AC, KEYNECTIS a déployé une Infrastructure à Clés Publiques (ICP) au sein de son centre de production. Cette ICP est constituée des éléments suivants pour la prise en charge des services de l'AC KEYNECTIS SSL :

- Génération de la clé d'AC SSL : l'AC KEYNECTIS SSL génère ses paires de clés dans le centre de production de KEYNECTIS au cours d'une opération spécifique appelée « Cérémonie de Clés »
- Génération de certificats d'AC SSL : l'AC KEYNECTIS SSL demande à l'ACR KEYNECTIS un certificat conformément à la PC d'ACR ;
- Authentification de l'AE : l'AC KEYNECTIS SSL authentifie l'Autorité d'Enregistrement chargée d'enregistrer les demandes de certificats SSL.
- Génération des bi-clés pour les certificats SSL : le demandeur de certificat SSL génère sa ou ses propres paires de clés cryptographiques.
- Authentification du demandeur de certificat SSL : avant de délivrer des certificats SSL, l'AE recueille et vérifie les informations incluses dans les demandes.
- Génération de certificats SSL : si la demande est correcte et validée par l'AE, alors l'AC KEYNECTIS SSL génère un certificat SSL.
- Révocation des certificats SSL : lorsque le lien entre le demandeur de certificat et la clé publique définie dans le certificat délivré par l'AC KEYNECTIS SSL est considéré comme n'étant plus valide, le certificat SSL doit être révoqué soit par le demandeur, soit par l'AE soit par l'AC KEYNECTIS SSL.

- **Renouvellement des certificats SSL** : le renouvellement d'un certificat SSL implique la génération d'un nouveau certificat avec des informations (clé, nom...) identiques à celles du certificat précédent ou différentes. Le demandeur est responsable de la demande de renouvellement.
- **Services de Publication** : les certificats ACR et AC SSL ainsi que les Listes des Certificats Révoqués (LCR) associées sont publiés par KEYNECTIS sur ses sites Web. De même, les certificats ACR et AC SSL sont distribués aux principaux éditeurs de navigateurs Internet (Microsoft, fondation Mozilla...) par KEYNECTIS afin d'être publiés dans leurs logiciels.

La PC suivante définit les exigences de sécurité pour tous les services décrits. La DPC correspondante donnera plus de détails sur les pratiques prises en charge par chaque entité.

1.3.1 Autorité de Certification SSL de KEYNECTIS (AC KEYNECTIS SSL)

L'AC KEYNECTIS SSL est une AC qui génère des certificats SSL pour des clients (entreprises, agences gouvernementales...) et qui les autorise à configurer des communications sécurisées. L'AC KEYNECTIS SSL utilise le service de publication de KEYNECTIS pour publier ses certificats et les LCR générés.

L'AC KEYNECTIS SSL opère sa propre infrastructure à clés publiques conformément à sa PC/DPC.

1.3.2 Autorité d'Enregistrement (AE)

Une AE est une entité qui procède à l'authentification et à la vérification des demandeurs de certificats SSL. Un demandeur SSL formule une ou plusieurs demandes de certificat conformément à la présente PC. Une AE est authentifiée et reconnue par l'AC KEYNECTIS SSL.

Le service clients de l'AC KEYNECTIS SSL agit en tant qu'AE pour les offres K.SSL Gold et Silver.

Les administrateurs SSL agissent en tant qu'AE pour les offres Club SSL et ISP SSL (voir la section 1.3.6 ci-dessous).

1.3.3 Service de Publication

Un service de publication est une entité qui met à disposition sur Internet les informations concernant les certificats, les LCR et les AC.

1.3.4 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 SSL. Le nom de domaine est géré par un administrateur de nom de domaine. Une phase « d'authentification » permet à l'AC KEYNECTIS SSL d'établir que :

- L'organisation mentionnée dans la CSR (Requête de Signature du Certificat) existe et est légalement autorisée à utiliser de façon exclusive son nom ;
- Le nom de domaine inclus dans la demande appartient à cette organisation, qui est par conséquent autorisée à l'utiliser ;
- un administrateur SSL (voir la section 1.3.6 ci-dessous) agit en tant que demandeur du certificat SSL, ou un contact technique (voir la section 1.3.5 ci-dessous) agit en tant que demandeur du certificat SSL, et est autorisé à soumettre la demande, car il appartient à l'organisation propriétaire du nom de domaine, ou à une entreprise nommée par le propriétaire du nom de domaine et qui l'autorise à effectuer la demande.

1.3.5 Contact Technique (CT)

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

- Agir en tant que demandeur SSL pour la génération de la CSR ;
- Remplir les formulaires de demande de certificat SSL ;
- Retirer les certificats SSL.

1.3.6 Administrateur SSL



Un administrateur SSL est une personne autorisée à agir comme demandeur de certificat SSL par le client SSL pour les offres Club SSL et ISP SSL. L'administrateur SSL peut aussi révoquer des certificats au nom du client Club SSL.

- Dans le cas de l'offre Club SSL, l'administrateur SSL agit en tant que demandeur pour une organisation qui détient les noms de domaine.
- Dans le cas de l'offre ISP SSL, l'administrateur SSL agit en tant que demandeur pour le compte du FAI qui agit lui-même au nom de l'organisation qui possède les noms de domaine et qu'il héberge.

Pour l'offre Club SSL, l'administrateur SSL agit en tant qu'AE et gère les services d'enregistrement des demandes pour l'AC KEYNECTIS SSL. Dans cette perspective, l'administrateur SSL est tenu de :

- Remplir les demandes de certificat SSL pour le compte du client Club SSL ;
- Transmettre les codes de retrait du certificat SSL au contact technique approprié ;
- Révoquer le certificat SSL ;
- Authentifier le certificat auprès de l'AC KEYNECTIS SSL si nécessaire.

Pour l'offre ISP SSL, l'administrateur SSL agit en tant qu'AE et gère les services d'enregistrement des demandes pour l'AC KEYNECTIS SSL. Dans cette perspective, l'administrateur SSL est tenu de :

- Remplir les demandes de certificat SSL de l'organisation hébergée et propriétaire du nom de domaine ;
- Transmettre les codes de retrait du certificat SSL au contact technique approprié ;
- Révoquer le certificat SSL ;
- Authentifier le certificat auprès de l'AC KEYNECTIS SSL si nécessaire.

Lorsque l'utilisateur d'une AC SSL de KEYNECTIS possède son propre service d'AE, un contrat doit être conclu au préalable avec l'AC KEYNECTIS SSL. Le contrat stipule que :

- L'organisation est chargée des authentifications internes et de toutes les vérifications nécessaires à la validation des certificats SSL conformément à la présente PC ;
- L'organisation, en tant qu'AE, met en œuvre les sections des PC/DPC applicables ;
- L'organisation doit informer l'AC KEYNECTIS SSL, dans un délai raisonnable, de toute modification relative à l'identité et à la position de ses représentants par rapport à l'AC KEYNECTIS SSL ;
- Son administrateur SSL utilise des certificats électroniques d'organisation pour s'authentifier sur le site Web de l'AC KEYNECTIS SSL lors de la demande et de la validation du certificat SSL ;
- Ses services d'AE peuvent faire l'objet d'audits de la part de l'AC KEYNECTIS SSL.

1.3.7 Autres composantes

1.3.7.1 Autorité Administrative de KEYNECTIS (AAK)

L'AAK établit la présente PC mise en œuvre par l'AC KEYNECTIS SSL conformément à la PC de l'ACR. L'AAK définit le processus de conformité de l'AC KEYNECTIS SSL.

KEYNECTIS dispose de son propre cadre de vérification pour auditer l'AC KEYNECTIS SSL.

Toutes les décisions de l'AAK relatives à la mise en œuvre d'une AC sous l'AC racine de KEYNECTIS, comme l'établissement d'une AC KEYNECTIS SSL, sont approuvées par le conseil des actionnaires de KEYNECTIS.

1.3.7.2 Autorité de Certification Racine (ACR)

L'ACR est régie par KEYNECTIS. L'ACR signe et révoque les certificats AC KEYNECTIS SSL. Dans la présente PC, lorsque le terme ACR est utilisé sans précision supplémentaire (AE, SP...), il englobe tous les aspects de l'ICP déployée traitant des questions juridiques et commerciales de l'ACR. L'ACR prend en charge les services de l'ICP. L'ACR utilise son AE pour authentifier et identifier l'AC KEYNECTIS SSL pour les demandes de certificat, de révocation et de renouvellement. L'ACR utilise le Service de Publication pour publier les certificats et les ARL (Listes d'Autorités Révoquées) générées. L'ARL gère ses services conformément à la PC ACR et la DPC correspondante. L'ACR ne peut fonctionner sans l'approbation de l'AAK.

1.3.7.3 Tierces parties de confiance

La tierce partie de confiance est un individu ou une organisation qui s'appuie sur des certificats et/ou des signatures électroniques. Dans ce contexte, l'utilisateur Internet qui fait confiance aux certificats SSL, fait confiance au chemin de certification de l'AC KEYNECTIS SSL, pour ses relations commerciales (contrôle d'accès sur des réseaux privés, transmission de données sur serveur sécurisé...) avec l'organisation dont le nom de domaine est inclus dans le certificat SSL.

1.4 Utilisation du certificat

1.4.1 Utilisation appropriée du certificat

1.4.1.1 Certificat AC SSL

Le certificat d'AC KEYNECTIS SSL est utilisé par un client Internet pour vérifier l'identité d'un certificat SSL délivré, conformément à la PC de l'AC KEYNECTIS SSL.

1.4.1.2 Certificat SSL

Un certificat SSL délivré par l'AC KEYNECTIS SSL est utilisé par les tierces parties de confiance (Internet ou intranet) pour vérifier l'identité d'un nom de domaine sur un serveur donné.

1.4.2 Utilisation interdite du certificat

Toute autre demande que la délivrance de certificats SSL, c'est-à-dire l'utilisation d'un profil et/ou d'une fonction différente, n'est pas couverte par la présente PC.

Les certificats d'AC ne doivent pas être utilisés pour d'autres fonctions que les fonctions de l'AC.

L'AC KEYNECTIS SSL ne sera pas tenue pour responsable de toute autre utilisation que celle définie dans la présente PC.

Les certificats doivent être utilisés exclusivement dans le cadre de la loi applicable, uniquement dans la mesure permise par les lois relatives à l'importation et l'exportation.

1.5 Administration de la politique

1.5.1 Organisation régissant le document

L'AAK est responsable de tous les aspects de cette PC.

1.5.2 Contact

Le Responsable de la Politique de Certification est chargé de l'AAK.

KEYNECTIS

Contact : Responsable Qualité et Sécurité

30, rue du Château des Rentiers, 75647 Paris Cedex 13 - FRANCE

Téléphone : +33 (0)1 53 94 22 00

Fax : +33 (0)1 53 94 22 01

info@keynectis.com

1.5.3 Responsable de la conformité de la PC

L'AC KEYNECTIS SSL est chargée de la mise en œuvre et de la révision de la présente PC. L'AC KEYNECTIS SSL est chargée de la définition, du fonctionnement et de la révision de la DPC associée.

L'AAK contrôle la conformité des PC/DPC de l'AC KEYNECTIS SSL afin d'autoriser la signature de l'AC KEYNECTIS SSL par l'ACR, comme décrit dans la PC de l'ACR.

1.5.4 Procédure d'Approbation de la DPC

Le terme DPC est défini dans le document RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework comme « une déclaration des pratiques qu'une AC utilise pour l'émission des certificats ». Il s'agit d'une description complète de la mise en œuvre des offres de service et des procédures de la gestion du cycle de vie des certificats. Cette description est plus détaillée que la PC correspondante décrite ci-dessus.

La DPC de l'AC KEYNECTIS SSL n'est pas publiée. L'AC KEYNECTIS SSL soumet ses DPC à l'approbation de l'AAK.

L'AAK révisé et valide les résultats du contrôle effectué par les experts AAK suite à l'analyse de conformité de la DPC de l'AC KEYNECTIS SSL.

Les amendements à la DPC sont publiés en tant que nouvelle version. La nouvelle version de la DPC remplace automatiquement l'ancienne et devient effective dès la validation du résultat du contrôle de conformité par l'AAK.

Cette nouvelle version est toujours conforme à la présente PC afin de permettre à l'AC KEYNECTIS SSL de se reporter à cette PC pour délivrer les certificats SSL.

1.6 Définitions et acronymes

1.6.1 Définition

AAK : représente l'organisme faisant autorité au sein de KEYNECTIS. Voir la section 1.3.7 pour plus d'informations.

AC KEYNECTIS SSL : KEYNECTIS a établi sa propre AC, signée par l'ACR de KEYNECTIS pour délivrer des certificats SSL à des clients conformément à la présente PC. La conformité de l'AC KEYNECTIS SSL à la présente PC doit avoir été établie par l'AAK pour que celle-ci puisse délivrer des certificats SSL.

Accord d'utilisation de la LCR : accord définissant les termes et conditions selon lesquels une LCR ou les informations qu'elle comprend peuvent être utilisées.

Administrateur SSL : voir la section 1.3.6 ci-dessus.

Audit : révision et examen indépendants des activités et enregistrements du système pour évaluer le caractère adéquat et l'efficacité des contrôles du système, afin de garantir la conformité avec les politiques et procédures opérationnelles établies, ainsi que de recommander les changements nécessaires à apporter aux contrôles, politiques ou procédures. [Sécurité ISO/IEC POSIX]

Autorité de Certification (AC) : autorité chargée de créer et de distribuer les certificats. L'autorité de certification peut également créer les clés des utilisateurs [ISO/IEC 9594-8 ; ITU-T X.509].

Autorité de Certification Racine (ACR) : voir la section 1.3.7.2 ci-dessus

Autorité d'Enregistrement (AE) : entité chargée de l'identification et de l'authentification des demandeurs de certificats électroniques, mais qui ne signe ni ne délivre de certificats (un certain nombre de tâches est délégué à une AE pour le compte d'une AC).

Centre de production de KEYNECTIS : l'objectif initial du Centre de production de KEYNECTIS et des ressources gérées par KEYNECTIS est la génération de certificats électroniques. Ces services comprennent :

- la gestion du cycle de vie des autorités de certification ;
- la gestion du cycle de vie des certificats électroniques ;



- la personnalisation des cartes à puce et autres clés USB ;
- la production de jetons d'horodatage ;
- la publication des éléments associés à la gestion de ces cycles de vie ;
- la vérification des signatures électroniques ou de la validité des certificats.

Certificat auto-signé : certificat pour une AC signé à l'aide de sa clé privée.

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

Certificat : clé publique d'un client, ainsi que d'autres informations, rendues infalsifiables par chiffrement avec la clé privée de l'Autorité de Certification qui l'a émise [ISO/IEC 9594-8 ; ITU-T X.509]. Dans ce contexte, les certificats pour le client sont des certificats utilisés par un serveur pour établir une connexion SSL avec un nom de domaine certifié. Le certificat contient le Nom de Domaine pleinement Qualifié (FQDN, Fully Qualified Domain Name) qui appartient au client.

Chemin de certification : chaîne de plusieurs certificats nécessaires pour valider un certificat contenant la clé publique requise. Une chaîne de certificats est composée d'un certificat d'ACR, d'un certificat d'AC et des certificats SSL signés par l'AC KEYNECTIS SSL.

Clé privée : composante d'une paire de clés asymétriques d'une entité qui doit être utilisée uniquement par cette entité. [ISO/IEC 9798-1]

Clé publique : composante d'une paire de clés asymétriques d'une entité qui peut être rendue publique. [ISO/IEC 9798-1]

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.

Compromission : violation réelle ou supposée d'une politique de sécurité, dans laquelle la divulgation non autorisée, ou la perte de contrôle, d'informations sensibles pourrait avoir eu lieu. En matière de clés privées, une compromission correspond à la perte, au vol, à la divulgation, à la modification, à l'utilisation non autorisée ou à toute autre compromission de la sécurité de ladite clé privée.

Confidentialité : propriété selon laquelle les informations ne sont pas accessibles ou divulguées à des personnes, entités ou processus non autorisés [ISO/IEC 13335-1:2004]

Contact technique : voir la section 1.3.5 ci-dessus.

Déclaration des Pratiques de Certification (DPC) : énoncé des pratiques employées par KEYNECTIS (agissant en tant qu'Autorité de Certification) pour approuver ou rejeter les demandes de certification (délivrance, gestion, renouvellement et révocation des certificats). [RFC 2527]

Demande de certificat : message transmis par l'AE à l'AC afin d'obtenir un certificat SSL délivré par l'AC KEYNECTIS SSL.

Demandeur : personne autorisée par le propriétaire du nom de domaine ou le client SSL à effectuer les Demandes de certificat SSL

Disponibilité : propriété d'être accessible et utilisable à la demande par une entité autorisée [ISO/IEC 13335-1:2004]

Données d'activation secrètes de l'AC : ensemble de données d'activation (code PIN, partie de clé...) m (entier fixe déterminé dans la DPC) qui sont utilisées pour activer la clé privée de l'AC. La DPC définit le nombre de données d'activation n ($n > 1$) nécessaires pour activer la clé privée de l'AC. Une seule donnée d'activation ne peut pas être utilisée pour activer la paire de clés privées de l'AC. Toutes les données d'activation secrètes m sont fournies aux personnes autorisées m qui doivent protéger leur confidentialité et intégrité.

Données d'activation : valeurs de données, autres que les clés, requises pour faire fonctionner les modules cryptographiques et devant être protégées (par exemple, un PIN, un mot de passe, ou un échange de clés manuel).

Fonction de hachage : fonction qui, à partir d'une chaîne de caractères de taille variable, élabore une chaîne de caractères de longueur fixe, satisfaisant aux deux propriétés suivantes :

- il est mathématiquement impossible de trouver pour une entrée donnée une deuxième entrée qui mène à la même sortie. [ISO/IEC 10118-1]
- il est mathématiquement impossible de trouver pour une sortie donnée une entrée qui mène à cette sortie ;

Infrastructure à Clés Publiques (ICP) : infrastructure nécessaire à la génération, la distribution, la gestion et l'archivage des clés, certificats et listes des certificats révoqués et le service d'annuaire sur lequel les certificats et LCR doivent être publiés. [2e DIS ISO/IEC 11770-3 (08/1997)]

Intégrité : fait référence à l'aspect approprié des informations, de l'auteur des informations, et du fonctionnement du système qui les traite.

Interopérabilité : implique que l'équipement et les procédures utilisés par deux entités ou plus sont compatibles, et qu'il est donc possible d'entreprendre des activités communes ou liées.

Jeton : matériel utilisé pour transporter les clés vers une entité et capable de protéger ces clés pendant leur utilisation. [ISO/IEC 9798-1 (2e édition) : 1997]

Key Ceremony : procédure par laquelle une paire de clés de l'AC ou de l'AE est générée à l'aide d'un module cryptographique et où la clé publique est certifiée.

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

Modules cryptographiques : ensemble de composants logiciels et matériels utilisés pour activer une clé cryptographique privée permettant des opérations cryptographiques (signature, chiffrement, authentification, génération de clés...). Lorsqu'un module cryptographique stocke une clé privée, il a besoin de données d'activation pour activer la clé privée qui y est stockée. Pour une AC, un module cryptographique est un module matériel de sécurité HSM (Hardware Security Module) évalué (norme FIPS ou EAL) qui est utilisé pour stocker et activer la clé privée de l'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 légalement autorisé à utiliser ce nom de domaine.

Période de validité du certificat : période pendant laquelle l'AC garantit qu'elle conservera des informations concernant l'état du certificat. [RFC 3280]

PKCS #10 : norme de cryptographie à clé publique (PKCS) #10, développée par RSA Security Inc., définissant une structure pour une Requête de Signature de Certificat.

Plan de reprise après sinistre : plan défini par l'AC pour récupérer l'ensemble ou une partie de ses services, endommagés à la suite d'un sinistre, dans un délai défini dans la PC/DCP.

Point de distribution de la LCR : entrée d'annuaire ou autre source de distribution des LCR ; une LCR diffusée via un point de distribution de LCR peut contenir des entrées de révocation uniquement pour un sous-ensemble de l'ensemble complet des certificats délivrés par une AC ou pour plusieurs AC. [ISO/IEC 9594-8 ; ITU-T X.509]



Politique de Certification (PC) : ensemble de règles, identifié par un nom, relatives à l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications ayant des besoins de sécurité communs. [ISO/IEC 9594-8 ; ITU-T X.509]. Le présent document est la PC de l'AC KEYNECTIS SSL.

Politique de sécurité : ensemble de règles défini par l'autorité de sécurité régissant l'utilisation et la prestation des services de sécurité et installations [ISO/IEC 9594-8 ; ITU-T X.509]. Dans ce contexte, la politique de sécurité sera définie par KEYNECTIS qui héberge et gère l'AC KEYNECTIS SSL.

Processus de contrôle de conformité : processus établi par l'AAK pour déterminer si le fonctionnement de l'AC SSL de KEYNECTIS est conforme ou non à la présente PC. À cette fin, l'AAK utilise la présente PC, la DPC de l'AC KEYNECTIS SSL et toute autre procédure applicable en tant qu'ensemble de référence des exigences de KEYNECTIS pour la délivrance de certificats SSL. L'AAK doit vérifier la politique et les pratiques et définir s'il existe une différence par rapport aux exigences de sécurité définies.

Protocole de vérification en ligne de l'état du certificat (OCSP, Online Certificate Status Protocol) : protocole qui fournit aux Parties utilisatrices des informations en temps réel sur l'état du certificat.

Qualificateur de politique : informations relatives à la politique accompagnant un identificateur de politique de certification dans un certificat X.509. [RFC 2527]

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

Secure Socket Layer (SSL) : méthode standard de protection des communications Web développée par Netscape Communications Corporation. Le protocole de sécurité SSL assure le chiffrement de données, l'authentification du serveur, l'intégrité des messages et l'authentification facultative du client pour une connexion TCP/IP.

Service de Publication (SP) : service qui diffuse des informations aux clients, puis aux parties utilisatrices.

Services d'horodatage : service qui constitue une déclaration signée électroniquement (un reçu électronique) prouvant qu'un document particulier ou un ensemble de données existait à un moment donné. Service d'horodatage : service offrant une association de confiance entre une donnée et un instant particulier dans le temps, dans le but d'établir une preuve fiable indiquant une date à laquelle la donnée existait.

Tierce partie de confiance : voir la section 1.3.7.3 ci-dessus.

1.6.2 Acronymes

ANSI : The American National Standards Institute ;

LAR : Liste des Autorités de certification Révoquées ;

AC KEYNECTIS SSL : Autorité de certification qui fournit les certificats SSL au client ;

PC : Politique de Certification ;

DPC : Déclaration des Pratiques de Certification ;

LCR : Liste des Certificats Révoqués ;

ND : Nom Distinctif ;

DNS : Domain Name Server ;

EAL : Evaluation Assurance Level (conformément aux Critères Communs);

FIPS : Federal Information Processing Standards des États-Unis ;

HTTP : HyperText Transport Protocol ;

IP : Internet Protocol ;

ISO : International Organization for Standardization ;

AAK : Autorité Administrative de KEYNECTIS ;

CCK : Centre de confiance de KEYNECTIS ;

LDAP : Lightweight Directory Access Protocol ;

OCSP : Online Certificate Status Protocol ;

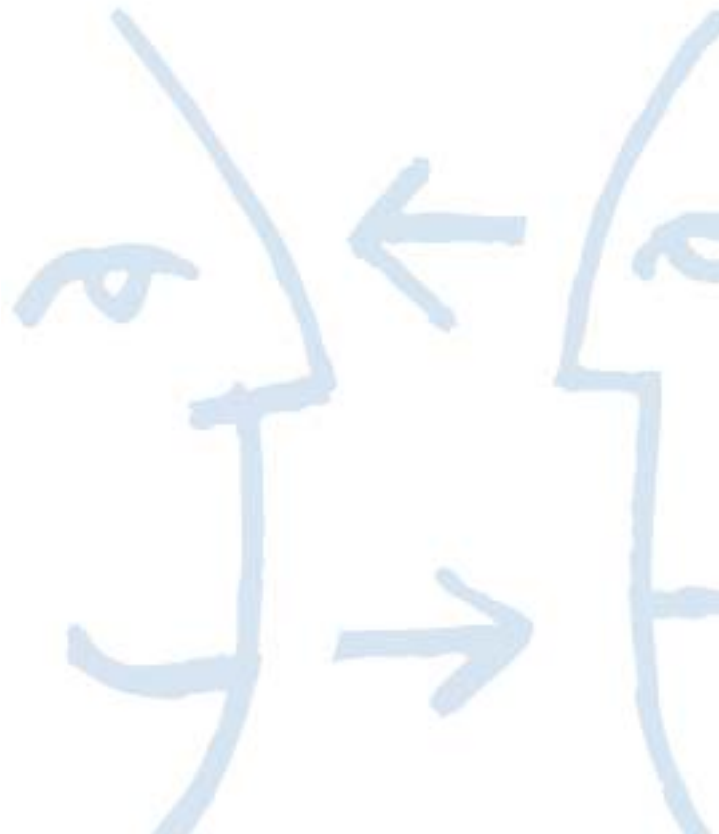
PDN : Propriétaire du Nom de Domaine

OID : Identifiant d'objet ;

PIN : Personal Identification Number ;



PKCS : Public-Key Cryptography Standard ;
PKI : Public Key Infrastructure (ICP, Infrastructure à Clé Publique) ;
SP : Service de Publication ;
AE : Autorité d'Enregistrement ;
ACR : Autorité de Certification Racine ;
RFC : Request for comment ;
RSA : Rivest, Shamir, Adleman (système cryptographique à clé publique) ;
SHA : Secure Hash Algorithm (norme US) ;
SSL : Secure Socket Layer ;
URL : Uniform Resource Locator.



2 RESPONSABILITÉS EN TERMES D'ANNUAIRE ET DE PUBLICATION

2.1 Annuaire

L'AC KEYNECTIS SSL s'appuie sur l'annuaire du Service de Publication pour que les informations définies ci-dessous soient accessibles aux clients et aux tierces parties de confiance.

2.2 Publication des informations de certification

L'AC KEYNECTIS SSL garantit que les termes et conditions de la PC et des certificats sont accessibles aux clients via le SP de KEYNECTIS. Sont publiées les informations suivantes :

- Certificat de l'AC racine
- PC de l'ACR de KEYNECTIS
- Certificat de l'AC KEYNECTIS SSL
- PC de l'AC KEYNECTIS SSL
- Documentation relative à la demande, au retrait et à la demande de révocation de certificats
- État des certificats SSL

Ces informations sont publiées sur le site Web de KEYNECTIS à l'adresse suivante :

- www.keynectis.com/PC pour les politiques de certification
- www.keynectis.com/PC pour les certificats de l'AC
- <http://trustcenter-crl.certificat2.com/keynectis/crl/class2keynectisca.crl> pour l'état des certificats SSL (LCR)
- <http://trustcenter-crl.certificat2.com/keynectis/crl/testkeynectisca.crl> pour l'état des certificats de test SSL (LCR)
- <http://ssl.keynectis.com> pour la documentation relative à la demande, au retrait et à la demande de révocation de certificats.

L'AC KEYNECTIS SSL ne publie pas d'informations relatives aux certificats K.SSL de test.

2.3 Date et fréquence de publication

La PC et les documents relatifs aux certificats sont publiés 2 (deux) jours au plus tard après l'approbation de la version applicable.

Les certificats de l'AC sont publiés 24 (vingt-quatre) heures au plus tard après leur génération.

L'état des certificats SSL peut être consulté via les LCR.

Les LCR sont publiées au minimum toutes les 24 (vingt-quatre) heures.

2.4 Contrôles d'accès à l'annuaire

Le service de publication de KEYNECTIS garantit que les informations sont accessibles et que leur intégrité et authenticité sont protégées de toute modification non autorisée.

Les informations sont accessibles publiquement et internationalement sur Internet. Toutes les informations de l'annuaire de l'ICP qui ne sont pas destinées à être modifiées ou divulguées au public sont protégées.

3 IDENTIFICATION ET AUTHENTIFICATION

L'AC KEYNECTIS SSL ne procède à aucune identification ni authentification en relation avec toute demande de certificats K.SSL de test.

3.1 Dénomination

3.1.1 Conventions de noms

Le certificat SSL a un Nom Distinctif (ND) X.501 clairement visible et unique dans le champ du nom du porteur du certificat, conformément à la norme RFC3280. Le nom distinctif est composé des éléments suivants :

Organisation	L'entité pour laquelle le certificat SSL est émis. Le terme « Organisation » est un nom générique englobant les différents types d'entités demandant des certificats SSL (entreprise, administration, communauté locale, association...). Le nom de l'Organisation doit être le même que celui associé au numéro de SIREN ou de DUNS indiqué dans la demande.
Common Name	Le Common Name est le Nom de Domaine Pleinement Qualifié (FQDN, Fully Qualified Domain Name). C'est le nom du site Web à sécuriser. Le Common Name est donc tout ce qui suit http://, extension incluse. Le Common Name ne peut jamais être une adresse IP.
Localité	Le client doit indiquer dans ce champ le nom de la ville où le siège de son organisation se situe.
État	Le client indique l'état, la région ou le département où se situe son organisation.
Pays	Le client doit entrer le code pays à 2 lettres (norme ISO).

Si le client modifie les informations contenues dans le Common Name, il doit en informer l'AE. La nouvelle identité est alors vérifiée conformément à la section 3.2.2 ci-dessous. Si la vérification est validée, le client peut de nouveau être certifié par l'AC KEYNECTIS SSL.

3.1.2 Utilisation de noms explicites

Les certificats émis conformément à cette PC sont explicites uniquement si les noms qui apparaissent dans les certificats peuvent être compris et utilisés par les parties utilisatrices. Les noms utilisés dans les certificats doivent identifier le domaine de façon explicite.

3.1.3 Anonymat ou pseudonyme des clients

L'identité utilisée pour les certificats SSL ne peut être un pseudonyme ou un nom anonyme.

3.1.4 Règles d'interprétation des différentes formes de noms

Les règles d'interprétation des formes de noms sont intégrées dans le profil du certificat applicable comme défini dans les sections 3.1.1 et 7.1.

3.1.5 Unicité des noms

Les identités de certificat SSL (voir la section 3.1.1 ci-dessus) sont uniques pour les certificats SSL générés par l'AC KEYNECTIS SSL. L'AE garantit l'unicité à travers son processus d'enregistrement (voir la section 3.2.2).

Un contact technique demandant un certificat SSL auprès de l'AC KEYNECTIS SSL manifeste son droit d'utiliser un nom particulier pour son identité. Lorsqu'il y a conflit sur le nom d'un certificat, l'AC KEYNECTIS SSL est chargée de résoudre le problème lié au nom.

3.1.6 Reconnaissance, authentification et rôle des marques de commerce

Un client n'est pas assuré que son nom contienne une marque de commerce. L'AC KEYNECTIS SSL n'est pas obligée de rechercher les marques de commerce ou de résoudre les conflits s'y rapportant.

3.2 Validation initiale de l'identité

3.2.1 Méthode permettant de prouver la possession d'une clé privée

Le contact technique procède à la génération des paires de clés et de la CSR pour le compte du client de l'AC KEYNECTIS SSL.

L'AC KEYNECTIS SSL garantit que le client demandant un certificat SSL détient la clé privée correspondant à la clé publique à certifier, en utilisant la CSR sur le format PKCS #10.

3.2.2 Vérification de l'identité d'une organisation

L'authentification d'une organisation repose sur la vérification des informations fournies par cette dernière. Ces informations comprennent le nom et l'adresse de l'organisation ainsi que les documents ou les références de l'existence de celle-ci, et le nom de domaine qu'elle détient.

L'entité 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 SSL 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.

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, 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.

3.2.3 Vérification de l'identité d'une personne

Les identités individuelles sont vérifiées à l'aide de moyens et procédures adaptés au rôle attribué à l'individu.

L'identité du contact technique est vérifiée pendant l'étape de validation de la demande de certificat SSL, via un processus de questions/réponses réalisé par l'AE.

L'identité d'un administrateur Club SSL ou ISP SSL est vérifiée par l'AC KEYNECTIS SSL pendant le processus d'enregistrement du certificat électronique qu'il demande à des fins d'administration SSL. La vérification de l'identité d'un administrateur SSL repose sur la présentation d'un document national d'identité qui comprend une photo de la personne et qui permet de le reconnaître.

3.2.4 Informations non vérifiées

Les informations qui ne sont pas vérifiées ne doivent pas être incluses dans les certificats.

3.2.5 Validation de l'Autorité

Une autorité est vérifiée pendant le processus d'enregistrement et de validation des demandes de certificats SSL auxquelles elle procède. L'authentification d'un demandeur repose sur une requête envoyée au propriétaire du nom de domaine, indiquant s'il ou elle autorise ou non le demandeur à agir en tant que demandeur pour le nom de domaine pour lequel il ou elle a fait une demande de certificat SSL.

L'autorisation d'un contact technique est vérifiée pendant le retrait du certificat SSL par la présentation d'un code de retrait qui a été transmis à l'AE pendant le processus d'enregistrement. Le code de retrait est uniquement connu du demandeur qui le transmet au contact technique avant le retrait du certificat SSL.

L'autorisation d'un administrateur Club SSL ou ISP SSL repose également sur un document fourni par l'organisation qui donne la preuve que l'administrateur Club SSL ou ISP SSL est nommé par l'organisation à ce poste.

Si l'authentification de l'organisation ou de l'individu est nécessaire, les principes expliqués dans les sections 3.2.2 et 3.2.3 s'appliquent.

3.2.6 Critères d'interfonctionnement

Un client qui obtient un certificat SSL est assuré d'être certifié par l'AC KEYNECTIS SSL qui a adhéré aux exigences suivantes :

- être conforme à une DPC, à la suite d'un contrôle effectué par l'AAK par rapport à la présente PC ;
- gérer une ICP qui a réussi un contrôle de conformité conformément à la section 8 de cette PC ;
- délivrer des certificats SSL et des informations sur l'état des certificats conformes aux profils décrits dans la PC et accessibles aux parties utilisatrices.

3.3 Identification et authentification des demandes de renouvellement de clés

3.3.1 Identification et authentification pour le renouvellement des clés après leur expiration

Une demande de renouvellement de clés peut-être présentée par le client au nom duquel les clés ont été émises. Le client s'identifie à l'aide du processus de confirmation de l'identité initial, comme décrit dans la section 3.1.6 ci-dessus.

3.3.2 Identification et authentification pour le renouvellement des clés après leur révocation

Lorsqu'un certificat SSL a été révoqué à un autre moment que pendant son renouvellement ou sa mise à jour, le client SSL suit le processus d'enregistrement initial, comme décrit dans la section 3.1.6 ci-dessus, afin d'obtenir un nouveau certificat SSL.

Si le certificat SSL a été révoqué pour des raisons de compromission de la clé, alors le client génère une nouvelle paire de clés avant de procéder à une demande de certificat SSL.

3.4 Identification et authentification des demandes de révocation

Les demandes de révocation sont authentifiées par l'AE.

La procédure d'authentification exige le même niveau de confiance que celui défini pour l'enregistrement initial (voir les sections 3.2.2 et 3.2.3 ci-dessus) afin de s'assurer que le client certifié a effectivement demandé la révocation.

4 EXIGENCES OPÉRATIONNELLES LIÉES AU CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

4.1.1.1 Offres K.SSL Gold et K.SSL Silver

Seuls les demandeurs (propriétaire du nom de domaine ou contact technique) peuvent remplir des demandes de certificat SSL.

4.1.1.2 Offres Club SSL et ISP SSL

Seuls les administrateurs Club SSL ou ISP SSL autorisés peuvent remplir des demandes de certificat SSL.

4.1.1.3 Certificats de test K.SSL

Toute personne souhaitant se familiariser avec les certificats SSL peut demander un certificat K.SSL de test auprès de l'AC KEYNECTIS SSL de test.

4.1.2 Processus et responsabilités d'inscription

4.1.2.1 Offres K.SSL Gold et K.SSL Silver

Le processus d'inscription à l'offre K.SSL Gold comprend deux étapes.

Tout d'abord, le demandeur remplit un formulaire sur le site Web de l'AC KEYNECTIS SSL (ssl.keynectis.com). Le formulaire comprend les éléments suivants :

- les informations d'identification du contact technique, c'est-à-dire le nom complet (nom de famille et prénoms), l'adresse e-mail, la fonction, l'adresse postale complète, les numéros de téléphone (numéros standard et directs) ;
- les données d'identification de l'organisation pour laquelle un certificat SSL est requis, c'est-à-dire le nom complet et le statut juridique de la personne morale associée et toute information d'enregistrement pertinente existante (par exemple, enregistrement de l'entreprise) ;
- la clé publique au format PKCS#10 ;
- l'identification du nom de domaine ;
- la durée du certificat SSL (un ou deux ans) ;
- les informations secrètes permettant à l'autorité d'enregistrement de l'AC KEYNECTIS SSL de procéder à la vérification de la demande ;
- le code secret pour le retrait du certificat SSL par le contact technique.

La connexion est protégée (confidentialité et intégrité des informations) à l'aide du protocole https.

Dans un deuxième temps, le demandeur transmet un bon de commande à l'AC KEYNECTIS SSL en y joignant le paiement à l'adresse suivante :

KEYNECTIS,
Service Clients SSL
30, rue du Château des Rentiers,
75647 Paris Cedex 13 - FRANCE

Avant d'établir une relation contractuelle avec un client, l'AC KEYNECTIS SSL informe ce dernier des termes et conditions d'utilisation des certificats SSL. Ces termes sont inclus dans la présente PC.

4.1.2.2 Offres Club SSL et ISP SSL

L'organisation détenant un compte Club SSL ou ISP SSL bénéficie d'une interface dédiée à l'enregistrement. Pour se connecter à cette interface, l'administrateur Club SSL ou ISP SSL (nommé par le client pour agir en son nom) s'authentifie à l'aide d'un certificat électronique individuel.

Il accède alors à un formulaire détaillé sur l'interface d'enregistrement qui permet :

- la génération d'une CSR ;

- la saisie de quelques informations administratives (nom de famille, prénom et adresse e-mail) sur le demandeur.

Les demandes de certificats SSL nécessitent la conclusion d'un accord contractuel avec l'AC KEYNECTIS SSL avant que l'interface d'enregistrement ne soit accessible.

4.1.2.3 Certificats K.SSL de test

Le processus d'inscription aux certificats K.SSL de test consiste à remplir un formulaire de demande sur le site Web de l'AC KEYNECTIS SSL, à l'adresse <http://ssl.keynectis.com>.

Le formulaire comprend les éléments suivants :

- les informations d'identification du contact technique, c'est-à-dire le nom complet (nom de famille et prénoms), l'adresse e-mail, la fonction, l'adresse postale complète, les numéros de téléphone (numéros standard et directs) ;
- les données d'identification de l'organisation pour laquelle un certificat SSL est requis, c'est-à-dire le nom complet et le statut juridique de la personne morale associée et toute information d'enregistrement pertinente existante (par exemple, enregistrement de l'entreprise) ;
- la clé publique au format PKCS#10 ;
- l'identification du nom de domaine ;
- le code secret pour le retrait du certificat SSL par le contact technique.

4.2 Traitement d'une demande de certificat

4.2.1 Fonctions d'identification et d'authentification

4.2.1.1 Offres K.SSL Gold et K.SSL Silver

Le processus d'identification et d'authentification débute après réception par l'AC KEYNECTIS SSL du bon de commande et du paiement correspondant.

Le service client de l'AC KEYNECTIS SSL effectue les opérations suivantes :

- vérification de l'envoi et de l'exactitude du bon de commande et du paiement ;
- authentification de l'organisation du client conformément à la section 3.2.2 ci-dessus ;
- vérification que l'organisation du client détient le nom de domaine ;
- vérification que le contact technique agit au nom du client SSL conformément à la section 3.2.3 ci-dessus ;
- vérification que l'organisation du propriétaire du nom de domaine accepte la demande de certificat du client SSL pour les noms de domaine qu'il ou elle détient.

Le service clients SSL enregistre toutes les informations utilisées pour vérifier l'identité du client et, le cas échéant, les attributs spécifiques, notamment le numéro de référence de la documentation utilisée aux fins de vérification ainsi que toute limite concernant sa validité.

4.2.1.2 Offre Club SSL

Le processus d'identification et d'authentification débute après réception par l'AC KEYNECTIS SSL du bon de commande ou de la proposition commerciale.

Le service clients de l'AC KEYNECTIS SSL effectue les opérations suivantes :

Pour la délivrance d'un certificat électronique d'administrateur SSL :

- vérification de l'identité du ou des administrateurs du Club SSL désignés ;
- vérification que l'administrateur a clairement été désigné par l'organisation du propriétaire du nom de domaine pour agir en son nom.

Pour l'ouverture de l'interface d'enregistrement du Club SSL :

- authentification de l'organisation du client du Club SSL conformément à la section 3.2.2 ci-dessus ;
- vérification que l'organisation du client du Club SSL détient le nom de domaine déclaré ;
- vérification que l'administrateur SSL nommé agit au nom du client du Club SSL conformément à la section 3.2.3 ci-dessus.

Le service client SSL enregistre toutes les informations utilisées pour vérifier l'identité du client et, le cas échéant, les attributs spécifiques, notamment le numéro de référence de la documentation utilisée aux fins de vérification ainsi que toute limite concernant sa validité.

4.2.1.3 Offre ISP SSL

L'identification et l'authentification des clients ISP SSL sont effectuées au moment de l'établissement de la relation contractuelle avec l'AC KEYNECTIS SSL, avant que les clients ISP SSL ne procèdent à l'enregistrement des certificats SSL.

Le service client de l'AC KEYNECTIS SSL effectue les opérations suivantes :

- authentification de l'organisation du client ISP SSL conformément à la section 3.2.2 ci-dessus ;
- vérification que l'organisation du client ISP SSL est autorisée à demander des certificats SSL pour le nom de domaine qu'elle déclare ;
- vérification que l'administrateur SSL nommé agit au nom du client ISP SSL conformément à la section 3.2.3 ci-dessus ;
- délivrance d'un certificat électronique d'administrateur SSL à l'administrateur ISP SSL.

Le service clients SSL enregistre toutes les informations utilisées pour vérifier l'identité du client et, le cas échéant, les attributs spécifiques, notamment le numéro de référence de la documentation utilisée aux fins de vérification ainsi que toute limite concernant sa validité.

4.2.1.4 Certificats K.SSL de test

Aucune opération n'est effectuée dans le cadre d'une demande de certificat K.SSL de test.

4.2.2 Approbation ou rejet des demandes de certificat

4.2.2.1 Offres K.SSL Gold et K.SSL Silver

L'approbation ou le rejet des demandes de certificats K.SSL Gold sont traités par le service clients SSL, d'après les résultats des actions décrites dans la section 4.2.1 ci-dessus.

Lorsque toutes les opérations d'authentification et de vérification s'avèrent probantes, les demandes de certificats SSL sont approuvées et transmises à l'AC KEYNECTIS SSL pour leur génération.

Pendant ce temps, un e-mail est envoyé au contact technique l'informant qu'il ou elle peut retirer le certificat.

4.2.2.2 Offres Club SSL et ISP SSL

L'approbation de la demande de certificat est effectuée par l'administrateur Club SSL ou ISP SSL.

Une fois que l'administrateur Club SSL ou ISP SSL a approuvé une demande de certificat SSL, celle-ci est transmise à l'AC KEYNECTIS SSL pour sa génération.

Pendant ce temps, un e-mail est envoyé au contact technique l'informant qu'il ou elle peut retirer le certificat.

4.2.2.3 Certificats K.SSL de test

Les demandes de certificats K.SSL de test sont automatiquement approuvées à condition que le formulaire de demande soit correctement rempli.

4.2.3 Durée de traitement des demandes de certificats

4.2.3.1 Offres K.SSL Gold et K.SSL Silver

La durée du processus d'identification et d'authentification d'une demande de certificat SSL s'élève à 48 heures ouvrables sous réserve que le service clients ait été en mesure d'effectuer toutes les validations et vérifications requises.

4.2.3.2 Offres Club SSL et ISP SSL

Les administrateurs SSL sont chargés d'approuver les demandes de certificats pour le compte de l'organisation qui les a nommés. La durée de traitement de la demande de certificat est définie par le client lui-même puisqu'il est chargé de sa validation.

4.2.3.3 Certificats K.SSL de test

Lorsqu'un formulaire de demande K.SSL de test est approuvé (automatiquement), le demandeur reçoit un e-mail lui indiquant l'URL à laquelle il peut retirer le certificat K.SSL de test.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance d'un certificat K.SSL Silver

Aucune disposition.

4.3.2 Actions de l'AC concernant la délivrance d'un certificat (offres K.SSL Gold et K.SSL Silver, offres Club SSL et ISP SSL)

Avant de générer le certificat SSL, l'AC KEYNECTIS SSL vérifie que tous les champs et extensions du certificat à signer sont correctement renseignés.

Le contact technique qui procède au téléchargement du certificat doit s'authentifier à l'aide du code de retrait qui a été transmis à l'AC KEYNECTIS SSL lors du processus de demande.

Toutes les opérations sont protégées afin de garantir l'intégrité, la confidentialité (lorsque nécessaire) et l'origine des données transmises ainsi que pour sécuriser le lien entre l'opération et les composantes.

4.3.2.1 Certificats K.SSL de test

Le contact technique qui procède au téléchargement du certificat doit s'authentifier à l'aide du code de retrait qui a été transmis à l'AC KEYNECTIS SSL lors du processus de demande.

Toutes les opérations sont protégées afin de garantir l'intégrité, la confidentialité (lorsque nécessaire) et l'origine des données transmises ainsi que pour sécuriser le lien entre l'opération et les composantes.

4.3.3 Notification par l'AC de la délivrance du certificat au porteur

Lorsqu'un certificat SSL a été généré et récupéré, le contact technique et l'administrateur SSL (dans le cadre d'une offre Club SSL ou ISP SSL) sont informés du retrait du certificat SSL.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Dès que le CT a téléchargé son certificat SSL, l'AC KEYNECTIS SSL considère le certificat comme accepté.

4.4.2 Publication du certificat par l'AC

Les certificats SSL délivrés par l'AC KEYNECTIS SSL ne sont pas publiés par le service de publication de KEYNECTIS.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

Le demandeur, le contact technique (CT) et l'administrateur SSL (dans le cadre d'une offre Club SSL ou ISP 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 KEYNECTIS SSL est également informé de la délivrance d'un certificat SSL.

4.5 Utilisation du certificat et de la paire de clés

4.5.1 Utilisation du certificat et de la clé privée SSL

La paire de clés SSL est utilisée pour définir le protocole SSL.

4.5.2 Utilisation du certificat et de la clé publique par la partie utilisatrice

Les parties utilisatrices utilisent le chemin de certification de confiance et les clés publiques associées aux fins limitées par les extensions de certificat SSL (telles que l'utilisation de la clé, l'utilisation étendue de la clé, les politiques de certification, etc.) ainsi que pour authentifier l'identité commune de confiance des « services SSL » conformément à la présente PC.

4.6 Renouvellement du certificat

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

4.6.1 Motifs de renouvellement du certificat

Un certificat peut être renouvelé si la période de validité de sa clé publique n'a pas expiré, si la clé privée associée n'a pas été révoquée ou compromise et si le nom de domaine et les attributs n'ont pas été modifiés. Par ailleurs, la période de validité du certificat ne doit pas excéder la durée de vie restante de la clé privée, comme spécifié dans la section 5.6. L'AE doit vérifier l'existence et la validité du certificat à renouveler et s'assurer que les informations utilisées pour vérifier l'identité et les attributs de l'objet sont toujours valables en suivant la même procédure définie dans les sections 3.2.2 et 3.2.3 ou en suivant des procédures qui présentent le même niveau de confiance.

Cette opération est possible uniquement si la clé réutilisée dans le certificat est toujours conforme aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé.

L'AC KEYNECTIS SSL envoie des messages d'avertissement au client pour l'informer de l'expiration prochaine de son certificat SSL (voir la section 4.1.1).

4.7 Renouvellement de la clé du certificat

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

Plus une clé est utilisée, plus elle est susceptible d'être perdue ou découverte, c'est pourquoi elle doit être changée régulièrement. Le renouvellement de la clé d'un certificat implique la création d'un nouveau certificat conformément à la présente PC. L'AC KEYNECTIS SSL envoie un message d'avertissement au CT pour l'informer de l'expiration prochaine de son certificat SSL.

4.8 Modification du certificat

Cette section décrit 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.

Tout changement de l'identité contenue dans le certificat SSL peut être à l'origine de modifications du certificat.

4.9 Suspension et révocation du certificat

Les services de révocation et de suspension des certificats ne sont pas proposés pour les certificats de test K.SSL.

4.9.1 Motifs de révocation

Un certificat SSL est révoqué lorsque le lien entre ce dernier et la clé publique associée n'est plus valable. Ce lien peut disparaître pour les raisons suivantes :

- la cessation d'activité de l'AC KEYNECTIS SSL ;
- la violation par l'AC KEYNECTIS SSL des dispositions de son accord avec KEYNECTIS ;
- le changement de la longueur de la clé émanant d'un organisme de réglementation ou d'un institut de normes international ;
- la révocation de l'AC KEYNECTIS SSL ;
- la modification de l'enregistrement du nom de domaine ou du nom de l'organisation impliquant que le demandeur n'est plus autorisé à utiliser le nom de domaine ;
- les informations du nom de domaine n'ont pas été correctement renseignées ;
- la perte ou la compromission du certificat SSL correspondant à la clé privée ;
- l'utilisation par le demandeur d'un nom de domaine incorrect dans sa demande initiale ;
- l'organisation du propriétaire du nom de domaine souhaite révoquer le certificat SSL.

Dans les cas ci-dessus, le certificat associé devra être révoqué et placé dans la prochaine LCR.

4.9.1.1 Origine d'une demande de révocation (offres K.SSL Gold et K.SSL Silver, Offres Club SSL et ISP SSL)

Le CT et l'administrateur SSL (dans le cadre d'une offre Club SSL Gold ou ISP SSL) sont autorisés à effectuer des demandes de révocation pour les raisons suivantes :

- la modification de l'enregistrement du nom de domaine ou du nom de l'organisation impliquant que le demandeur n'est plus autorisé à utiliser le nom de domaine ;
- les informations du nom de domaine n'ont pas été correctement renseignées ;
- la perte ou la compromission du certificat SSL correspondant à la clé privée ;
- l'utilisation par le demandeur d'un nom de domaine incorrect dans sa demande initiale ;
- l'organisation du propriétaire du nom de domaine souhaite révoquer le certificat SSL.

L'AC KEYNECTIS SSL est autorisée à effectuer des demandes de révocation pour les raisons suivantes :

- la cessation d'activité de l'AC KEYNECTIS SSL ;
- la violation par l'AC KEYNECTIS SSL des dispositions de son accord avec KEYNECTIS ;
- la révocation de l'AC KEYNECTIS SSL.

4.9.2 Procédure de traitement d'une demande de révocation

4.9.2.1 Offres K.SSL Gold et K.SSL Silver

Le CT transmet un formulaire de demande de révocation au service client SSL comprenant au minimum les éléments suivants :

- ses données d'identification personnelle ;
- les informations secrètes qui ont été précédemment utilisées pour vérifier l'identité du CT au cours du processus d'enregistrement.

La demande de révocation est transmise en ligne à support_ssl@keynectis.com, ou par télécopie au numéro du service client SSL +33(0)1 53 94 22 98.

Le service clients SSL authentifie et autorise les demandes de révocation. En cas d'authentification réussie, le service client SSL transmet la demande de révocation à l'AC KEYNECTIS SSL qui authentifie le service clients SSL et révoque le certificat SSL (à l'aide de la clé privée de l'AC).

Toutes les opérations sont protégées afin de garantir l'intégrité, la confidentialité (lorsque nécessaire) et l'origine des données transmises, ainsi que pour sécuriser le lien entre l'opération et les composantes.

Une fois le certificat SSL révoqué, l'AC KEYNECTIS SSL informe le CT du changement d'état du certificat SSL. Il ne peut alors plus être de nouveau certifié.

4.9.2.2 Offres Club SSL et ISP SSL

Le CT ou l'administrateur SSL transmet un formulaire de demande de révocation à l'AC KEYNECTIS SSL comprenant au minimum les éléments suivants :

- ses données d'identification personnelle ;
- les informations secrètes qui ont été précédemment utilisées pour vérifier l'identité du CT au cours du processus d'enregistrement.

La demande de révocation est transmise en ligne à support_ssl@keynectis.com, ou par télécopie au numéro du service client SSL +33(0)1 53 94 22 98.

Le service clients SSL authentifie et autorise les demandes de révocation. En cas d'authentification réussie, le service client SSL transmet la demande de révocation à l'AC KEYNECTIS SSL qui authentifie le service client SSL et révoque le certificat SSL (à l'aide de la clé privée de l'AC).

Toutes les opérations sont protégées afin de garantir l'intégrité, la confidentialité (lorsque nécessaire) et l'origine des données transmises, ainsi que pour sécuriser le lien entre l'opération et les composants.

Une fois le certificat SSL révoqué, l'AC KEYNECTIS SSL informe le CT et l'administrateur SSL du changement d'état du certificat SSL. Il ne peut alors plus être de nouveau certifié.

4.9.3 Délai accordé pour formuler la demande de révocation

Aucun délai n'est accordé pour la formulation de la demande de révocation. Les parties concernées doivent formuler la demande de révocation auprès de l'AE dès qu'elles en ont identifié le besoin.

4.9.4 Délai de traitement par l'AC d'une demande de révocation

Les services de gestion en ligne des révocations sont disponibles en permanence.

Le service clients SSL qui s'occupe des demandes de révocation est ouvert de 9 h 00 à 18 h 00 du lundi au vendredi, sauf les jours fériés. En cas de défaillance du système, du service ou pour tout autre motif hors de son contrôle, KEYNECTIS déploie tous les efforts possibles pour garantir que le service de l'AC KEYNECTIS SSL ne reste pas indisponible plus longtemps que la période maximale indiquée dans la Déclaration des Pratiques de Certification. L'AC KEYNECTIS SSL traitera une demande de révocation dès que possible après réception de la demande en question, de préférence immédiatement.

4.9.5 Exigences de vérification de la révocation pour les parties utilisatrices

L'utilisation de certificats révoqués pourrait avoir des conséquences catastrophiques sur certaines applications d'un client Internet agissant en tant que partie utilisatrice. La fréquence d'obtention de nouvelles données de révocation doit être déterminée par la partie utilisatrice. S'il est temporairement impossible d'obtenir des informations de révocation, la partie utilisatrice rejette alors l'utilisation du certificat, ou prend la décision avertie d'accepter le risque, la responsabilité et les conséquences découlant de l'utilisation d'un certificat, en d'autres termes d'un chemin de certification fourni conformément à la présente PC, dont l'authenticité ne peut être garantie selon les normes de ladite PC. Une telle utilisation peut parfois s'avérer nécessaire pour répondre à des exigences opérationnelles urgentes.

4.9.6 Fréquence d'établissement des LCR

Les LCR sont publiées toutes les 24 heures. Elles sont disponibles en permanence grâce au SP de KEYNECTIS, même s'il n'y a pas de changements ou de mises à jour à effectuer afin de garantir l'actualité des informations. L'AC KEYNECTIS SSL garantit que les LCR obsolètes sont retirées de l'annuaire au moment de la publication d'une nouvelle LCR. En cas de défaillance du système, du service ou pour tout autre motif hors de son contrôle, l'AC KEYNECTIS SSL déploie tous les efforts possibles pour garantir que ces informations ne restent pas indisponibles plus longtemps que la période maximale indiquée dans la Déclaration des Pratiques de Certification.

4.9.7 Délai maximum de publication d'une LCR

Le délai maximum entre le moment où un certificat SSL est révoqué par l'AC KEYNECTIS SSL et le moment où les informations de révocation correspondantes sont accessibles aux parties utilisatrices ne dépasse pas 24 heures.

4.9.8 Disponibilité d'un service de vérification en ligne de la révocation et de l'état des certificats

Aucune disposition.

4.9.9 Exigences de vérification en ligne des révocations

Aucune disposition.

4.9.10 Autres moyens disponibles d'information sur les révocations

Aucune disposition.

4.9.11 Exigences spécifiques en cas de compromission de la clé

Il n'existe pas d'exigences spécifiques autres que celles spécifiées dans la section 4.9.3.

4.9.12 Motifs de suspension

Non applicable.

4.9.13 Origine d'une demande de suspension

Non applicable.

4.9.14 Procédure de traitement d'une demande de suspension

Non applicable.

4.9.15 Limites relatives à la période de suspension

Non applicable.

4.10 Services de vérification de l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'état des informations est accessible via le service de publication comme décrit dans la section 2.

4.10.2 Disponibilité du service

L'état des informations relatives aux certificats est disponible en permanence. En cas de défaillance du système, du service ou pour tout autre motif hors de son contrôle, l'AC KEYNECTIS SSL déploie tous les efforts possibles pour garantir que ce service d'informations ne reste pas indisponible pendant plus de 4 (quatre) heures.

4.10.3 Dispositifs optionnels

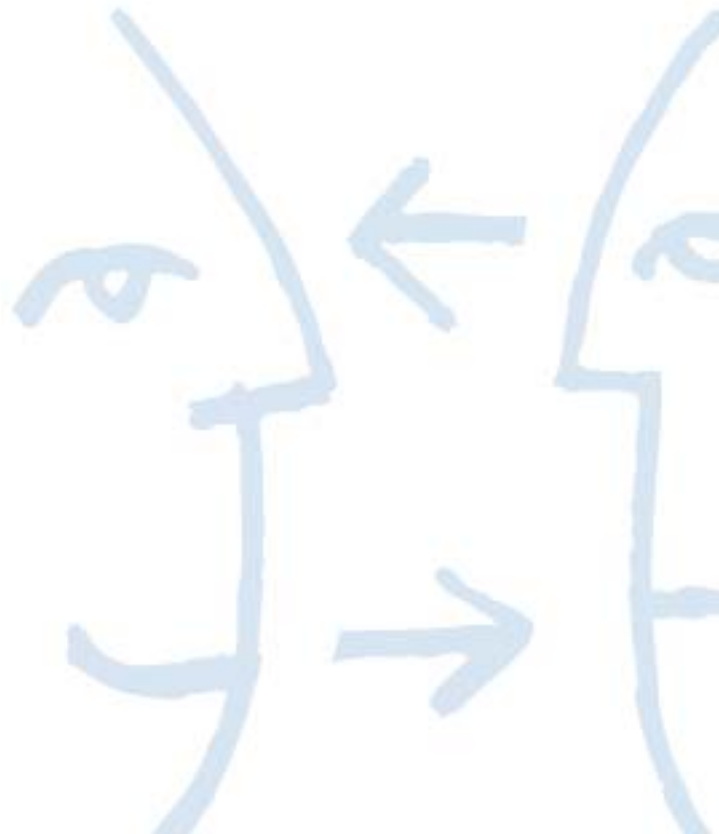
Aucune disposition.

4.11 Expiration de l'abonnement

Les certificats SSL qui ont expiré avant ou à la fin de l'abonnement sont révoqués. Lorsque le porteur met fin à sa relation avec l'AC KEYNECTIS SSL, toutes les garanties octroyées dans le cadre de la présente PC sur le certificat SSL ne sont plus applicables et tous les certificats sont révoqués.

4.12 Séquestre et recouvrement de clé

La clé d'un certificat SSL n'est en aucun cas séquestrée par une tierce partie ou toute autre entité.



5 CONTRÔLES D'INSTALLATION, D'EXPLOITATION ET DE GESTION

5.1 Mesures de sécurité physiques

La politique de sécurité logique et physique de l'AC KEYNECTIS SSL utilisée pour la gestion du cycle de vie des certificats SSL aborde le contrôle d'accès physique, la protection contre les catastrophes naturelles, les facteurs de sécurité incendie, la défaillance des services publics (électricité, télécommunications), l'effondrement de la structure, les fuites d'eau, la protection contre le vol et les entrées par effraction, et la reprise après sinistre, etc. Des mesures de sécurité sont mises en œuvre afin d'éviter toute perte, dommage ou compromission des actifs, toute interruption des activités de l'entreprise, ainsi que le vol des informations ou des installations de traitement des informations.

5.1.1 Situation géographique et construction de sites

Les installations de traitement des informations sensibles et essentielles de l'AC KEYNECTIS SSL sont hébergées dans des zones sécurisées équipées de barrières de sécurité et de contrôles à l'entrée appropriés. Elles sont physiquement protégées de tout accès non autorisé, dommage ou interférence. Les protections fournies sont proportionnelles aux risques identifiés dans le cadre de l'analyse des risques de l'AC KEYNECTIS SSL.

5.1.2 Accès physique

Les installations utilisées pour la gestion du cycle de vie des certificats SSL sont situées dans un environnement qui protège physiquement les services de toute tentative de compromission par le biais d'un accès non autorisé aux systèmes ou aux données. Les personnes non autorisées qui pénètrent dans cette zone physiquement sécurisée sont toujours accompagnées par un employé SSL autorisé de KEYNECTIS. Les protections physiques reposent sur la création de périmètres de sécurité clairement définis (barrières physiques) autour des systèmes hébergeant les opérations. Aucune partie des locaux de l'AC KEYNECTIS SSL n'est partagée avec d'autres organisations dans ce périmètre.

5.1.3 Alimentation électrique et climatisation

L'AC KEYNECTIS SSL garantit que les installations électriques et de climatisation sont suffisantes pour assurer le bon fonctionnement du système de l'AC KEYNECTIS SSL.

5.1.4 Expositions à l'eau

L'AC KEYNECTIS SSL garantit que son système est protégé contre les expositions à l'eau.

5.1.5 Prévention et protection contre les incendies

L'AC KEYNECTIS SSL garantit que son système est protégé par un système d'extinction incendie.

5.1.6 Stockage des supports

Les supports utilisés par l'AC KEYNECTIS SSL sont sécurisés de telle sorte qu'ils soient protégés contre tout dommage, vol et accès non autorisé. Les procédures de gestion des supports sont protégées contre l'obsolescence et la détérioration des supports pendant la période pendant laquelle les enregistrements doivent être conservés. Tous les supports sont sécurisés conformément aux exigences du programme de classification des informations et les supports contenant des informations sensibles sont mis au rebut de façon sécurisée lorsqu'ils ne sont plus requis.

5.1.7 Traitement des déchets

Tous les supports utilisés pour le stockage des informations telles que les clés, les données d'activation ou les fichiers de l'AC KEYNECTIS SSL sont rendus inutilisables ou détruits avant d'être mis au rebut.

5.1.8 Sauvegarde hors site

Des sauvegardes du système complet de l'AC KEYNECTIS SSL, suffisantes pour assurer une récupération à la suite d'une défaillance du système, sont effectuées régulièrement comme le stipule la DPC correspondante. Des copies de sauvegarde des informations et des logiciels essentiels à l'entreprise sont effectuées régulièrement. Des équipements de sauvegarde adéquats sont fournis afin de garantir la récupération de toutes les informations et logiciels essentiels à l'entreprise après un sinistre ou une défaillance du support de stockage. Les équipements de sauvegarde des systèmes individuels sont régulièrement testés afin de garantir qu'ils répondent aux exigences des plans de continuité des activités. Au moins une copie de sauvegarde complète est conservée hors site (dans un lieu séparé de l'équipement de l'AC KEYNECTIS SSL), dans un lieu où les mesures de sécurité physiques et procédurales sont proportionnelles à celles de l'AC KEYNECTIS SSL opérationnelle.

5.2 Mesures de sécurité en termes de procédures

5.2.1 Rôles de confiance

Les différents rôles de confiance impliqués dans le fonctionnement de l'AC KEYNECTIS SSL sont les suivants :

- Agent de sécurité : chargé d'administrer la mise en œuvre des pratiques de sécurité de manière globale.
- Administrateur : approuve la génération/révocation/suspension des certificats.
- Ingénieur système : autorisé à installer, configurer et assurer la maintenance des systèmes de l'AC KEYNECTIS SSL utilisés pour la gestion du cycle de vie des certificats SSL.
- Opérateur : chargé du fonctionnement quotidien des systèmes de l'AC KEYNECTIS SSL. Il est autorisé à effectuer les procédures de sauvegarde et de restauration des systèmes.
- Auditeur : autorisé à consulter les archives et les journaux d'audit des systèmes sécurisés de l'AC KEYNECTIS SSL.
- Détenteur des données d'activation de l'AC KEYNECTIS SSL : personne autorisée qui détient les données d'activation de l'AC KEYNECTIS SSL nécessaires au fonctionnement du module de sécurité matérielle.

5.2.2 Nombre de personnes requises par tâche

Le nombre de personnes nécessaires à la fourniture des services de l'AC KEYNECTIS SSL est détaillé dans la DPC. L'objectif est de garantir la fiabilité de tous les services de l'AC KEYNECTIS SSL (génération de clés, révocation, génération de certificats...) afin d'empêcher tout acte malveillant. Lorsqu'un contrôle multi utilisateurs est requis, l'une des composantes au moins doit être un administrateur. Toutes les composantes doivent occuper un rôle de confiance comme défini dans la section 5.2.1 ci-dessus.

5.2.3 Identification et authentification de chaque rôle

Avant de nommer une personne à un rôle de confiance, l'AC KEYNECTIS SSL procède à une vérification des antécédents.

Chaque personne occupant un rôle, comme décrit dans la présente PC, est identifiée et authentifiée de façon à garantir que la bonne personne occupe le bon rôle au sein de l'AC KEYNECTIS SSL. La DPC décrit les mécanismes utilisés pour identifier et authentifier les personnes nommées à des rôles de confiance.

5.2.4 Rôles nécessitant la séparation des attributions

La séparation des rôles peut être imposée par l'équipement de l'AC KEYNECTIS SSL ou par les procédures ou par ces deux moyens.

Des employés de l'AC KEYNECTIS SSL sont spécifiquement nommés aux cinq rôles définis dans la section 5.2.1 ci-dessus. Il est interdit d'occuper au même moment les rôles suivants :

- agent de sécurité et ingénieur système ou opérateur ;
- évaluateur et agent de sécurité ou opérateur ou administrateur ou ingénieur système ;
- ingénieur système et opérateur ou administrateur.

Il ne doit pas être attribué plus d'une identité à chaque individu.

5.3 Mesures de sécurité en termes de personnel

5.3.1 Qualifications, expérience et habilitations requises

L'AC KEYNECTIS SSL emploie suffisamment de personnes qui possèdent les connaissances, l'expérience et les qualifications nécessaires pour les services offerts, en fonction du poste. Le personnel de l'AC KEYNECTIS SSL répond aux exigences en termes de « connaissances, expérience et qualifications » à travers une formation officielle et une expérience réelle, ou une combinaison des deux. Les rôles et responsabilités de confiance, tels que spécifiés dans la DPC de l'AC KEYNECTIS SSL, sont détaillés dans les descriptions des postes et sont clairement identifiés. Les descriptions des postes du personnel de l'AC KEYNECTIS SSL (intérimaire et permanent) sont définies en s'appuyant sur la séparation des attributions et des droits d'accès minimaux, déterminant la sensibilité du poste selon les tâches et les niveaux d'accès, les antécédents, la formation et la prise de conscience de l'employé. Le personnel de l'AC KEYNECTIS SSL doit être officiellement nommé aux rôles de confiance par la direction supérieure chargée de la sécurité.

La description du poste comprend les compétences et l'expérience nécessaires. Des cadres sont employés, qui possèdent une certaine expérience ou ont suivi une formation dans la technologie des signatures électroniques et qui se sont familiarisés avec les procédures de sécurité pour le personnel avec des responsabilités de sécurité et une expérience en matière d'évaluation des risques et de sécurité des informations suffisante pour mener à bien des fonctions de direction.

5.3.2 Procédures de vérification des antécédents

Le personnel de l'AC KEYNECTIS SSL occupant des rôles de confiance doit être libre de tout conflit d'intérêts qui pourrait porter atteinte à l'impartialité des opérations de l'AC. L'AC KEYNECTIS SSL ne devra pas nommer à des rôles de confiance ou des postes de direction toute personne ayant été reconnue coupable d'un crime grave ou de toute autre infraction qui affecterait sa capacité à occuper le poste. Le personnel n'aura pas accès aux fonctions de confiance jusqu'à ce que les vérifications nécessaires aient été effectuées. L'AC KEYNECTIS SSL demande au candidat de présenter son casier judiciaire et rejette toute candidature en cas de refus. Toutes les personnes postulant à des rôles de confiance seront sélectionnées d'après des valeurs de loyauté, fiabilité et intégrité et feront l'objet d'une vérification de leurs antécédents.

5.3.3 Exigences en matière de formation

L'AC KEYNECTIS SSL garantit que tout le personnel participant au fonctionnement de l'AC KEYNECTIS SSL reçoit une formation complète dans les domaines suivants :

- Principes et mécanismes de sécurité de l'AC/AE
- Versions des logiciels utilisés sur le système ICP de l'AC
- Tâches qu'ils doivent effectuer
- Procédures de reprise après sinistre et de continuité des activités

Le personnel de l'AE et de l'AC KEYNECTIS SSL suivra une nouvelle formation en cas de changements apportés aux systèmes de l'AE ou de l'AC KEYNECTIS SSL. Un stage de perfectionnement devra être effectué si nécessaire et l'AC KEYNECTIS SSL devra réviser les exigences du stage de perfectionnement au moins une fois par an.

5.3.4 Exigences et fréquence des formations

Les personnes occupant des rôles de confiance doivent être informées des changements dans le fonctionnement de l'AE ou de l'AC KEYNECTIS SSL. Tout changement significatif du fonctionnement doit être accompagné d'un programme de formation et l'exécution d'un tel programme doit être documentée.

5.3.5 Séquence et fréquence de rotation des emplois

L'AC KEYNECTIS SSL garantit que tout changement de personnel n'affectera pas l'efficacité opérationnelle du service, ni la sécurité du système.

5.3.6 Sanctions en cas d'actions non autorisées

Des sanctions disciplinaires appropriées seront appliquées à l'encontre des employés violant la PC ou la DPC.

5.3.7 Exigences vis-à-vis des entrepreneurs indépendants

Les employés des entrepreneurs indépendants travaillant pour l'AC KEYNECTIS SSL devront respecter les mêmes exigences que celles applicables aux employés de KEYNECTIS.

5.3.8 Documentation fournie au personnel

L'AC KEYNECTIS SSL met à la disposition de ses employés la présente PC, la DPC correspondante et tous les règlements, politiques ou contrats pertinents. Les autres documents techniques, administratifs et opérationnels (manuel de l'administrateur, manuel d'utilisation, etc.) sont fournis pour permettre aux employés de confiance d'effectuer leur travail.

Des documents permettant d'identifier tous les employés ayant reçu une formation et le niveau de formation reçu sont conservés.

5.4 Procédures de journalisation

5.4.1 Types d'événements enregistrés

Des fichiers de journalisation sont générés pour tous les événements touchant à la sécurité et aux services des composantes de l'AC KEYNECTIS SSL. Lorsque possible, les journaux d'audit de la sécurité doivent être collectés automatiquement. Le cas contraire, un registre papier, ou tout autre mécanisme physique doit être utilisé. Tous les journaux d'audit de la sécurité, qu'ils soient électroniques ou non, doivent être conservés et rendus accessibles lors des contrôles de conformité.

L'AC KEYNECTIS SSL garantit que tous les événements liés au cycle de vie des certificats sont journalisés de façon à pouvoir imputer à une personne occupant un rôle de confiance une action requise pour les services de l'AC KEYNECTIS SSL. La DPC donne des informations sur les éléments journalisés. Chaque enregistrement comprend au minimum les éléments suivants (enregistrés manuellement ou automatiquement) :

- le type d'événement ;
- la date et l'heure de l'événement ;
- la réussite ou l'échec le cas échéant ;
- l'identité de l'entité et/ou de l'opérateur à l'origine de l'événement ;
- l'identité pour laquelle l'événement a eu lieu ;
- la cause de l'événement.

5.4.2 Fréquence de traitement des journaux d'audit

Les journaux d'audit sont examinés régulièrement pour détecter toute preuve d'activité malveillante et à la suite de toute opération importante.

5.4.3 Période de conservation des journaux d'audit

Les enregistrements concernant les certificats de l'AC SSL et de l'AC KEYNECTIS SSL sont conservés pendant une durée appropriée déterminée par la législation applicable. Ils sont susceptibles d'être requis au moins pendant aussi longtemps que l'exécution d'une transaction reposant sur un certificat valable peut être prouvée.

5.4.4 Protection des journaux d'audit

Les événements sont journalisés de façon à ne pas pouvoir être supprimés ou détruits (sauf en cas de transfert vers un support de stockage à long terme) pendant toute la durée pendant laquelle ils doivent être conservés.

Les événements sont journalisés de façon à garantir que seules les personnes ayant un accès de confiance autorisé peuvent effectuer des opérations relatives à leur rôle sans pour autant affecter l'intégrité, l'authenticité et la confidentialité des données.

Les événements sont protégés de façon à être toujours lisibles pendant toute la durée de leur conservation.

Les événements sont datés de façon à garantir, de la date de leur création jusqu'à la fin de la période d'archivage, la conservation du lien de confiance entre l'événement et le moment de sa réalisation.

5.4.5 Procédures de sauvegarde des journaux d'audit

Les journaux et résumés d'audit sont sauvegardés en lieux sûrs (coffres, etc.), sous le contrôle d'un rôle de confiance autorisé, séparés de la génération de leur source composante. Les sauvegardes des journaux d'audit sont protégées avec le même niveau de confiance que celui défini pour le journal original.

5.4.6 Système de collecte des journaux d'audit (interne ou externe)

Le système de collecte des journaux d'audit est interne aux composantes de l'AC KEYNECTIS SSL. Les processus d'audit sont exécutés au moment du démarrage du système et se terminent uniquement lors de son arrêt. Le système de collecte des journaux d'audit garantit l'intégrité et la disponibilité des données collectées. Si nécessaire, le système de collecte protège la confidentialité des données. En cas de problème pendant le processus du système de collecte des journaux d'audit, l'AC KEYNECTIS SSL détermine s'il est nécessaire de suspendre le fonctionnement de l'AC KEYNECTIS SSL jusqu'à la résolution du problème et d'en informer les composantes concernées.

5.4.7 Notification au responsable d'un événement

Aucune disposition.

5.4.8 Analyse des vulnérabilités

L'auditeur doit indiquer tous les événements importants dans un résumé des journaux d'audit. Cette analyse consiste à vérifier que le journal n'a pas été altéré, qu'il n'existe aucune discontinuité ou autre perte de données, puis à examiner brièvement toutes les entrées du journal, en s'attardant sur toute alerte ou irrégularité des journaux. Les actions prises à la suite de cette analyse sont documentées.

5.5 Archivage des enregistrements

5.5.1 Types d'enregistrements archivés

Les enregistrements archivés de l'AC et de l'AE doivent être suffisamment détaillés pour établir la validité d'une signature et du bon fonctionnement de l'ICP. Les données suivantes doivent être au minimum archivées :

- les enregistrements des événements de l'AC KEYNECTIS SSL ;
- la documentation d'audit de l'AC KEYNECTIS SSL ;
- le document de la PC de l'AC KEYNECTIS SSL ;
- les documents de la DPC de l'AC KEYNECTIS SSL ;
- tout accord contractuel entre un porteur du certificat SSL et l'AC KEYNECTIS SSL (offres Club SSL et ISP SSL) ;
- la configuration de l'équipement du système ;
- les certificats et LCR (ou toute autre information de révocation) ;
- d'autres données ou applications suffisantes pour vérifier le contenu des archives ;
- toutes les communications émanant ou provenant de l'AC KEYNECTIS SSL et des auditeurs de conformité.

5.5.2 Période de conservation des archives

La période minimum de conservation des données archivées est de 10 ans.

5.5.3 Protection des archives

Les archives sont créées de façon à ne pas pouvoir être supprimées ou détruites (sauf en cas de transfert vers un support de stockage à long terme) pendant toute la durée pendant laquelle elles doivent être conservées. La protection des archives garantit que seules les personnes ayant un accès de confiance autorisé peuvent effectuer des opérations relatives à leur rôle sans pour autant affecter l'intégrité, l'authenticité et la confidentialité des données. Si le support original n'est pas en mesure de conserver les données pour la période requise, un

mécanisme visant à transférer régulièrement les données archivées vers un nouveau support sera défini par le site d'archivage.

5.5.4 Procédures de sauvegarde des archives

Aucune disposition.

5.5.5 Exigences en matière d'horodatage des enregistrements

Si un service d'horodatage est utilisé pour dater les enregistrements, il doit respecter les exigences définies dans la section 6.8.

5.5.6 Système de collecte des archives (interne ou externe)

Le système de collecte des archives respecte les exigences de sécurité définies dans la section 5.3.

5.5.7 Procédures de récupération et de vérification des archives

Les supports sur lesquels sont stockées les informations archivées de l'AC KEYNECTIS SSL font l'objet d'une vérification lors de la création. Des échantillons statistiques de ces informations sont régulièrement testés pour vérifier leur intégrité et lisibilité.

Seuls les équipements autorisés de l'AC KEYNECTIS SSL, rôles de confiance et autres personnes autorisées (personne morale, etc.) ont accès aux archives.

5.6 Changement de clé d'une composante

5.6.1 Certificat SSL

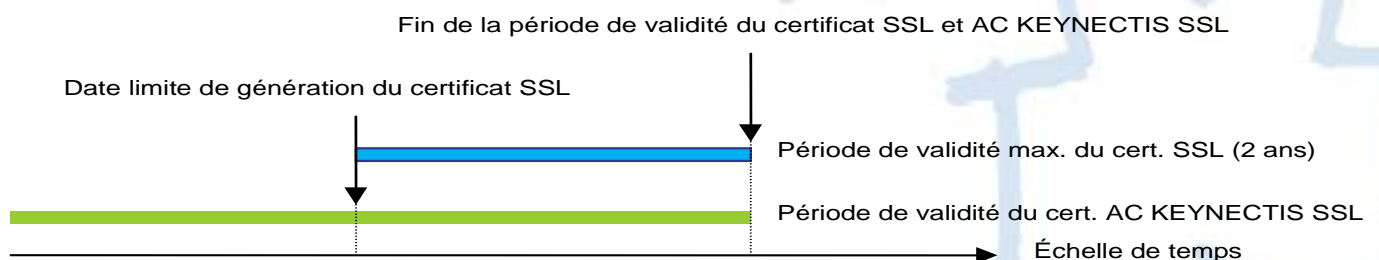
La période de validité d'un certificat K.SSL de test est de 14 jours.

La période de validité d'un certificat SSL est de 1 ou 2 ou 3 ans.

Il est recommandé de générer les certificats SSL dont la période de validité est de 2 ans à l'aide d'une clé de 2048 bits pour l'algorithme RSA.

5.6.2 Certificat de l'AC KEYNECTIS SSL

L'AC KEYNECTIS SSL ne peut générer de certificats SSL dont la date d'expiration excède celle du certificat AC SSL. Par conséquent, la paire de clés de l'AC KEYNECTIS SSL est renouvelée au plus tard 2 (deux) ans avant l'expiration du certificat AC SSL actuel.



Dès qu'une nouvelle paire de clés de l'AC KEYNECTIS SSL est générée, seule la nouvelle clé privée de l'AC SSL est utilisée pour signer les certificats SSL et la LCR.

Le précédent certificat AC SSL reste valide pendant le processus de validation du chemin de certification jusqu'à ce que tous les certificats SSL aient expiré.

Les changements de clé de l'AC KEYNECTIS SSL sont conformes aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé ou de compromission.

5.7 Compromission et reprise après sinistre

5.7.1 Procédures de gestion des incidents et des compromissions

L'AC KEYNECTIS SSL a établi des procédures de continuité des activités pour l'ICP de l'AC KEYNECTIS SSL qui définissent les mesures à prendre en cas de corruption ou de perte de ressources informatiques, logicielles et/ou de données qui pourrait perturber ou compromettre les services de l'AC KEYNECTIS SSL. L'AC KEYNECTIS SSL réalise une évaluation des risques pour déterminer les risques commerciaux ainsi que les procédures opérationnelles et les exigences nécessaires en termes de sécurité, dans le but d'élaborer un plan de reprise après sinistre. Cette analyse des risques est régulièrement révisée si nécessaire (évolution des menaces, évolution des vulnérabilités, etc.). Ces procédures font partie intégrante du processus d'audit décrit dans la section 8, qui permet de valider les opérations faisant l'objet d'une attention immédiate à la suite d'un sinistre, ainsi que le plan de reprise.

Les personnes de l'AC KEYNECTIS SSL qui occupent un rôle de confiance et opérationnel sont spécialement formées pour agir conformément aux procédures définies dans le plan de reprise après sinistre de l'AC SSL pour les activités les plus sensibles.

Si une AC KEYNECTIS SSL détecte une possible tentative de piratage ou toute autre forme de compromission, elle effectue une enquête pour déterminer la nature et le degré des dommages. Sinon, la portée des dommages potentiels est évaluée par l'AC KEYNECTIS SSL afin de déterminer si l'AC KEYNECTIS SSL doit être reconstruite, si seuls certains certificats doivent être révoqués et/ou si l'AC SSL doit être déclarée compromise, les services devant faire l'objet d'une maintenance (informations sur l'état des certificats et la révocation) et le type de maintenance nécessaire d'après le plan de reprise après sinistre de l'AC KEYNECTIS SSL.

L'AC KEYNECTIS SSL est informée de toute compromission réelle ou supposée (logique, physique, électrique, etc.) d'un système de l'AC KEYNECTIS SSL qui aurait compromis, compromettra ou perturbera les services de l'AC KEYNECTIS SSL. L'AC KEYNECTIS SSL est ainsi en mesure d'activer son propre plan de reprise après sinistre afin de protéger ses intérêts et ceux des parties utilisatrices.

5.7.2 En cas de compromission des ressources informatiques, logicielles et/ou des données

Si l'équipement de l'AC KEYNECTIS SSL est endommagé ou ne fonctionne plus, mais que les clés de signature ne sont pas détruites, son fonctionnement est rétabli dès que possible, en donnant priorité à la capacité de générer des informations sur l'état des certificats conformément au plan de reprise après sinistre de l'AC KEYNECTIS SSL.

5.7.3 En cas de compromission de la clé privée d'une composante

En cas de compromission, perte, destruction ou compromission supposée d'une clé de signature de l'AC KEYNECTIS SSL :

- l'AC KEYNECTIS SSL, après avoir mené une enquête, décide de révoquer le certificat de l'AC KEYNECTIS SSL ;
- tous les porteurs de certificats SSL délivrés par l'AC KEYNECTIS SSL compromise sont informés le plus rapidement possible de la révocation possible de leurs certificats SSL et de la façon de les utiliser conformément à leur application commerciale ;
- une nouvelle paire de clés de l'AC KEYNECTIS SSL est générée ;
- en cas de génération d'un nouveau certificat de l'AC KEYNECTIS SSL, cette dernière propose aux porteurs de certificats SSL de générer ou non de nouveaux certificats SSL.

5.7.4 Capacité de continuité des activités après un sinistre

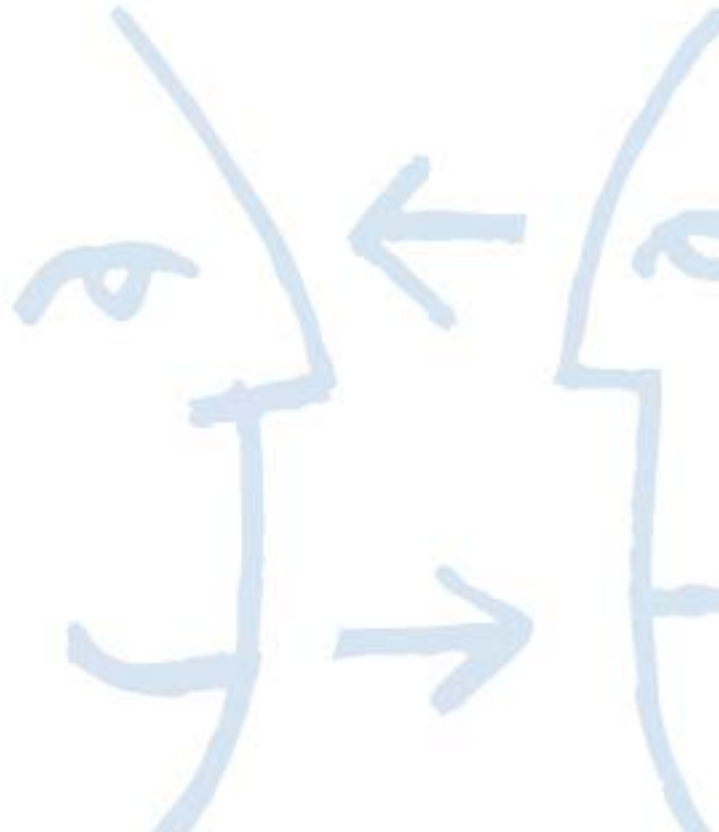
Le plan de reprise après sinistre traite de la continuité des activités comme décrite dans la section 5.7.1. Le service de publication contenant les certificats et les informations sur l'état des certificats est déployé afin de garantir une disponibilité permanente (soit une disponibilité de 99,95 % sauf opérations de maintenance planifiées).

5.8 Fin de vie d'une composante AC SSL

Une AC KEYNECTIS SSL en fin de vie fait révoquer son certificat par l'ACR KEYNECTIS qui le lui a délivré.

L'AC KEYNECTIS SSL en fin de vie informe alors tous ses clients avant sa date de cessation d'activité et :

- cesse de délivrer des certificats SSL conformément à la présente PC ;
- archive tous les journaux d'audit et autres enregistrements avant sa date de cessation d'activité ;
- détruit toutes ses clés privées lors de la cessation de son activité ;
- s'assure que les enregistrements archivés sont transférés vers une autorité appropriée telle qu'une AC qui délivre des services identiques ;
- utilise un moyen sécurisé pour demander à ses clients de supprimer toutes les ancrés de confiance représentant l'AC SSL et veille à leur bonne application.



6 MESURES DE SÉCURITÉ TECHNIQUES

6.1 Génération et installation d'une paire de clés

6.1.1 Génération d'une paire de clés

La génération de clés par l'AC KEYNECTIS SSL est effectuée dans un environnement physiquement sécurisé par des personnes occupant des rôles de confiance dans le cadre au minimum d'un double contrôle composé du détenteur des données d'activation secrètes de l'AC et d'un témoin. La génération de clés par l'AC KEYNECTIS SSL est effectuée dans le cadre d'un dispositif qui est au minimum certifié ISO 15408 (« Critères communs ») au niveau EAL 4+ ou supérieur.

6.1.2 Délivrance de la clé privée au client

Les porteurs de certificats SSL génèrent une clé cryptographique dont la clé publique correspondante est contenue dans la demande de certificat fournie à l'AC KEYNECTIS SSL.

6.1.3 Délivrance de la clé publique à l'émetteur de certificats

Les clés publiques des porteurs de certificats SSL sont délivrées de façon sécurisée (protection de l'intégrité, preuve de l'origine) à l'AC KEYNECTIS SSL pour la délivrance des certificats par l'AE. Le mécanisme de délivrance lie l'identité vérifiée du CT à sa clé publique à certifier.

6.1.4 Délivrance de la clé publique d'une AC aux parties utilisatrices

Les certificats AC SSL sont accessibles aux parties utilisatrices par le biais du SP.

6.1.5 Taille des clés des certificats SSL

Si l'AAK estime que la sécurité d'un algorithme particulier a pu être compromise, elle peut demander à l'AC SSL de révoquer les certificats affectés.

Les porteurs des certificats SSL génèrent des paires de clés RSA d'une taille minimum de 1024 bits (2048 bits recommandés pour l'algorithme RSA). L'AC KEYNECTIS SSL ne peut pas approuver une clé de certificat SSL dont la taille est inférieure à 1024 bits pour l'algorithme RSA.

Il est recommandé d'utiliser l'algorithme RSA avec une fonction de hachage SHA-1.

6.1.6 Génération et contrôle de la qualité des paramètres de clé publique

Les porteurs des certificats SSL génèrent des clés conformément aux exigences techniques du générateur de clés qu'ils utilisent et de façon à garantir qu'il ne subsiste aucune information permettant de déduire la clé privée.

6.1.7 Utilisation de la clé (selon le champ d'utilisation des clés du certificat X.509 v3)

L'utilisation de la clé privée des certificats SSL est définie dans le profil du certificat (voir la section 7.1 ci-dessous). L'utilisation de la clé est configurée de telle sorte à autoriser l'établissement de connexions SSL uniquement par la clé privée et le certificat SSL correspondant.

Cette restriction est mise en œuvre dans le certificat via l'extension d'utilisation des clés.

6.2 Protection des clés privées et fonctionnement du module cryptographique

Les clés des certificats SSL sont générées par les clients SSL à l'aide de fournisseurs de services cryptographiques offerts par la station de travail ou par le serveur sur lequel la paire de clés est générée, conformément aux conditions d'utilisation de ces derniers.

6.2.1 Contrôles et normes du module cryptographique

Le module de sécurité matérielle de l'AC KEYNECTIS SSL est certifié ISO 15408 (« Critères communs ») au niveau EAL 4+ ou supérieur.

Les porteurs des certificats SSL sont chargés de sélectionner le module de sécurité (logicielle, matérielle, etc.) qu'ils utilisent pour générer, utiliser et stocker leurs clés privées.

6.2.2 Contrôle des clés privées (m sur n) par plusieurs personnes

L'activation de la clé privée de l'AC KEYNECTIS SSL pour chaque opération cryptographique s'accompagne d'un contrôle par plusieurs personnes (à l'aide des données d'activation de l'AC), chargées d'effectuer les tâches associées à leurs rôles de confiance. Les rôles de confiance autorisés à participer aux contrôles des clés privées par plusieurs personnes sont rigoureusement authentifiés (jeton avec code PIN).

Le CT est chargé de protéger et de contrôler les clés privées pour le porteur du certificat SSL au nom duquel il agit, afin de garantir uniquement l'utilisation autorisée de celles-ci.

6.2.3 Séquestre des clés privées

Les clés privées de l'AC KEYNECTIS SSL ne sont jamais séquestrées pour aucune raison.

6.2.4 Sauvegarde des clés privées

Les clés privées de l'AC KEYNECTIS SSL sont sauvegardées dans le cadre du même contrôle par plusieurs personnes aux fins du plan de reprise après sinistre de la clé privée d'origine.

6.2.5 Archivage des clés privées

Les clés privées de l'AC KEYNECTIS SSL ne sont pas archivées.

6.2.6 Transfert des clés privées vers ou à partir d'un module cryptographique

Les clés privées de l'AC KEYNECTIS SSL sont générées, activées et stockées dans un module de sécurité matérielle. Lorsque les clés privées se trouvent à l'extérieur du module de sécurité (à des fins de stockage ou de transfert), elles sont chiffrées à l'aide de l'algorithme AES ou Triple DES. Une clé privée chiffrée ne peut être déchiffrée autrement que dans un module cryptographique sous le contrôle de plusieurs personnes aux rôles de confiance définis.

6.2.7 Stockage des clés privées sur un module cryptographique

Les clés privées de l'AC KEYNECTIS SSL sont stockées avec le même niveau de confiance et les mêmes mécanismes opérationnels que le module cryptographique d'origine.

6.2.8 Méthode d'activation des clés privées

La clé privée de l'AC KEYNECTIS SSL est activée sous le contrôle de 4 personnes minimum occupant des rôles de confiance, parmi lesquelles se trouvent les détenteurs des données d'activation.

6.2.9 Méthode de désactivation des clés privées

Les modules de sécurité matérielle de l'AC KEYNECTIS SSL qui ont été activés ne sont pas laissés sans surveillance ou à la merci d'un possible accès non autorisé. Lorsque le module cryptographique de l'AC KEYNECTIS SSL est en ligne, il est uniquement utilisé pour signer les certificats SSL et les LCR émanant de l'AE authentifiée. Lorsqu'une AC KEYNECTIS SSL n'est pas opérationnelle, les clés privées sont supprimées du module de sécurité matérielle.

6.2.10 Méthode de destruction des clés privées



Les clés privées de l'AC KEYNECTIS SSL sont détruites lorsqu'elles ne sont plus nécessaires ou lorsque les certificats auxquels elles correspondent ont expiré ou sont révoqués. La destruction des clés privées requiert la destruction de toutes les données d'activation de l'AC associées de façon à garantir qu'il ne subsiste aucune information permettant de déduire la clé privée.

6.2.11 Certification du module cryptographique

Les modules de sécurité matérielle de l'AC KEYNECTIS SSL sont certifiés ISO 15408 (« Critères communs ») au niveau EAL 4+ ou supérieur.

6.3 Autres aspects de la gestion des paires de clés

6.3.1 Archivage des clés publiques

La clé publique est archivée dans le cadre du processus d'archivage du certificat, tel que décrit dans la section 5.5.2 ci-dessus.

6.3.2 Périodes de validité des certificats et périodes d'utilisation des paires de clés

Les périodes de validité du certificat de l'AC KEYNECTIS SSL et SSL sont définies dans la PC conformément à la section 0.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

La génération et l'utilisation des données d'activation de l'AC KEYNECTIS SSL nécessaires à l'activation des clés privées de cette dernière sont effectuées au cours d'une procédure appelée la « Key ceremony » (voir la section 6.1.1). Les données d'activation sont générées automatiquement et remises au détenteur, une personne occupant un rôle de confiance, de façon à maintenir la confidentialité et l'intégrité des données d'activation.

Les porteurs des certificats SSL garantissent que les paires de clés sont protégées par des moyens appropriés.

6.4.2 Protection des données d'activation

Les données d'activation de l'AC KEYNECTIS SSL sont protégées contre la divulgation grâce à une combinaison de mécanismes de contrôle d'accès physique et cryptographique. Les données d'activation de l'AC KEYNECTIS SSL sont stockées sur des cartes à puce.

Les porteurs des certificats SSL garantissent que leurs données d'activation sont protégées de telle manière que la clé privée ne peut être activée que par l'entité autorisée (personne et/ou machine).

6.4.3 Autres aspects des données d'activation

Les données d'activation de l'AC KEYNECTIS SSL sont uniquement détenues par des employés de KEYNECTIS occupant des rôles de confiance. Toute autre exigence spécifique quant aux données d'activation est détaillée dans la DPC de l'AC KEYNECTIS SSL.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les fonctions suivantes de sécurité informatique sont fournies par le système d'exploitation ou à travers une combinaison de systèmes d'exploitation, de protections logicielles et physiques. Les composants de l'ICP de l'AC KEYNECTIS SSL comprennent les fonctionnalités suivantes :

- authentification des utilisateurs occupant des rôles de confiance ;
- contrôle d'accès discrétionnaire ;

- fonction de vérification de la sécurité (intégrité protégée) ;
- interdiction de réutiliser des objets ;
- utilisation de la cryptographie pour la communication de session ;
- chemin de confiance pour l'identification et l'authentification ;
- isolation du domaine à des fins de traitement ;
- auto-protection du système d'exploitation.

Lorsqu'un équipement de l'ICP de l'AC KEYNECTIS SSL est hébergé sur une plate-forme évaluée, conformément aux exigences en terme de sécurité informatique, alors le système (matériel, logiciel et système d'exploitation), lorsque possible, fonctionne dans une configuration évaluée. Ces plates-formes doivent utiliser au minimum la même version de système d'exploitation que celui qui a été évalué. Les systèmes informatiques sont configurés avec le nombre minimum de comptes requis, services réseau et ne doivent pas être accessibles à distance.

6.5.2 Évaluation de la sécurité des systèmes informatiques

Tous les composants logiciels de l'ICP de l'AC KEYNECTIS SSL doivent être conformes aux exigences du profil de protection de l'agence française Infosec (PP_IGC, PP_AC et PP_AE disponibles sur www.ssi.gouv.fr).

6.6 Mesures de sécurité techniques du cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Les mesures de sécurité liées au développement des systèmes de l'AC KEYNECTIS SSL sont les suivantes :

- les logiciels utilisés ont été conçus et développés en suivant une méthodologie de développement officielle et documentée ;
- l'acquisition du matériel et des logiciels se fait de telle façon à réduire la probabilité de sabotage de tout composant particulier (par exemple en s'assurant que l'équipement a été choisi au hasard au moment de l'achat) ;
- le matériel et les logiciels sont développés dans un environnement contrôlé, et le processus de développement est défini et documenté (cette exigence ne s'applique pas au matériel ou logiciels commerciaux standard) ;
- le matériel doit être expédié ou livré via des méthodes contrôlées qui offrent une chaîne continue de responsabilité, du lieu d'achat à celui des opérations ;
- le matériel et les logiciels sont dédiés aux activités de l'ICP : toutes les applications, périphériques matériels, connexions réseau ou composants logiciels installés font partie du fonctionnement de l'ICP ;
- des mesures appropriées sont prises pour empêcher l'installation de tout logiciel malveillant sur l'équipement. Seules les applications requises pour effectuer les opérations de l'ICP sont obtenues auprès de sources autorisées par les règlements en vigueur au niveau local. Le matériel et les logiciels de l'AC KEYNECTIS SSL sont analysés lors de leur première utilisation, puis régulièrement par la suite afin de détecter d'éventuels programmes malveillants ;
- les mises à jour matérielles et logicielles sont achetées ou développées de la même façon que l'équipement original et doivent être installées par des employés formés et de confiance selon une méthode définie.

6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système de l'AC KEYNECTIS SSL ainsi que toute modification et mise à jour sont documentées et contrôlées par l'autorité administrative de l'AC KEYNECTIS SSL. Un mécanisme permet de détecter toute modification non autorisée apportée à la configuration ou au logiciel de l'AC KEYNECTIS SSL. Une méthodologie officielle de la gestion de la configuration est utilisée pour l'installation et la maintenance continue du système de l'AC KEYNECTIS SSL. Le logiciel de l'AC KEYNECTIS SSL, lorsqu'il est chargé pour la première fois, est vérifié comme étant celui fourni par le vendeur, sans aucune modification, et correspondant à la version appropriée.

6.6.3 Mesures de sécurité liées au cycle de vie

L'AC KEYNECTIS SSL contrôle en permanence les exigences en termes de processus de maintenance afin de veiller à ce que les logiciels et le matériel évalués et certifiés conservent le même niveau de confiance.

6.7 Mesures de sécurité réseau

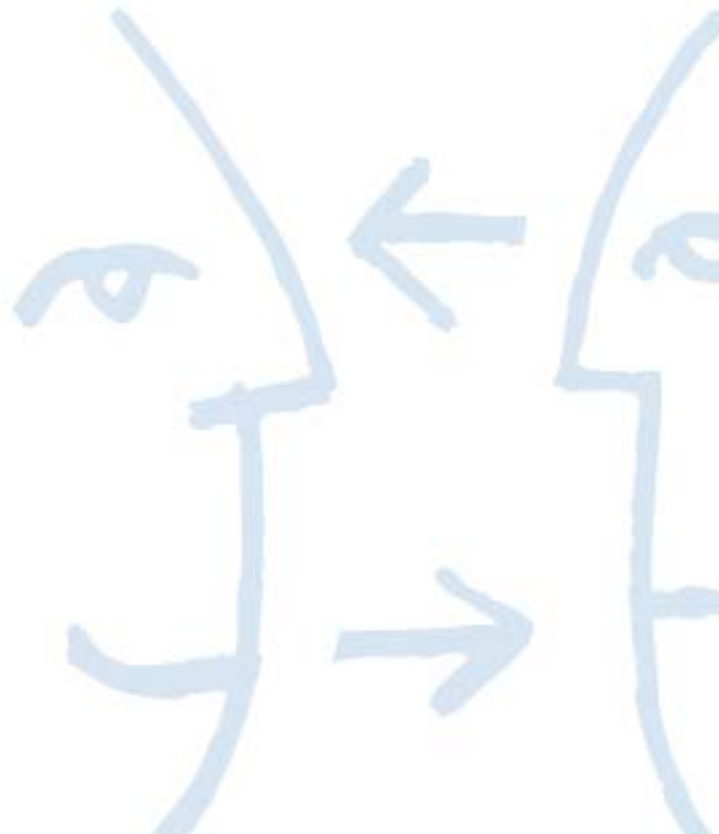
Les composantes de l'ICP de l'AC KEYNECTIS SSL mettent en œuvre des mesures de sécurité adéquates pour garantir leur protection contre les attaques par déni de service et par intrusion. De telles mesures comprennent l'utilisation de protections, pare-feu et routeurs filtrants. Les services et ports réseau inutilisés sont désactivés. Les dispositifs de contrôle utilisés pour protéger le réseau sur lequel l'équipement de l'ICP est hébergé rejettent tous les services sauf ceux nécessaires à l'équipement de l'ICP, même si ces services sont autorisés pour d'autres périphériques sur le réseau.

6.8 Horodatage

Toutes les composantes de l'AC KEYNECTIS SSL sont régulièrement synchronisées avec un service d'horloge tel qu'une Horloge atomique ou le service Network Time Protocol (NTP). Une autorité spécialisée (Autorité d'Horodatage) peut être utilisée pour fournir cette heure de confiance. L'heure dérivée du service d'horloge doit être utilisée pour établir l'heure de :

- la validité initiale du certificat d'une AC ;
- la révocation du certificat d'une AC ;
- la publication des mises à jour des LCR.

La maintenance de l'heure du système peut être assurée à l'aide de procédures électroniques ou manuelles. Les réglages de l'horloge sont des événements pouvant faire l'objet d'audits.



7 PROFILS DES CERTIFICATS, LCR ET OCSP

7.1 Profil des certificats

Les certificats SSL sont des certificats X.509 v3 (renseigner le champ de version avec le nombre entier « 2 »). Les champs des certificats sont ceux définis dans la norme RFC 3280.

7.1.1 Extensions de certificats

Pour un certificat SSL, les extensions suivantes au minimum doivent être utilisées :

- Identifiant de la clé de l'autorité
- Utilisation de la clé
- Identifiant de la clé du sujet
- Points de distribution des LCR
- Contraintes de base

La DPC indiquera sur le certificat les autres extensions.

7.1.2 Identifiants objet d'algorithme

Il s'agit de : sha-1WithRSAEncryption : {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}.

7.1.3 Structure des noms

La structure des noms respecte les exigences décrites dans la section 3.1.

7.1.4 Identifiant d'objet de politique de certification

Le certificat SSL contient l'OID défini dans la PC de l'AC KEYNECTIS SSL.

7.1.5 Utilisation d'extensions de contraintes sur les politiques

Aucune disposition.

7.1.8 Syntaxe et sémantique des qualificatifs de politiques

Aucune disposition.

7.1.6 Règles de traitement de l'extension critique des politiques de certification

Aucune disposition.

7.2 Profil des LCR

L'ACR doit publier des LCR X.509 version deux (v2) (renseigner le champ de version avec le nombre entier « 1 »). Les champs des LCR sont ceux définis dans la norme RFC 3280.

7.2.1 LCR et extensions des entrées des LCR

La DPC doit indiquer les champs d'extension des LCR (numéro de la LCR et identifiant de la clé de l'autorité).

7.3 Profil OCSP

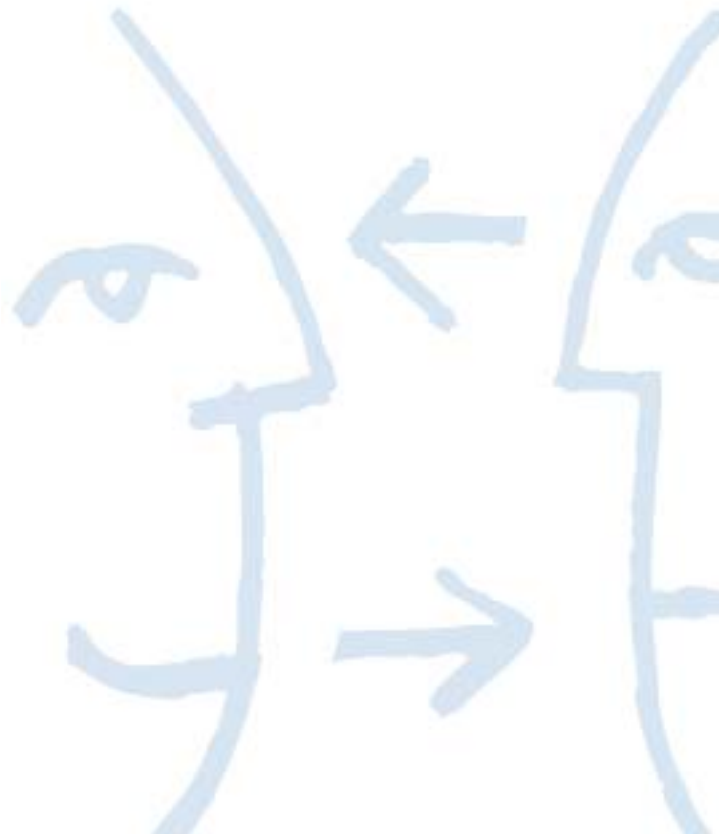
Si un protocole OCSP est utilisé, il doit être conforme à la norme RFC 2560.

7.3.1 Numéro(s) de version

La version 1 de la spécification OCSP comme défini par la norme RFC 2560 est prise en charge.

7.3.2 Extensions OCSP

La DPC doit indiquer l'utilisation d'un protocole OCSP.



8 AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

8.1 Fréquence et circonstances des évaluations

L'ICP de l'AC KEYNECTIS SSL fait l'objet d'audits de conformité réguliers afin de permettre à l'ACR KEYNECTIS SSL d'autoriser ou non (selon les résultats de l'audit) l'AC KEYNECTIS SSL à exercer ses activités dans le cadre de cette PC.

L'AAK a le droit de demander et d'effectuer un audit de conformité de l'ICP de l'AC KEYNECTIS SSL et d'autres entités (par exemple l'AE) qui exercent leurs activités dans le cadre de la présente PC.

8.2 Identité et compétences de l'auditeur

L'auditeur doit posséder des compétences dans le domaine des audits de conformité, et doit être parfaitement au fait des exigences de cette PC. La réalisation de ces audits est la principale responsabilité de l'auditeur. L'AC KEYNECTIS SSL porte une attention particulière à la méthode employée pour vérifier les composantes de l'ICP, par rapport à sa propre base d'exigences d'audit. L'AC KEYNECTIS SSL sélectionne elle-même l'auditeur.

8.3 Relation entre l'auditeur et l'entité évaluée

L'auditeur est soit une entreprise privée, indépendante de l'entité évaluée, soit suffisamment éloigné au niveau organisationnel de cette entité pour fournir une évaluation indépendante et impartiale.

L'AAK détermine si l'auditeur répond à cette exigence.

8.4 Domaines abordés par l'évaluation

L'objectif d'un audit de conformité est de vérifier qu'une composante exerce ses activités conformément aux processus définis par la présente PC et la DPC associée.

8.5 Mesures prises suite au constat de lacunes

L'AAK peut déterminer qu'une AC KEYNECTIS SSL ou une entité agissant pour le compte de l'AC KEYNECTIS SSL exerce ses activités en conformité ou non avec les obligations définies dans la PC, auquel cas et selon la gravité de la non-conformité, l'AC KEYNECTIS SSL peut :

- cesser son activité, ou
- suspendre le fonctionnement de la composante de l'AC KEYNECTIS SSL non conforme, ou
- cesser ses relations avec l'entité affectée agissant pour le compte de l'AC KEYNECTIS SSL, ou
- décider de mettre en place des mesures correctives.

Lorsque l'auditeur découvre une divergence entre la conception, le fonctionnement ou la maintenance de l'AC SSL et les exigences de la PC, les mesures suivantes doivent être prises :

- prise en compte de la divergence par l'évaluateur ;
- notification de l'entité par l'auditeur de la divergence. L'entité doit rapidement en informer l'AAK ;
- détermination par la partie chargée de corriger la divergence des notifications à envoyer ou des mesures nécessaires conformément aux exigences de cette PC, puis envoi de ces notifications et mise en œuvre de ces mesures suite à l'approbation de l'AAK.

Selon la nature et la gravité de la divergence, et selon la rapidité à laquelle elle peut être corrigée, l'AC KEYNECTIS SSL peut décider d'interrompre temporairement le fonctionnement d'une AC KEYNECTIS SSL afin de révoquer un certificat délivré par l'ACR, ou pour prendre d'autres mesures qu'elle juge appropriées.

8.6 Communications des résultats

Le Rapport de conformité de l'audit, comprenant l'identification des mesures correctives mises en œuvres ou qui le seront par la composante, est remis à l'AAK et à l'AC KEYNECTIS SSL. Le rapport identifie les versions de la PC et de la DPC utilisées pour l'audit. Le Rapport de conformité de l'audit n'est pas disponible sur Internet pour les parties utilisatrices.

9 AUTRES QUESTIONS JURIDIQUES ET COMMERCIALES

9.1 Tarification

9.1.1 Frais de délivrance des certificats

Certificat K.SSL Gold	1 an	2 ans
	380 €HT	650 €HT

Club SSL - packs	1 an	2 ans
Pack 10	2 660 €HT	4 550 €HT
Pack 25	6 460 €HT	11 050 €HT
Pack 50	12 350 €HT	21 125 €HT
Pack 100	22 800 €HT	39 000 €HT
Club SSL – Certificats SSL	Certificat SSL 1 an	Certificat SSL 2 ans
1 -12 certificats	266 €HT	455 €HT
13 - 25 certificats	258 €HT	442 €HT
26 - 50 certificats	247 €HT	422 €HT
51 - 100 certificats	228 €HT	390 €HT
101 - 200 certificats	210 €HT	376 €HT

9.1.2 Frais d'accès à un certificat

Le service de publication de l'AC KEYNECTIS SSL (qui contient le certificat de l'ACR et de l'AC KEYNECTIS SSL) est accessible gratuitement sur Internet.

9.1.3 Frais de révocation ou d'accès aux informations d'état

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 Frais découlant d'autres services

Les conditions générales s'appliquant aux offres de l'AC KEYNECTIS SSL mentionnent les frais particuliers le cas échéant.

9.1.5 Politique de remboursement

Si la demande de remplacement de certificat est faite à moins de 15 jours calendaires de la validation de la demande initiale et si toutes les conditions suivantes sont respectées :

- Le nom du contact est le même
- L'organisation est la même
- Le CN du certificat est le même



Alors il n'est pas nécessaire de procéder à l'authentification et la vérification téléphonique. L'émission du nouveau certificat est faite immédiatement et gratuitement

Si la demande de remplacement de certificat est faite dans un délai de 15 à 90 jours calendaires par rapport à la validation de la demande initiale et si toutes les conditions suivantes sont respectées :

- Le nom du contact est le même
- L'organisation est la même
- Le CN du certificat est le même

Alors il n'est pas nécessaire de procéder à l'authentification et la vérification téléphonique. L'émission du nouveau certificat est faite immédiatement mais le client est facturé la moitié du prix d'une acquisition initiale

Si la demande de remplacement de certificat est faite dans un délai supérieur à 90 jours calendaires de la validation de la demande initiale, on considère que les vérifications antérieures ne sont plus valables et on recommence tout le processus d'authentification et de vérification comme si c'était une demande initiale. Le certificat est alors facturé au prix d'une demande initiale.

9.2 Responsabilité financière

9.2.1 Couverture d'assurance

L'AC KEYNECTIS SSL applique des niveaux de couverture d'assurance raisonnables et a souscrit à cet effet une assurance responsabilité civile au titre de la réalisation de son activité professionnelle.

9.2.2 Autres actifs

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

9.2.3 Couverture d'assurance ou de garantie pour les entités finales

En cas de dommage pour un client SSL causé par l'AC KEYNECTIS SSL, celle-ci fera appel à son assurance pour couvrir une partie des dommages du client dans la limite de la responsabilité de l'AC KEYNECTIS SSL définie dans les conditions générales de services SSL et aux présentes.

9.3 Confidentialité des informations de l'entreprise

9.3.1 Étendue des informations confidentielles

L'AC KEYNECTIS SSL garantit que seules les personnes de confiance et autorisées ont accès et utilisent les informations confidentielles suivantes :

- enregistrements et archives ;
- données d'identité personnelle ;
- clés privées de l'AC KEYNECTIS SSL ;
- données d'activation secrètes de l'AC KEYNECTIS SSL ;
- rapports et résultats des audits ;
- plans de reprise après sinistre ;
- accord et contrat avec l'AC KEYNECTIS SSL ;
- procédures et politique de sécurité internes de l'AC KEYNECTIS SSL ;
- portion de la DPC définie comme confidentielle.

9.3.2 Informations non confidentielles

Les informations publiées par le SP ne sont pas considérées comme confidentielles, mais sont protégées conformément aux lois applicables sur les droits de propriété intellectuelle.

9.3.3 Protection des informations confidentielles

L'AC KEYNECTIS SSL doit respecter les exigences énoncées dans la législation européenne sur la protection des données personnelles (données personnelles et confidentielles).

9.4 Confidentialité des informations personnelles

9.4.1 Programme de confidentialité

L'AC KEYNECTIS SSL collecte, stocke, traite et divulgue les informations personnelles identifiables conformément à la loi européenne sur la protection des informations confidentielles.

L'AC KEYNECTIS SSL agit en conformité avec la législation européenne sur la gestion et la protection des données personnelles et une AC KEYNECTIS SSL de confiance veille au respect des dispositions légales.

9.4.2 Informations jugées confidentielles

L'AC KEYNECTIS SSL considère les informations suivantes comme confidentielles :

- formulaire de demande de certificat ;
- formulaire de demande de révocation ;
- motif de la révocation.

9.4.3 Informations non jugées confidentielles

Aucune disposition.

9.4.4 Protection des informations privées

Les composantes de l'AC KEYNECTIS SSL traitent et protègent toutes les informations privées de façon à permettre l'accès uniquement aux rôles de confiance (entité juridique ou interne).

9.4.5 Avis et autorisation d'utilisation des informations privées

Les informations privées ne peuvent être utilisées, aux fins des services SSL, sans l'autorisation expresse du client. L'autorisation est obtenue lors du retrait du certificat SSL, via l'acceptation du certificat de l'AC KEYNECTIS SSL délivré par cette dernière.

9.4.6 Divulgence conformément au processus judiciaire ou administratif

L'AC KEYNECTIS SSL respecte la législation en vigueur dans le pays d'enregistrement de la personne morale, et octroie l'accès aux données privées à la personne morale par le biais d'une procédure protégée comprenant l'authentification et l'accès contrôlé et sécurisé à ces données.

9.4.7 Autres circonstances de divulgations des informations

L'AC KEYNECTIS SSL obtient l'autorisation du client SSL de transférer ses informations privées si les activités doivent être transférées d'une entité à une autre, comme décrit dans la section 0.

9.5 Droits de propriété intellectuelle

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

Le client SSL conserve tous les droits de propriété intellectuelle sur les informations contenues dans le certificat SSL délivré par l'AC KEYNECTIS SSL et dont il est propriétaire.

9.6 Déclarations et garanties

9.6.1 Déclarations et garanties de l'AC KEYNECTIS SSL

L'AC KEYNECTIS SSL garantit que toutes les exigences, détaillées dans la présente PC et dans les DPC correspondantes, sont mises en œuvre pour délivrer et gérer les certificats SSL.

L'AC KEYNECTIS SSL doit être en conformité avec les procédures définies dans la PC, même lorsque la fonctionnalité de l'AC KEYNECTIS SSL est menée par des sous-traitants. L'AC KEYNECTIS SSL fournit tous ses services de certification conformément à sa Déclaration des Pratiques de Certification.

Les obligations communes des composantes de l'AC KEYNECTIS SSL comprennent :

- la protection et la garantie de l'intégrité et de la confidentialité de leurs données secrètes et/ou clés privées ;
- l'utilisation de leurs certificats et clés cryptographiques, ainsi que des outils associés spécifiés dans la DPC, uniquement aux fins pour lesquelles ils ont été générés ;
- le respect et l'application de la portion de la DPC qui se rapporte à leur tâche ;
- le respect du travail des auditeurs et la transmission de toutes les informations utiles au contrôle et à la vérification de la conformité avec la présente PC et avec les sections de la DPC applicables ;
- le respect de tout ou partie des accords qui les lient aux représentants SSL ;
- la documentation de leur procédure interne pour compléter la DPC globale ;
- l'utilisation de tous les moyens (techniques et humains) nécessaires à la réalisation de la PC/DPC qu'elles ont mise en œuvre et dont elles sont responsables.

9.6.2 Déclarations et garanties du demandeur

Les obligations du demandeur du certificat SSL sont les suivantes :

- la soumission d'informations précises et complètes à l'AE ;
- le maintien de la confidentialité des informations secrètes utilisées à des fins d'authentification avec les composantes de l'AC KEYNECTIS SSL ;
- le respect de la présente PC.

9.6.3 Déclarations et garanties de l'AE

Les obligations de l'AE (que ce soit l'administrateur SSL ou le service client de KEYNECTIS) sont les suivantes :

- l'authentification du demandeur ;
- la réalisation de toutes les vérifications requises pour la délivrance des certificats SSL ;
- l'authentification de la demande de certificat ;
- l'authentification de la demande de révocation.

9.6.4 Déclarations et garanties du CT

Les obligations du CT sont les suivantes :

- le maintien de la confidentialité des informations secrètes utilisées à des fins d'authentification pendant la récupération du certificat SSL ;
- le respect de la présente PC ;
- la lutte contre toute utilisation non autorisée de la clé privée du certificat SSL et la protection de sa confidentialité ;
- la notification immédiate de l'AC KEYNECTIS SSL de toute demande de révocation du certificat SSL dont il/elle est responsable ;
- la maintenance de l'état des informations de révocation concernant le certificat de l'ACR ou de l'AC KEYNECTIS SSL.

9.6.5 Déclarations et garanties des autres composantes

9.6.5.1 AAK

Les obligations de l'AAK sont les suivantes :

- l'élaboration de la PC et de la DPC ;
- l'audit de la DC SSL ou de l'AC KEYNECTIS SSL ;
- le contrôle de la relation contractuelle avec la DC SSL agissant en tant qu'AE.

9.6.5.2 Administrateur SSL

Les obligations de l'administrateur SSL sont les suivantes :

- la soumission d'informations précises et complètes à l'AC KEYNECTIS SSL ;
- l'utilisation uniquement de certificats obtenus auprès de l'AC KEYNECTIS SSL pour agir en tant qu'AE ;
- le respect de la présente PC et les PC/DPC correspondantes en tant qu'AE ;
- la lutte contre toute utilisation non autorisée de la clé privée du certificat de l'administrateur qu'il/elle détient et la protection de sa confidentialité ;
- la notification immédiate de l'AC KEYNECTIS SSL de toute demande de révocation du certificat SSL dont il/elle est responsable ;
- la maintenance de l'état des informations de révocation concernant le certificat de l'ACR ou de l'AC KEYNECTIS SSL.

9.7 Exonération de garanties

KEYNECTIS garantit les éléments suivants via l'AC SSL et l'AC Racine de KEYNECTIS :

- l'identification et l'authentification de l'AC Racine de KEYNECTIS, avec un certificat auto-signé de l'AC Racine ;
- l'identification et l'authentification de l'AC SSL, avec un certificat de l'AC SSL généré par l'AC racine de KEYNECTIS ;
- l'identification et l'authentification du nom de domaine hébergé par un serveur, avec un certificat SSL généré par l'AC SSL ;
- la gestion des certificats correspondants et des informations sur l'état des certificats concernant la présente PC.

Aucune garantie supplémentaire ne peut être exigée par le client SSL et la partie utilisatrice dans leurs relations contractuelles (le cas échéant).

9.8 Limitations de responsabilité

En ce qui concerne les certificats SSL, l'AC KEYNECTIS SSL est uniquement responsable des exigences et principes de la présente PC.

L'AC KEYNECTIS SSL est responsable de tout dommage direct, certain et immédiat causé à un client ou à une partie utilisatrice du fait de la mauvaise application de la présente PC et de la DPC correspondante.

L'AC KEYNECTIS SSL ne sera pas responsable des préjudices indirects subis par le Client ou par le tiers utilisateur, ceux-ci n'étant en aucun cas préqualifiés par avance par les présentes.

L'AC KEYNECTIS SSL décline toute responsabilité quelle qu'elle soit à l'égard de l'utilisation du certificat de l'ACR, des certificats de l'AC KEYNECTIS SSL et des certificats SSL ou des paires de clés publiques/privées associées à toute autre fin que celle spécifiée dans la présente PC.

9.9 Indemnisation

Dans le cas où la responsabilité de KEYNECTIS serait retenue pour un préjudice subi par le Client et/ou par le tiers utilisateur du Certificat, il est expressément convenu que KEYNECTIS ne serait tenue à réparation des dommages directs certains et immédiats par Certificat concerné, dans les limites maximums suivantes : pour un certificat K.SSL Gold dans une limite qui ne saurait excéder 50.000 euros, et pour un certificat K.SSL Silver dans une limite qui ne saurait excéder 500 euros.

9.10 Durée et résiliation

9.10.1 Durée

La PC et ses amendements entrent en vigueur lors de l'adoption par l'AAK et de la publication par le SP.

9.10.2 Résiliation

Une nouvelle version de la présente PC acceptée par l'AC KEYNECTIS SSL et publiée par le SP peut obliger les composantes de l'AC KEYNECTIS SSL à modifier leur propre DPC afin de rester conformes à la nouvelle version



de la PC. Selon l'ampleur des modifications, l'AAK pourra décider d'auditer le certificat SSL KEYNECTIS ou demander à l'AC KEYNECTIS SSL de prendre les mesures nécessaires au rétablissement de sa conformité dans un délai donné. Selon l'ampleur des modifications apportées à la PC, il se peut que le certificat de l'AC KEYNECTIS SSL n'ait pas à être de nouveau certifié par anticipation.

9.10.3 Effet de la résiliation et survie

La fin de la validité de la présente PC met un terme à toutes les obligations et responsabilités de l'AC KEYNECTIS SSL.

9.11 Avis individuels et communications avec les composantes

L'AC KEYNECTIS SSL fournit une nouvelle version de la PC dès que l'AAK l'a validée, via le SP.

9.12 Amendements

9.12.1 Procédure d'amendement

L'AC KEYNECTIS SSL révisé sa PC et DPC au moins une fois par an. Des révisions supplémentaires peuvent être décidées à tout moment, à l'entière discrétion de l'AC KEYNECTIS SSL ou à la demande de l'AAK. La correction d'erreurs typographiques ou orthographiques qui n'affectent pas la signification de la PC est autorisée sans préavis. L'AC KEYNECTIS SSL peut informer les clients SSL des conséquences des modifications proposées.

9.12.2 Période et mécanisme de notification

L'AC KEYNECTIS SSL informe ses composantes de son intention de modifier la PC/DPC au plus tard 30 jours avant le début du processus de modification.

9.12.3 Circonstances dans lesquelles l'OID doit être modifié

L'OID de la présente PC est modifié si l'AC KEYNECTIS SSL estime qu'un changement de la PC modifie le niveau de confiance fourni par les exigences de la PC ou la documentation de la DPC aux certificats délivrés.

9.13 Dispositions relatives à la résolution des conflits

KEYNECTIS propose de résoudre les conflits portant sur l'identité à définir dans le certificat, et au cas où les parties en conflit ne trouvent pas d'arrangement, le différend sera réglé devant un tribunal français.

9.14 Législation applicable

Les lois applicables qui régissent la validité d'application de la PC/DPC sont les lois de l'État français, conformément à toutes les directives européennes pertinentes qui pourraient s'appliquer. Ce choix a pour objet de garantir l'uniformité des procédures et de l'interprétation pour tous les clients SSL quelle que soit leur situation géographique.

9.15 Conformité avec la législation applicable

Cette PC est soumise aux lois, règles, réglementations, arrêtés, décrets et ordres nationaux, étatiques, locaux et étrangers applicables, notamment mais sans s'y limiter, aux restrictions sur l'exportation et l'importation de matériels, logiciels cryptographiques ou informations techniques.

9.16 Dispositions diverses

9.16.1 Accord complet



Le cas échéant, les conditions générales d'utilisation des services de l'AC KEYNECTIS SSL et/ou de la DPC identifieront les exigences spécifiques.

9.16.2 Cession

Sauf mention contraire dans d'autres contrats, seule l'AC KEYNECTIS SSL peut céder et déléguer cette PC à toute autre partie de son choix.

9.16.3 Divisibilité

Toute partie de la DPC déclarée inapplicable par une cour de justice ne rend pas l'autre partie de la DPC non valide.

9.16.4 Renonciation de droits

Les exigences définies dans la PC/DPC de l'AC KEYNECTIS SSL doivent être mises en œuvre conformément à la PC et la DPC correspondante sans renonciation de droit possible dans l'intention de modifier tout droit ou obligation défini.

9.16.5 Catastrophe naturelle

L'AC KEYNECTIS SSL n'est pas responsable de tout dommage indirect et interruption de services découlant d'une catastrophe naturelle ayant causé des dommages directs aux clients SSL et/ou parties utilisatrices.

9.17 Autres dispositions

La DPC mentionnera les autres dispositions le cas échéant.

