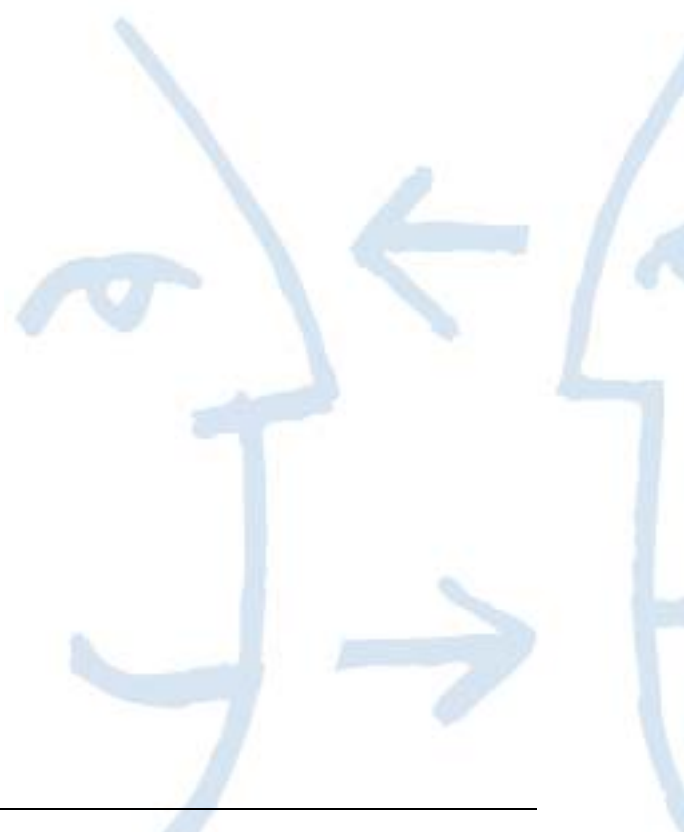




■ POLITIQUE DE CERTIFICATION

KEYNECTIS SERVICES ELECTRONIQUES DE CERTIFICATION CDS

Date:05/11/2010





POLITIQUE ET DECLARATION DES PRATIQUES DE CERTIFICATION POUR LES SERVICES DE CERTIFICATION ÉLECTRONIQUE DE KEYNECTIS-CDS

Numéro de version	1.2	Nombre total de pages :	83
Statut du document	<input type="checkbox"/> Projet		<input checked="" type="checkbox"/> Version finale
Rédacteur du document	Dominique MANENC	KEYNECTIS	

Liste de diffusion :	<input checked="" type="checkbox"/> Externe	<input type="checkbox"/> Interne
-----------------------------	---	----------------------------------

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
15/05/2008	0.9	DM	Version Française	Manenc
24/12/2008	1.0	DM	Version Française contrôlée	Manenc
5/11/2009	1.1	DM	Modification adresses	Manenc
5/11/2010	1.2	DM	Corrections et erreur schema AC	Manenc

Date de publication : 5/11/2010
Date d'entrée en vigueur : 5/11/2010



Préambule

Sans préjudice des droits réservés et sauf autorisation ci-dessous, aucune partie de cette publication ne peut être reproduite, enregistrée ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autres), sans l'autorisation écrite préalable de KEYNECTIS Corporation.

Nonobstant ce qui précède, l'autorisation de reproduire et de diffuser la présente Politique de Certification & Déclaration des Pratiques de Certification (PC/DPC) est consentie sans exclusivité et sans droits d'auteur, sous la réserve que :

- l'avis de droit d'auteur ci-dessus et les paragraphes préliminaires soient mis en évidence au début de chaque exemplaire, et que
- ce document soit reproduit exactement, intégralement et avec mention de la source : KEYNECTIS Corporation.

Toute autre demande de reproduction de la présente Déclaration des Pratiques de Certification de KEYNECTIS doit être adressée à KEYNECTIS – 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France.

Remarque : la PC/DPC de KEYNECTIS peut faire l'objet d'une concession sous licence de KEYNECTIS, à des entités commerciales souhaitant en faire usage dans le cadre de leurs propres services de certification électronique.

KEYNECTIS est une marque déposée de KEYNECTIS Corporation.

Née en 2004, de la fusion des sociétés Certplus et PK7, KEYNECTIS a acquis une expertise dans la commercialisation de services de certification électronique.

Cette PC/DPC régit la délivrance et l'utilisation de services de certification électronique de KEYNECTIS comprenant : la demande de certification, la validation de la demande, la délivrance du certificat, son acceptation, son utilisation et sa révocation. Cette PC/DPC s'applique à une autorité de certification propriété de KEYNECTIS intégrée dans une chaîne de confiance dont la racine autosignée est propriété de ADOBE Corp.

Cette PC/DPC et tous ses amendements sont incorporés par renvoi dans tous les certificats délivrés. La PC/DPC et le certificat sont protégés par des droits d'auteur : © KEYNECTIS. Tous droits réservés.

PRÉSENTATION

En tant qu'utilisateur, vous reconnaissez que KEYNECTIS ou l'AE vous a conseillé de rechercher une formation et d'obtenir des informations appropriées pour vous familiariser avec les signatures numériques et les certificats, avant de demander, d'utiliser et de faire confiance à un certificat. Il est de votre responsabilité de décider si le certificat proposé par KEYNECTIS est conforme ou non à vos besoins.

Avant de soumettre une demande de certificat, vous devez générer une paire de clés et protéger la clé privée contre toute violation, en faisant appel à une méthode digne de confiance, ainsi qu'il est décrit ici plus



en détail. Il appartient à ces dispositifs et à ces applications logicielles extérieurs approuvés d'assurer cette sécurité.

Vous devez accepter un certificat tel que spécifié à la section 4 avant de le communiquer à des tiers ou de l'utiliser d'une manière quelconque. En acceptant un certificat, vous reconnaissez que vous faites implicitement des déclarations importantes.

Si vous êtes le destinataire d'un document électronique portant une signature numérique avec un certificat, il vous appartient de décider si vous pouvez faire confiance à la signature ou au certificat. Au préalable, vous devez contrôler les informations diffusées par KEYNECTIS pour vous assurer que le certificat est valide et qu'il n'est pas révoqué. Puis, à l'aide du certificat, vous devez vérifier que la signature numérique a été créée à une date de validité active du certificat, au moyen de la clé privée correspondant à la clé publique figurant sur le certificat. Cette vérification vous permet également de vous assurer que le message associé à la signature numérique n'a pas été modifié.

Si vous êtes le porteur du certificat ; vous vous engagez à informer l'autorité de certification concernée, en cas de violation de votre clé privée, ainsi qu'il est décrit ici plus en détail.

Cette Politique et Déclaration des Pratiques de Certification contient différents engagements et garanties de KEYNECTIS. Hormis ces engagements et garanties, aucune garantie n'est accordée et la responsabilité de KEYNECTIS et des autorités de certification est limitée.

La Politique et Déclaration des Pratiques de Certification comporte une série de dispositions diverses et interdit les infractions.

Pour en savoir plus, vous pouvez visiter le site Web de KEYNECTIS à l'adresse : <http://www.keynectis.com>.

COMMENTAIRES ET SUGGESTIONS

KEYNECTIS vous invite à lui faire part de vos commentaires et suggestions, en vue des révisions futures de cette PC/DPC.

Veuillez envoyer vos commentaires à : info@keynectis.com.



TABLE DES MATIERES

1	INTRODUCTION	13
1.1	Présentation générale	13
1.2	Identification	13
1.3	Mention de la PC/DPC	13
1.4	Communauté et applicabilité	14
1.5	Autorités de Certification	15
1.6	Autorités d'Enregistrement	15
1.7	Entités finales	15
1.8	Applicabilité	15
1.9	Autorité de Politique	15
1.10	Adresse de l'Autorité de Politique	15
1.11	Texte souligné	15
1.12	Assistance et formation de la clientèle	15
1.13	Table des acronymes et des abréviations	17
2	DISPOSITIONS GÉNÉRALES	18
2.1	Obligations de l'AC	18
2.1.1	Obligations de l'AC KEYNECTIS-CDS (niveau 1)	18
2.1.2	Obligations des Sous-AC KEYNECTIS-CDS (niveau 2)	19
2.2	Obligations des AE	19
2.3	Obligations des entités finales	19
2.3.1	Entités finales dans des rôles de confiance pour le processus de génération de Sous-AC	19
2.3.2	Abonnés	20
2.4	Obligations des parties utilisatrices	21
2.5	Obligations relatives à l'annuaire	22
2.6	Responsabilité	22
2.6.1	Responsabilité de l'AC Racine Adobe	22
2.6.2	Responsabilité de l'AC KEYNECTIS-CDS et des AC subordonnées	22
	<input type="checkbox"/> Limites de responsabilité de l'AC KEYNECTIS-CDS	22
	<input type="checkbox"/> Exclusion de certains éléments de dommages	22
	<input type="checkbox"/> Limitations en matière de dommages et de pertes	23
2.6.3	Responsabilité du demandeur vis-à-vis des parties utilisatrices	23
2.6.4	Responsabilité de l'AE	23
2.7	Responsabilité financière	23
2.7.1	Indemnisations	23
2.7.2	Absence de relation fiduciaire	24
2.7.3	Activités dangereuses	24
2.7.4	Procédure administrative	24
2.8	Interprétation et mise en application	24
2.8.1	Droit applicable	24
2.8.2	Respect des lois et réglementations en matière d'exportation	24
2.8.3	Règlement des litiges et procédures	24
	<input type="checkbox"/> Notification entre les parties en litige	24
	<input type="checkbox"/> Règlement officiel des litiges	25
	<input type="checkbox"/> Succession et cession	25
	<input type="checkbox"/> Fusion	25
	<input type="checkbox"/> Divisibilité	25
2.8.4	Interprétation et traduction	25
2.8.5	Abandon de droit	26
2.8.6	Communications	26
2.9	Facturation des frais	26
2.10	Publication et annuaire	26
2.10.1	Publication d'informations de l'AC KEYNECTIS-CDS et des AC Subordonnées	26
2.10.2	Fréquence de publication	26



2.10.3	Contrôles d'accès	26
2.10.4	Annuaire.....	26
2.11	Audit de conformité et établissement des rapports	27
2.11.1	Fréquence des audits de conformité d'entités	27
2.11.2	Identité/qualification de l'auditeur	27
2.11.3	Relation de l'auditeur avec la partie auditée.....	27
2.11.4	Thèmes abordés par l'audit	27
2.11.5	Mesures prises suite au constat de lacunes.....	28
2.11.6	Communication des résultats	28
2.12	Confidentialité.....	29
2.12.1	Types d'informations à garder confidentielles	29
2.12.2	Types d'informations non considérées comme confidentielles	29
2.12.3	Divulgence d'informations de révocation/suspension de certificats	29
2.12.4	Communication aux responsables de l'application des lois	29
3	IDENTIFICATION ET AUTHENTIFICATION	30
3.1	Enregistrement initial.....	30
3.1.1	Convention de nom.....	30
3.1.2	Nécessité d'utilisation de noms explicites.....	30
3.1.3	Règles d'interprétation des différentes formes de noms	31
3.1.4	Unicité des noms	31
3.1.5	Procédure de règlement des litiges portant sur les noms	31
3.1.6	Droit de KEYNECTIS d'enquêter sur les violations	31
3.1.7	Authentification de l'identité d'organisations et de personnes	31
3.1.8	Informations non vérifiées.....	32
3.1.9	Preuve de possession de clé privée	32
3.2	Renouvellement systématique de clés	33
3.2.1	Renouvellement des clés de l'AC subordonnée KEYNECTIS-CDS et unité d'horodatage.....	33
3.2.2	Renouvellement de clés d'abonnés.....	33
3.3	Renouvellement de clés après une révocation.....	33
3.4	Demande de révocation.....	33
4	EXIGENCES OPÉRATIONNELLES	34
4.1	Description générale du rôle de KEYNECTIS.....	34
4.2	Classification des certificats.....	35
4.2.1	Certificats CDS d'usage 1 (Classe 1)	35
4.2.2	Certificats CDS'USAGE 2 (Classe 2)	35
4.2.3	Certificats CDS Usage 3 (classe 3)	36
4.2.4	Certificat d'horodatage.....	36
4.2.5	Certificat d'AC Subordonnée (Ac Fille).....	37
4.2.6	Certificat de test.....	37
4.3	Principes de validation et propriétés des classes de certificats CDS.....	37
4.3.1	Principe du processus de validation	37
4.3.2	Propriétés des classes de certificats CDS.....	37
4.3.3	Confirmation par des tiers des informations d'une entreprise	39
4.3.4	Confirmation de l'adresse postale	39
4.3.5	Confirmation du détenteur d'un certificat français PRIS V1 ou PRIS V2	39
4.4	Exigences en matière de demande d'un certificat CDS de classe 1	39
4.4.1	Inscription de l'organisation	39
4.4.2	Enregistrement des demandeurs.....	39
4.4.3	Informations de certification.....	40
4.4.4	Procédure de traitement des demandes de certificat	40
4.5	Délivrance d'un certificat CDS de classe 1.....	40
4.6	Acceptation d'un certificat CDS de classe 1	40
4.7	Suspension et révocation d'un certificat CDS de classe 1	40
4.7.1	Motifs d'une révocation	40
4.7.2	Origine de la demande de révocation.....	40



4.7.3	Procédure de demande de révocation.....	40
4.7.4	Période de grâce d'une demande de révocation	40
4.7.5	Motifs d'une suspension	40
4.7.6	Origine de la demande de suspension	40
4.7.7	Procédure d'une demande de suspension	41
4.7.8	Limites relatives à la période de suspension	41
4.7.9	Fréquence de publication des LCR	41
4.7.10	Exigence de contrôle des AR/LCR	41
4.7.11	Contrôle en ligne du statut de révocation	41
4.7.12	Exigences de vérification en ligne des révocations.....	41
4.7.13	Autres moyens disponibles d'information sur les révocations	41
4.7.14	Exigences de vérification d'autres moyens d'information sur les révocations.....	41
4.7.15	Exigences spécifiques en cas de compromission de la clé.....	41
4.8	Exigences en matière de demande d'un certificat CDS de classe 2.....	42
4.8.1	Inscription d'une personne représentant une organisation (Mandataire).....	42
4.8.2	Enregistrement de demandeurs appartenant à une organisation ou représentant l'Organisation.....	42
4.8.3	Inscription d'une personne appartenant à une petite organisation (individuelle)	42
4.8.4	Enregistrement des demandeurs.....	43
4.8.5	Informations de certification.....	44
4.8.6	Procédure de traitement des demandes de certificats	44
4.9	Délivrance d'un certificat CDS de classe 2.....	45
4.10	Acceptation d'un certificat CDS de classe 2	45
4.11	Suspension et révocation d'un certificat CDS de classe 2.....	45
4.11.1	Causes de révocation	45
4.11.2	Origine de la demande de révocation.....	45
4.11.3	Procédure de traitement de la demande de révocation.....	46
4.11.4	Période de grâce d'une demande de révocation	46
4.11.5	Causes de suspension	46
4.11.6	Origine de la demande de suspension	46
4.11.7	Procédure de la demande de suspension	46
4.11.8	Limites relatives à la période de suspension	46
4.11.9	Fréquence de publication des LCR	46
4.11.10	Exigence de contrôle des AR/LCR	46
4.11.11	Contrôle en ligne du statut de révocation	46
4.11.12	Exigences de vérification en ligne des révocations	47
4.11.13	Autres moyens disponibles d'information sur les révocations	47
4.11.14	Exigences de vérification d'autres moyens d'information sur les révocations.....	47
4.11.15	Exigences spécifiques en cas de compromission de la clé.....	47
4.12	Exigences en matière de demande d'un certificat CDS de classe 3.....	47
4.12.1	Inscription.....	47
4.12.2	Enregistrement des demandeurs.....	47
4.12.3	Procédure d'enregistrement de certificats CDS de classe 3	48
4.12.4	Confirmation des contrôles d'exportation	49
4.12.5	Informations de certification.....	49
4.12.6	Procédure de traitement des demandes de certificats	50
4.13	Délivrance d'un certificat CDS de classe 3.....	50
4.14	Acceptation d'un certificat CDS de classe 3	50
4.15	Suspension et révocation d'un certificat CDS de classe 3.....	50
4.15.1	Causes de révocation	50
4.15.2	Origine de la demande de révocation.....	51
4.15.3	Procédure et traitement d'une demande de révocation de certificat en ligne	51
4.15.4	Procédure et traitement d'une demande de révocation de certificat hors ligne	51
4.15.5	Période de grâce d'une demande de révocation	51
4.15.6	Causes de suspension	51
4.15.7	Origine de la demande de suspension	51
4.15.8	Procédure de la demande de suspension	51



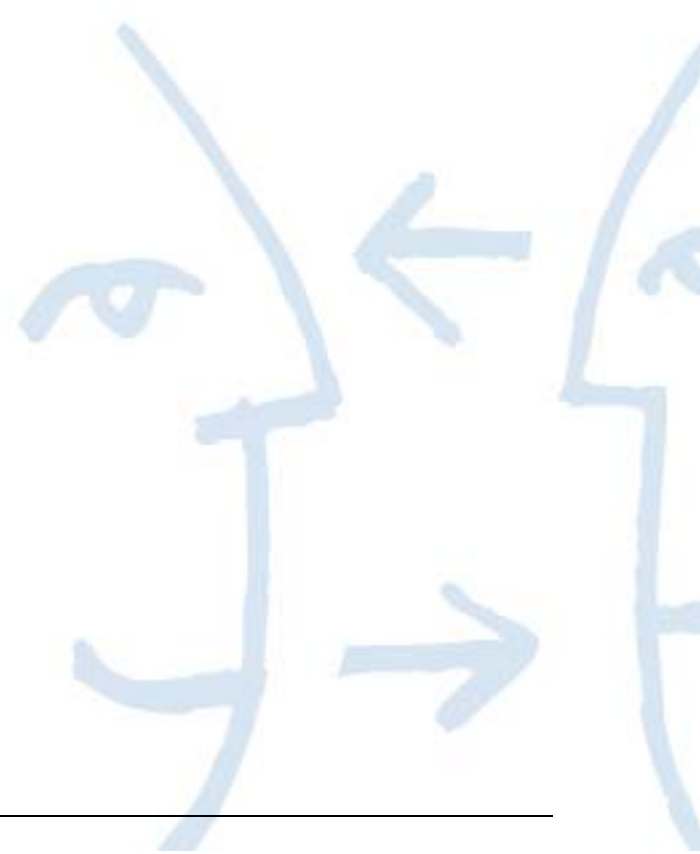
4.15.9	Limites relatives à la période de suspension	52
4.15.10	Fréquence de publication des LCR	52
4.15.11	Exigence de contrôle des AR/LCR	52
4.15.12	Vérification en ligne du statut de révocation	52
4.15.13	Exigences de vérification en ligne des révocations	52
4.15.14	Autres moyens disponibles d'information sur les révocations	52
4.15.15	Exigences de vérification d'autres moyens d'information sur les révocations	52
4.15.16	Exigences spécifiques en cas de compromission de la clé	52
4.16	Exigences en matière de demande de certificats CDS d'UH et d'AC subordonnée (Sous AC)	53
4.16.1	Inscription d'une organisation	53
4.16.2	Enregistrement des demandeurs	53
4.16.3	Informations de certification	53
4.16.4	Procédure de traitement des demandes de certificat	53
4.17	Délivrance d'un certificat CDS d'UH et de Sous-AC	53
4.18	Acceptation d'un certificat CDS d'UH et de Sous-AC	53
4.19	Suspension et révocation d'un certificat d'UH et de Sous-AC	53
4.19.1	Causes de révocation	53
4.19.2	Origine de la demande de révocation	54
4.19.3	Procédure et traitement d'une demande de révocation de certificat	54
4.19.4	Période de grâce d'une demande de révocation	54
4.19.5	Causes de suspension	54
4.19.6	Origine de la demande de suspension	54
4.19.7	Procédure de la demande de suspension	54
4.19.8	Limites relatives à la période de suspension	54
4.19.9	Fréquence de publication des LCR	54
4.19.10	Exigence de contrôle des AR/LCR	54
4.19.11	Vérification en ligne du statut de révocation d'un certificat d'UH et de Sous-AC	54
4.19.12	Exigences de vérification en ligne des révocations	55
4.19.13	Autres moyens disponibles d'information sur les révocations	55
4.19.14	Exigences de vérification d'autres moyens d'information sur les révocations	55
4.19.15	Exigences spécifiques en cas de compromission de la clé	55
4.20	Procédures d'audit de la sécurité	55
4.20.1	Systèmes de confiance	55
4.20.2	Horodatage	55
4.20.3	Types d'événements enregistrés	56
4.20.4	Durées de conservation des documents	56
4.20.5	Fréquence de journalisation	56
4.20.6	Période de conservation des journaux d'audit	56
4.20.7	Protection des journaux d'audit	56
4.20.8	Procédures de sauvegarde des journaux d'audit	56
4.20.9	Système de collecte des journaux d'audit (interne ou externe)	56
4.20.10	Notification au responsable d'un événement	57
4.20.11	Analyse des vulnérabilités	57
4.20.12	Audit relatif aux Sous-AC	57
4.21	Archivage des enregistrements	57
4.21.1	Types d'événements enregistrés	57
4.21.2	Période de conservation des archives	58
4.21.3	Protection des archives	58
4.21.4	Procédure de sauvegarde des archives	58
4.21.5	Exigences en matière d'horodatage des enregistrements	58
4.21.6	Système de collecte des archives (interne ou externe)	58
4.21.7	Procédure de récupération et de vérification des archives	58
4.22	Renouvellement de clés	58
4.23	Compromission et reprise après sinistre	58
4.23.1	En cas de compromission des ressources informatiques, logicielles et/ou des données	58
4.23.2	En cas de révocation de la clé publique d'une entité	58
4.23.3	En cas de compromission de la clé d'une entité	59



4.23.4	Plans d'urgence et reprise après sinistre.....	59
4.24	Fin de vie de l'AC.....	59
4.24.1	Fin de vie ou des activités de l'AC.....	59
4.24.2	Exigences avant la fin de vie.....	59
4.24.3	Réémission des certificats par l'AC successeur.....	59
5	MESURES DE SECURITE PHYSIQUES, PROCEDURALES ET RELATIVES AU PERSONNEL.....	60
5.1	Mesures de sécurité physiques.....	60
5.1.1	Situation géographique et construction de sites.....	60
5.1.2	Accès physique.....	60
5.1.3	Alimentation électrique et climatisation.....	60
5.1.4	Expositions à l'eau.....	60
5.1.5	Prévention et protection contre les incendies.....	60
5.1.6	Stockage des supports.....	60
5.1.7	Traitement des déchets.....	61
5.1.8	Sauvegarde hors site.....	61
5.2	Mesures de sécurité en termes de procédures.....	61
5.2.1	Rôle de confiance.....	61
5.2.2	Nombre de personnes requises par tâche.....	61
5.2.3	Identification et authentification de chaque rôle.....	62
5.3	Mesures de sécurité en termes de personnel.....	62
5.3.1	Procédures de gestion du personnel.....	62
6	MESURES DE SECURITE TECHNIQUES.....	63
6.1	Approbation des logiciels et équipements matériels.....	63
6.2	Génération, installation et protection d'une paire de clés.....	63
6.2.1	Génération d'une paire de clés par l'AC et la Sous-AC KEYNECTIS-CDS.....	63
6.2.2	Délivrance de la paire de clés privées.....	63
6.2.3	Délivrance de la clé publique à l'émetteur de certificats.....	63
6.2.4	Tailles des clés.....	64
6.3	Protection des clés privées.....	64
6.3.1	Protection à l'aide d'un module cryptographique.....	64
6.3.2	Partage de secret.....	64
<input type="checkbox"/>	Protection de la part de secret.....	64
<input type="checkbox"/>	Disponibilité et communication des parts de secret.....	65
<input type="checkbox"/>	Enregistrements à conserver par les émetteurs et détenteurs de parts de secret.....	65
6.3.3	Séquestre des clés privées.....	65
6.3.4	Sauvegarde des clés privées.....	65
6.3.5	Archivage des clés privées.....	65
6.3.6	Introduction des clés privées dans le module cryptographique.....	66
6.3.7	Méthode d'activation des clés privées.....	66
6.3.8	Méthode de désactivation des clés privées.....	66
6.3.9	Méthode de destruction des clés privées.....	66
6.4	Autre aspect de la gestion des paires de clés privées.....	66
6.4.1	Archivage des clés publiques.....	66
6.4.2	Périodes d'utilisation des clés publiques et privées.....	66
6.5	Données d'activation.....	66
6.5.1	Génération et installation des données d'activation.....	66
6.5.2	Protection des données d'activation.....	66
6.6	Mesures de sécurité des systèmes informatiques.....	66
6.6.1	Sécurité des communications.....	66
6.6.2	Sécurité des installations.....	66
6.7	Mesures de sécurité techniques du cycle de vie.....	67
6.7.1	Mesures de sécurité liées au développement des systèmes.....	67
6.7.2	Mesures liées à la gestion de la sécurité.....	67
6.7.3	Evaluation de la sécurité du cycle de vie.....	67
6.8	Mesures de sécurité réseau.....	67



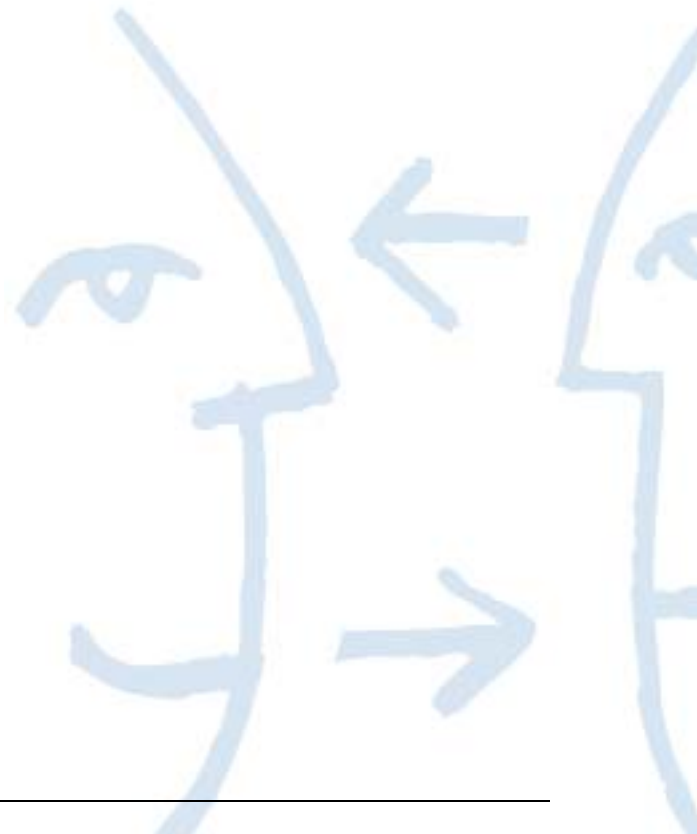
6.9	Mesures de sécurité liées à la conception des modules cryptographiques.....	67
7	PROFILS DES CERTIFICATS ET DES LCR	67
7.1	Extensions et règles de nommage	67
7.1.1	Mécanismes d'extension et cadre d'authentification	67
7.1.2	Extensions standard et spécifiques	67
7.1.3	Identification et criticité des extensions spécifiques	68
7.1.4	Chaînes de certificats et types d'AC.....	68
7.1.5	Extensions de certificats des utilisateurs finals	68
7.1.6	Extensions ISO « Contraintes de base ».....	68
7.1.7	Extensions ISO « Utilisation de la clé » et « Utilisation étendue de la clé ».....	68
7.1.8	Extension ISO « Politique de certification ».....	69
8	ADMINISTRATION DES SPECIFICATIONS	70
8.1	Procédures de modification de la PC/DPC	70
8.2	Politique de publication et de notification.....	70
8.3	Procédure d'approbation de la PC/DPC.....	70
9	ANNEXE	70





INDEX DES FIGURES

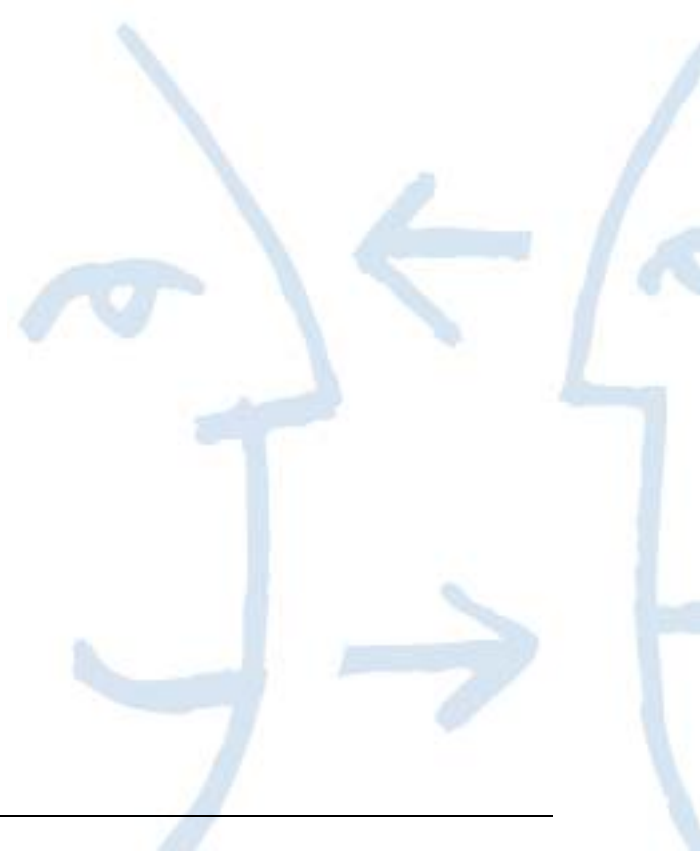
Figure 1 : L'ICP de CDS avec les AC KEYNECTIS-CDS 14





INDEX DES TABLEAUX

Tableau 1 – Acronymes et abréviations	17
Tableau 2 – Distribution des parts de secret.....	64





1 INTRODUCTION

Cette section présente la Politique et la Déclaration des Pratiques de Certification (PC/DPC) de KEYNECTIS et en décrit la structure, ainsi que les conventions sous-jacentes. À la fin de cette section figure une liste des abréviations et des acronymes employés dans cette PC/DPC, afin d'en faciliter la lecture et la compréhension.

1.1 Présentation générale

Cette Politique et Déclaration des Pratiques de Certification de KEYNECTIS énonce les pratiques mises en œuvre par KEYNECTIS, ses Autorités de Certification KEYNECTIS-CDS (CA) et des Autorités de Sous-Certification non KEYNECTIS et autorisées à participer à la fourniture de services de certification électronique KEYNECTIS-CDS, aux fins de la délivrance et de la gestion de certificats, ainsi que du maintien d'une infrastructure à clés publiques (ICP) reposant sur des certificats.

La PC/DPC décrit et régit le processus de certification, depuis la mise en place d'autorités de certification jusqu'à l'enregistrement de demandeurs de certificats, en passant par les opérations de mise en œuvre.

Les services de certification électronique CDS assurent la délivrance, la gestion, l'utilisation, la révocation et le renouvellement de certificats CDS. La DPS a pour but de lier légalement et de notifier toutes les parties qui créent, utilisent et valident des certificats, dans le cadre des services de certification électronique CDS.

Certified Document Services (CDS) est une nouvelle offre de plate-forme, disponible tout d'abord dans la famille de produits Acrobat 6.0. En faisant appel à la technologie de signature numérique, CDS donne aux destinataires, l'assurance que des documents PDF certifiés sont authentiques : qu'ils proviennent bien de leur auteur déclaré et que les parties du document signé par l'auteur n'ont pas été modifiées depuis leur création.

Adobe Systems Incorporated (Adobe) a conclu un contrat avec KEYNECTIS, aux termes duquel la société en tant que tiers est autorisée à offrir des services d'Autorité de Certification (AC), notamment les fonctions de l'Autorité d'Enregistrement (AE), pour Certified Document Services.

L'Autorité de Certification « KEYNECTIS-CDS » est régie par la politique suivante, en conformité avec la politique de certification d'AC de niveau supérieur, dénommée Politique de « Certification CDS », à laquelle a été attribué l'identifiant d'objet (OID) suivant : 1.2.840.113583.1.2.1.

Les services de certification électronique (SCE) de KEYNECTIS-CDS sont destinés à assurer l'échange sécurisé de documents et d'autres services généraux pour répondre aux besoins techniques, professionnels et personnels d'utilisateurs, en matière de signature électronique et d'autres services de sécurité de réseau. À cet effet, l'AC KEYNECTIS-CDS délivre, gère et révoque des certificats, conformément à des pratiques publiées.

Les fonctions d'administration et de gestion des SERVICES DE CERTIFICATION DE KEYNECTIS-CDS autorisent la prise en charge d'une vaste communauté d'utilisateurs, situés en plusieurs points et ayant différents besoins, en termes de sécurité des communications et des informations.

1.2 Identification

Cette Politique et Déclaration des Pratiques de Certification (PC/DPC) est dénommée PC/DPC KEYNECTIS-CDS.

L'identifiant d'objet d'attribut (OID) correspondant à cette PC/DPC est 1.3.6.1.4.1.22234.2.8.2.1.1.

1.3 Mention de la PC/DPC



La présente Politique et Déclaration des Pratiques de Certification doit être citée dans d'autres documents, en tant que « PC/DPC de KEYNECTIS-CDS » ou « Politique et Déclaration des Pratiques de Certification de KEYNECTIS-CDS ». Elle est désignée, en interne, en tant que « PC/DPC » ou « PC/DPC Section x » et ses annexes sont désignées « Annexe Section 1.x ». La PC/DPC est mise à jour régulièrement.

Les versions de la PC/DPC sont identifiées par « PC/DPC » suivi d'un numéro de version (par exemple : « version 1.0 » ou « PC/DPC 1.0 »).

1.4 Communauté et applicabilité

La communauté visée par cette PC/DPC comprend toutes les AC Subordonnées KEYNECTIS-CDS, les AE et les Abonnés dont les identifiants numériques sont liés, via l'AC KEYNECTIS-CDS, à l'AC Racine Adobe intégrée dans les produits Acrobat®, Reader® et LiveCycle® par Adobe, ainsi que toutes les Parties Utilisatrices qui font confiance à ces identifiants numériques.

La communauté concernée par cette PC/DPC appartient à la Communauté CDS d'ADOBE et l'extension de politique de certification de tous les identifiants numériques délivrés au sein de la communauté ICP de CDS est renseignée au moyen de l'OID identifié à la section 1.2.

Les certificats d'abonnés délivrés par l'AC KEYNECTIS-CDS et toutes les Sous-AC ne doivent être utilisés qu'aux seules fins de signature numérique de documents PDF Adobe et de vérification de ces documents, sur les plates-formes prises en charge.

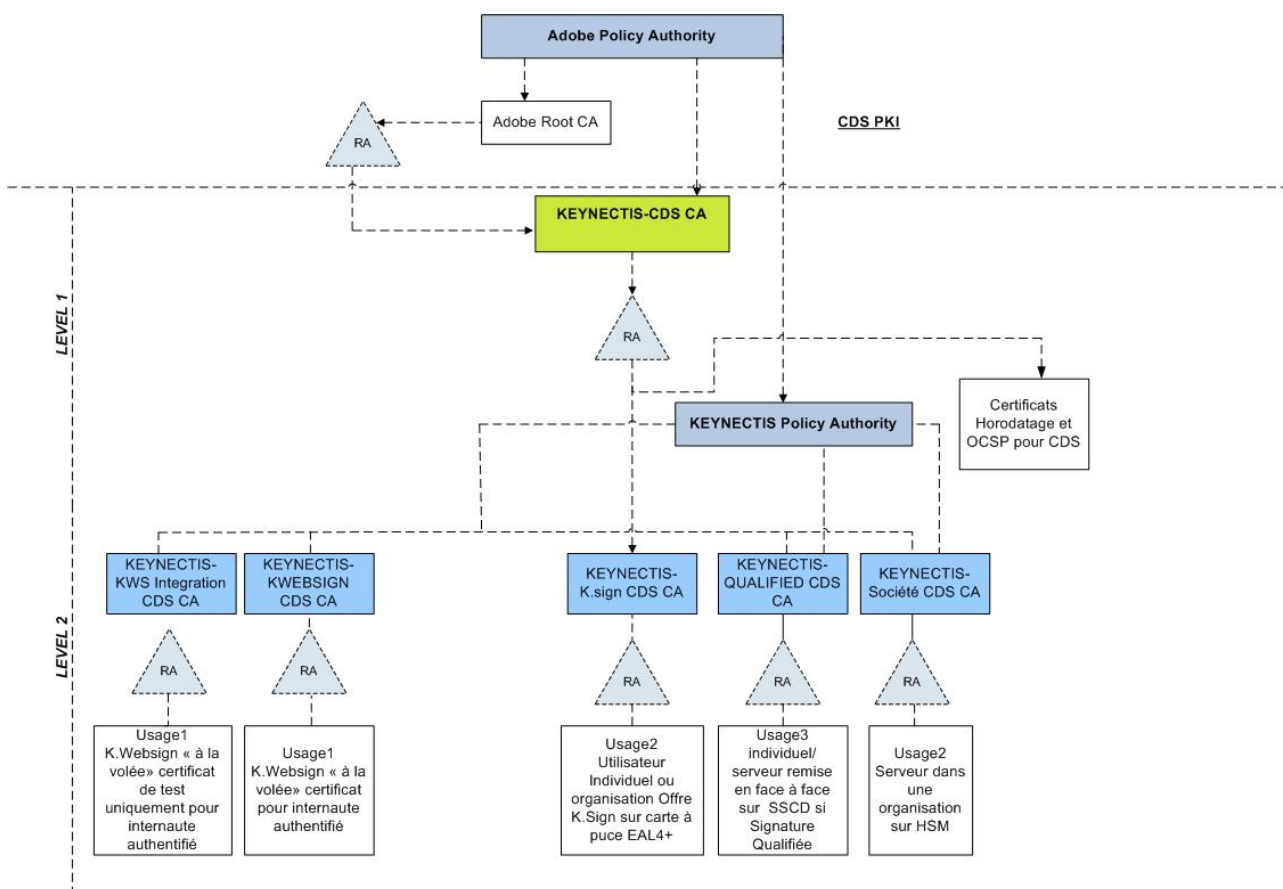


Figure 1 : L'ICP de CDS avec les AC KEYNECTIS-CDS



1.5 Autorités de Certification

L'AC KEYNECTIS-CDS est un tiers autorisé par Adobe à créer des identifiants numériques CDS et à les délivrer à des abonnés, dans le cadre de cette politique. Dans ce document, les AC KEYNECTIS-CDS correspondent à des AC de niveau 1 et de niveau 2.

1.6 Autorités d'Enregistrement

Les Autorités d'Enregistrement (AE) gèrent le cycle de vie des certificats pour leur AC respective. Les AE sont chargées de demander à l'AC de délivrer et de révoquer des identifiants numériques, conformément à cette politique, ainsi qu'à toutes politiques et procédures complémentaires pertinentes, y compris leur PC/DPC, procédure de fonctionnement respectives, etc.

1.7 Entités finales

Les Entités Finales sont des Abonnés et des Parties Utilisatrices.

Un Abonné est une personne ou une organisation autorisée qui possède un identifiant numérique CDS qui lui a été délivré et qui utilise cet identifiant numérique pour signer ou cosigner un document CDS.

Les Parties Utilisatrices sont des destinataires de documents CDS souhaitant vérifier la signature de l'Abonné.

1.8 Applicabilité

Seules des AC autorisées peuvent délivrer des identifiants numériques CDS de signature à des abonnés, conformément à cette PC/DPC. Les identifiants numériques CDS ne peuvent être utilisés qu'à des fins de signature numérique et de vérification des documents PDF Adobe sur les plates-formes prises en charge.

1.9 Autorité de Politique

Cette politique est gérée par l'Autorité de Politique de KEYNECTIS. L'Autorité de Politique de KEYNECTIS se compose de membres sélectionnés au sein de l'équipe dirigeante de KEYNECTIS.

1.10 Adresse de l'Autorité de Politique

Autorité de Politique de KEYNECTIS - 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France.

1.11 Texte souligné

Le texte souligné correspond à la première occurrence de termes définis, employés dans ce document. La PC/DPC est publiée par KEYNECTIS :

- au format électronique à l'adresse suivante : www.keynectis.com/PC
- au format papier disponible au 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France.
- L'accès à la version officielle de tous les documents ouverts via le Web, se fait sous mode « non protégé » (<http://>). Si un mode « protégé » est requis, il suffit de remplacer <http://> par <https://> pour appeler le protocole sécurisé Secure Socket Layer (SSL).

Pour tout complément d'information, merci d'envoyer un e-mail à info@keynectis.com.

1.12 Assistance et formation de la clientèle

Cette PC/DPC suppose que le lecteur est familiarisé avec la signature numérique, les ICP et les services de certification électronique de KEYNECTIS. Si ce n'est pas le cas, nous conseillons au lecteur de suivre une formation aux techniques de clés publiques, avant de demander un certificat.

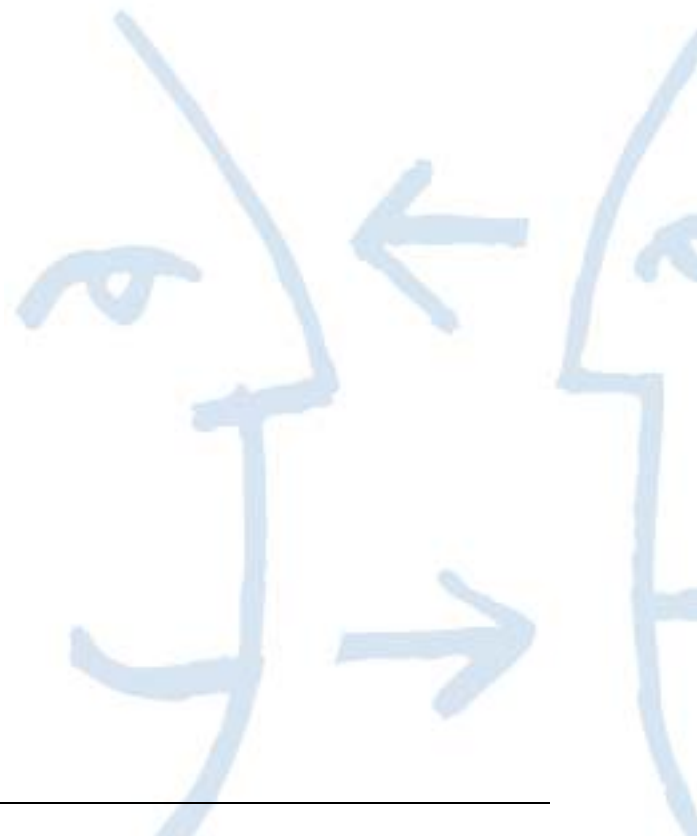
Des renseignements sur les formations sont disponibles auprès de KEYNECTIS.



Le service client de KEYNECTIS (service.clients@keynectis.com) peut également apporter une assistance complémentaire.

Tous les demandeurs de services de certification électronique et les abonnés reconnaissent cette PC/DPC (incorporée par renvoi dans l'accord d'abonnement) et reconnaissent que :

- il leur a été recommandé de suivre une formation adéquate à l'utilisation des techniques de clés publiques, avant de demander un certificat, et
- la documentation et la formation relatives aux signatures numériques, aux certificats, à l'IPC et aux services de certification électronique sont disponibles auprès de KEYNECTIS.





1.13 Table des acronymes et des abréviations

AC	Autorité de Certification
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
CDS	Certified Document Services d'ADOBE
DAM	Draft Amendment (projet d'amendement)
PC/DPC	Politique et Déclaration des Pratiques de Certification
DSC	Demande de Signature de Certificat
FIPS	Federal Information Processing Standard (norme fédérale de traitement de l'information)
FTP	File Transfer Protocol (protocole de transfert de fichiers)
GMT	Greenwich Meridian Time (Temps du Méridien de Greenwich)
HTTP	Hypertext Transfer Protocol (protocole de transfert hypertexte)
HTTPS	Hypertext Transfer Protocol with SSL (protocole de transfert hypertexte avec SSL)
HSM	HArdware Security Module
ICP	Infrastructure à Clé Publique
INV	Informations Non Vérifiées
LCR	Liste des Certificats Révoqués
MSM	Module de Sécurité Matérielle (cf HSM)
NDR	Nom Distinctif Relatif
PGP	Politique de Gestion de Preuves
PIN	Personal Identification Number (numéro d'identification personnel - données d'activation)
PKCS	Public-Key Cryptography Standard (normes de cryptographie à clé publique)
PRISV1/2	Politique de référencement intersectoriel de sécurité Version ½
PSC	Procédures de Sécurité KEYNECTIS
RSA	Système cryptographique
S/MIME	Secure Multipurpose Internet Mail Extensions (extensions S/MIME)
SCE	Services de Certification Électronique
SSL	Secure Socket Layer
UF	Utilisateur Final
URL	Uniform Resource Locator (localisateur normalisé de ressources uniformes sur le Web)
WWW ou WEB	World Wide Web
X.509	Norme UIT-T pour les certificats et le cadre d'authentification correspondant

Tableau 1 – Acronymes et abréviations



2 DISPOSITIONS GÉNÉRALES

2.1 Obligations de l'AC

2.1.1 Obligations de l'AC KEYNECTIS-CDS (niveau 1)

L'AC KEYNECTIS-CDS déclare et garantit à toutes les Parties Utilisatrices faisant raisonnablement confiance à un identifiant numérique délivré par l'AC CDS et lié à l'AC KEYNECTIS-CDS que : (a) l'AC KEYNECTIS-CDS a pris des mesures raisonnables (non inférieures à celles visées dans les procédures énoncées à la section 3.1.7 de ce document et aux sections 3.1.8 et 3.1.9 du document Politique de Certification CDS d'Adobe) pour vérifier que les informations contenues dans l'identifiant numérique sont exactes ; (b) les informations contenues dans l'identifiant numérique sont le reflet exact des informations fournies par l'Abonné à l'AC KEYNECTIS-CDS ; (c) l'Abonné a accepté l'identifiant numérique conformément aux dispositions de cette politique ; (d) l'AC KEYNECTIS-CDS s'est conformée à la politique CDS d'Adobe et à sa PC/DPC ; et (e) l'AC KEYNECTIS-CDS a mis en place des procédures d'audit pour s'assurer que toutes les AC de niveau 2 subordonnées à l'AC KEYNECTIS-CDS se sont conformées à cette PC/DPC en vigueur.

L'AC KEYNECTIS-CDS déclare et garantit, dans les limites spécifiées dans les sections citées de la PC/DPC, qu'elle :

- mettra en place l'infrastructure et les services de certification, y compris l'installation et la gestion des archives de référence de KEYNECTIS, tels qu'énoncés dans cette PC/DPC ;
- respectera la Politique d'ICP établie pour l'AC Racine ;
- exécutera des procédures de validation pour l'utilisation du certificat spécifié, telles que définies dans cette PC/DPC ;
- délivrera des certificats conformément à la PC/DPC et honorera les divers engagements vis-à-vis des abonnés et des parties utilisatrices, aux termes de cette PC/DPC ;
- publiera des certificats acceptés conformément à la PC/DPC ;
- veillera à ce que chaque abonné potentiel soit informé de la délivrance d'un certificat ;
- exécutera les obligations d'une AC et assurera le respect des droits des abonnés et des parties utilisatrices qui font usage des certificats, conformément à la PC/DPC ;
- révoquera des certificats conformément à la PC/DPC ; ainsi lors de la révocation d'un certificat, veillera à ce que les abonnés soient informés de la révocation par e-mail, courrier postal, téléphone ou télécopie ;
- notifiera la révocation d'un certificat par le biais des LCR figurant dans l'annuaire, conformément à cette PC/DPC ;
- assurera les opérations liées à l'expiration, à la réinscription et au renouvellement de certificats, conformément à la PC/DPC ;
- se conformera aux dispositions de la PC/DPC ;
- s'assurera que tous les abonnés potentiels sont liés par un Accord d'Abonnement applicable à l'utilisation d'un certificat (voir section 4) ;
- conservera des enregistrements (y compris, non limitativement, des LCR) des utilisateurs et des documents nécessaires pour répondre à des demandes concernant son fonctionnement, pendant la durée de validité de l'enregistrement ou du document concerné, et dans tous les cas, pendant au moins 3 (trois) ans.

L'AC KEYNECTIS-CDS déclare et garantit, en outre, que toutes les AC de niveau 2 se soumettront à la Politique de Certification CDS d'Adobe.

L'AC KEYNECTIS-CDS garantit que ses propres clés privées n'auront pas été violées ou compromises, sauf avis contraire de sa part, par le biais des archives de référence de KEYNECTIS et notification immédiate d'Adobe dès la constatation d'une telle violation ou compromission.



2.1.2 Obligations des Sous-AC KEYNECTIS-CDS (niveau 2)

Chaque Sous-AC KEYNECTIS-CDS déclare et garantit, dans les limites spécifiées dans les sections citées de la PC/DPC, qu'elle :

- mettra en place l'infrastructure et les services de certification, tels qu'énoncés dans cette PC/DPC ;
- se conformera à la PC/DPC de l'AC KEYNECTIS-CDS pour le niveau 1, telle qu'énoncée dans la politique de certification CDS d'Adobe ;
- exécutera des procédures de validation pour l'utilisation du certificat spécifié, au moins dans les limites définies dans cette PC/DPC ;
- s'assurera que tous les abonnés potentiels sont liés par un Accord d'Abonnement applicable à l'utilisation d'un certificat (voir section 4) ;
- délivrera des certificats conformément à la PC/DPC et honorera les divers engagements vis-à-vis des abonnés et des parties utilisatrices, aux termes de cette PC/DPC ;
- publiera des certificats acceptés conformément à la PC/DPC ;
- conservera des enregistrements (y compris, non limitativement, des LCR) des utilisateurs et des documents nécessaires pour répondre à des demandes concernant son fonctionnement, pendant la durée de validité de l'enregistrement ou du document concerné, et dans tous les cas, pendant au moins 3 (trois) ans.
- veillera à ce que chaque abonné potentiel soit informé de la délivrance d'un certificat ;
- exécutera les obligations d'une AC et assurera le respect des droits des abonnés et des parties utilisatrices qui font usage des certificats, conformément à PC et à la PC/DPC de la Sous-AC ;
- révoquera les identifiants numériques qu'elle a délivrés, selon les dispositions de cette politique en matière de révocation, y compris, non limitativement, les dispositions de la section 4 ;
- à la révocation d'un identifiant numérique, veillera à ce que l'abonné soit informé de la révocation, par e-mail, courrier postal, téléphone ou télécopie ;
- notifiera la révocation d'un certificat par le biais des LCR figurant dans l'annuaire, plus conformément à cette PC/DPC ;
- assurera le renouvellement et le remplacement des identifiants numériques ;
- publiera et respectera une politique de confidentialité.

2.2 Obligations des AE

En conformité avec la Politique de Certification CDS d'Adobe, l'AC KEYNECTIS-CDS, en tant qu'AC subordonnée à CDS, délègue des activités spécifiques d'enregistrement, à une ou plusieurs AE, en fonction de la classe de l'identifiant numérique à délivrer et de l'accord d'AE conclu avec KEYNECTIS.

Ainsi qu'il est décrit à la section 4 ci-dessous, on distingue les trois AE suivantes :

l'AE d'Organisation mise en œuvre dans la gestion du cycle de vie des certificats d'usage 1 ;

l'AE de KEYNECTIS mise en œuvre dans la gestion du cycle de vie des certificats d'usage 2 ;

l'AE Externe mise en œuvre dans la gestion du cycle de vie des certificats d'usage 3.

L'AC KEYNECTIS-CDS demeure responsable des services fournis par son AE de CDS, conformément à cette PC/DPC. L'AC ou la Sous-AC KEYNECTIS-CDS garantit que les activités de son AE de CDS sont conduites en conformité avec la politique de certification CDS d'Adobe.

2.3 Obligations des entités finales

2.3.1 Entités finales dans des rôles de confiance pour le processus de génération de Sous-AC

Chaque entité finale engagée dans un rôle de confiance, dans le cadre d'une procédure de génération des clés, est tenue de :

- conserver ses clés privées de façon sûre, conformément à cette PC/DPC ;
- ne jamais divulguer des informations donnant accès à ses clés privées, y compris, non limitativement, les PIN, mots de passe, expressions de passe ou d'autres informations ou mécanismes servant à protéger ses clés privées ;
- demander la révocation de son certificat, si elle a des raisons de supposer que ses clés privées ou des informations quelconques permettant d'accéder à ses clés privées ont été compromises ;



- se conformer à toutes les exigences et suivre toutes les instructions au cours de la procédure de génération des clés des AC KEYNECTIS-CDS ;
- se conformer à toutes les autres exigences pouvant être spécifiées, selon les besoins, par KEYNECTIS.

2.3.2 Abonnés

D'une manière générale et conformément aux dispositions d'un Accord d'Abonnement passé entre l'AC KEYNECTIS-CDS ou une AC Subordonnée et l'Abonné pour chaque utilisation d'identifiants numériques délivrés par l'AC KEYNECTIS-CDS ou l'AC Subordonnée, l'Abonné s'engage à :

- Garantir l'exactitude de sa représentation, dans toutes les communications avec l'AC KEYNECTIS-CDS ou l'AC Subordonnée ;
- protéger en permanence la clé privée associée à la clé publique contenue dans tout certificat numérique délivré par l'AC KEYNECTIS-CDS CA ou les AC Subordonnées, conformément à cette politique ;
- informer rapidement l'AC KEYNECTIS-CDS ou l'AC Subordonnée qui lui a délivré son certificat identifiant numérique, s'il soupçonne une compromission de sa clé privée ou s'il a des raisons de croire qu'elle a été compromise ; cette notification doit être adressée à l'AC KEYNECTIS-CDS ou à l'AC Subordonnée, aux termes de la PC/DPC de l'AC ;
- se conformer à tous les termes, conditions et restrictions énoncés dans cette politique et dans l'Accord d'Abonnement applicable.

L'AC Racine, l'AC KEYNECTIS-CDS et les AC Subordonnées se réservent le droit de révoquer le certificat numérique de tout Abonné ayant violé les obligations spécifiées dans cette section ou dans l'Accord d'Abonnement applicable. Dans l'éventualité d'une telle violation, le certificat identifiant numérique de l'Abonné doit être immédiatement révoqué par l'AC KEYNECTIS-CDS ou par l'AC Subordonnée et toutes les autres mesures appropriées doivent être prises.

Les certificats identifiants numériques peuvent être demandés soit directement par les Abonnés, soit par une organisation agissant pour le compte d'un Abonné ou d'un groupe d'Abonnés.

2.3.2.1 Le demandeur est une organisation obtenant un certificat pour le compte d'un abonné individuel

Lorsque le demandeur est une organisation obtenant et gérant une identification numérique pour le compte d'un abonné individuel (au nom de cette personne ou au nom du rôle de cette personne au sein de l'organisation), l'AC KEYNECTIS-CDS ou la SOUS-AC exige de l'organisation qu'elle :

- (a) mette en œuvre des processus qui assurent que la clé privée ne peut être utilisée que moyennant les connaissances et l'action explicite de l'abonné ;
- (b) conserve des informations qui permettent de déterminer le signataire spécifique d'un document particulier ;
- (c) assure que le demandeur d'un certificat numérique a reçu une formation à la sécurité, appropriée à la finalité pour laquelle le certificat numérique est délivré ;
- (d) avise immédiatement l'AC KEYNECTIS-CDS ou l'AC Subordonnée, en cas de perte, divulgation ou autre compromission réelle ou supposée de la clé privée de l'abonné ;
- (e) veille à ce que l'abonné nommé dans le certificat numérique ou responsable de l'utilisation de la clé privée correspondant à la clé publique contenue dans l'identifiant numérique, conclue un Accord d'Abonnement ayant force obligatoire et obligeant l'abonné à :
 - (i) générer ou utiliser une paire de clés générées conformément aux sections 4 et 6 de cette PC par l'AC KEYNECTIS-CDS ou l'AC Subordonnée ou encore son AE et prendre toutes les précautions raisonnables pour éviter toute perte, divulgation ou utilisation non autorisée de la clé privée ;



- (ii) reconnaître que les informations identifiant l'abonné dans l'identifiant numérique sont justes et exactes ou aviser l'AC KEYNECTIS-CDS ou l'AC Subordonnée, en cas d'inexactitude de ces informations ;
- (iii) utiliser le certificat à des fins se rapportant exclusivement à CDS, en conformité avec cette politique ; et
- (iv) demander immédiatement la révocation du certificat, en cas de perte, divulgation ou autre compromission réelle ou supposée de la clé privée de l'abonné.

2.3.2.2 Le demandeur est une organisation se procurant un certificat pour le compte de l'organisation

Lorsque le demandeur est une organisation se procurant et gérant un certificat numérique pour le compte de l'organisation (c'est-à-dire un identifiant numérique d'organisation ou de personne morale), l'AC CDS ou l'AC Subordonnée exige de l'organisation qu'elle :

- (a) mette en œuvre des processus, y compris, non limitativement, la modification de données d'activation, qui assurent que chaque clé privée ne peut être utilisée que moyennant les connaissances et l'action explicite d'une seule personne au sein de l'organisation (le responsable du certificat numérique) ;
- (b) conserve des informations qui permettent de déterminer le signataire spécifique d'un document particulier ;
- (c) assure que le responsable du certificat numérique a reçu une formation à la sécurité, appropriée à la finalité pour laquelle le certificat numérique est délivré ;
- (d) empêche le partage des certificats numériques d'organisation parmi des membres de l'organisation ;
- (e) reconnaisse que les informations identifiant l'organisation dans le certificat numérique sont justes et exactes ou avise l'AC KEYNECTIS-CDS ou la Sous-AC, en cas d'inexactitude de ces informations ;
- (f) veille à ce que le responsable du certificat numérique conclue un Accord d'Abonnement ayant force obligatoire et obligeant le responsable du certificat numérique à :
 - (i) générer ou utiliser une paire de clés générées conformément aux sections 4 et 6 de cette PC par l'AC CDS ou l'AC Subordonnée ou encore son AE et prendre toutes les précautions raisonnables pour éviter toute perte, divulgation ou utilisation non autorisée de la clé privée ;
 - (iii) utiliser le certificat numérique à des fins se rapportant exclusivement à CDS, en conformité avec cette politique ; et
 - (iii) ne pas partager l'identifiant numérique ou des données d'activation relatives à la clé privée correspondant à la clé publique contenue dans le certificat numérique d'organisation ; et
 - (iv) demander immédiatement la révocation du certificat numérique, en cas de perte, divulgation ou autre compromission réelle ou supposée de la clé privée de l'Abonné ;
- (g) avise immédiatement l'AC KEYNECTIS-CDS ou la Sous-AC, en cas de perte, divulgation ou autre compromission réelle ou supposée de la clé privée correspondant à la clé publique contenue dans le certificat numérique d'organisation ; et
- (h) demande la révocation d'un certificat numérique d'organisation, en cas de perte, divulgation ou autre compromission réelle ou supposée de la clé privée correspondant à la clé publique contenue dans le certificat numérique d'organisation.

2.4 Obligations des parties utilisatrices

Outre les obligations des Parties Utilisatrices au titre du Contrat de Licence d'Utilisateur Final d'Acrobat (CLUF), l'AC KEYNECTIS-CDS met en œuvre des efforts commercialement raisonnables pour informer toutes les parties utilisatrices, y compris, non limitativement, via le champ « Notice » (avis à l'utilisateur) dans chaque identifiant numérique qu'elle publie, qu'il n'est possible de faire confiance à un document signé par CDS que si la signature est vérifiée sur une Plate-forme Prise en Charge. Dans le contexte de cette politique, « Plate-forme Prise en Charge » désigne les applications de vérifications d'Adobe spécifiées sur la



page Web d'informations de CDS dont l'adresse actuelle est :
http://www.adobe.com/security/partners_cds.html

2.5 Obligations relatives à l'annuaire

Voir section 2.10.

2.6 Responsabilité

2.6.1 Responsabilité de l'AC Racine Adobe

Les exonérations et les limites de garanties relatives à la responsabilité de l'AC Racine Adobe sont énoncées dans la politique de certification CDS, identifiée par l'OID 1.2.840.113583.1.2.1, dans la section intitulée Responsabilité de l'AC Racine Adobe.

2.6.2 Responsabilité de l'AC KEYNECTIS-CDS et des AC subordonnées

Au moment de la délivrance d'un certificat, l'AC KEYNECTIS-CDS déclare, au titre de la garantie restreinte, que :

- (i) elle s'est conformée à la Politique de Certification CDS (OID = 1.2.840.113583.1.2.1) et à cette PC/DPC ;
- (ii) les informations contenues dans le certificat sont le reflet exact des informations fournies à l'AE de KEYNECTIS-CDS par le demandeur ;
- (iii) elle a pris des mesures raisonnables pour vérifier que les informations contenues dans le certificat sont exactes ; et
- (iv) elle a obtenu l'acceptation de l'Accord d'Abonnement par l'abonné. La nature des mesures prises par KEYNECTIS pour vérifier les informations contenues dans un certificat CDS est décrite dans la section 4.

Sauf expressément stipulé ci-dessus, l'AC KEYNECTIS-CDS et les AC subordonnées déclinent toutes garanties et toutes obligations quelles qu'elles soient, y compris toute garantie de qualité marchande ou de convenance à un usage spécial et toute garantie d'exactitude des informations fournies et déclinent également toute responsabilité pour négligence ou défaut de diligence raisonnable.

Limites de responsabilité de l'AC KEYNECTIS-CDS

Sous réserve des dispositions expresses de la PC/DPC, les AC :

- ne garantissent pas l'exactitude, l'authenticité, la fiabilité, l'exhaustivité, la justesse, la qualité marchande ou la convenance de toutes informations contenues dans des certificats ou par ailleurs compilées, publiées ou diffusées par ou pour le compte d'autorités de certification de KEYNECTIS.
- n'assument aucune responsabilité quant aux informations contenues dans un certificat, sous réserve que le certificat et les renseignements fournis par l'AC KEYNECTIS-CDS à cet effet soient conformes à cette PC/DPC ;
- ne garantissent pas la « non-répudiation » d'un certificat ou d'un message (la non-répudiation est déterminée exclusivement par la loi et par les mécanismes applicables de règlement des différends) ;
- ne garantissent aucun logiciel.

Exclusion de certains éléments de dommages

Sous réserve de toutes obligations d'indemnisation envers Adobe, au titre de la PC CDS d'Adobe ou de tous accords conclus entre KEYNECTIS et Adobe, la responsabilité des AC KEYNECTIS-CDS n'est nullement engagée pour tout dommage indirect, particulier, consécutif, immatériel ou pour tous dommages punitifs liés à l'utilisation, la délivrance, l'efficacité ou l'inexécution de certificats, de signatures numériques ou de toutes autres transactions ou services proposés ou prévus par cette PC/DPC, même si l'autorité de délivrance ou KEYNECTIS ou l'un et l'autre ont été avisés de la possibilité de ces dommages.

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



□ **Limitations en matière de dommages et de pertes**

Le cumul de responsabilités vis-à-vis de toutes les parties (y compris, non limitativement, un demandeur, un destinataire ou une partie utilisatrice) d'une autorité de certification et de toutes les AC de niveau supérieur dans la chaîne de certification à laquelle le certificat d'AC appartient, ne peut en aucun cas excéder la limite de responsabilité spécifiée dans la Politique de Certification de l'AC subordonnée à KEYNECTIS-CDS.

Le cumul de responsabilités de toutes les autorités de certification vis-à-vis de tous les individus concernés par un certificat, au titre de toutes les signatures numériques et des transactions se rapportant à ce certificat, n'excède pas la limite de responsabilité indiquée dans la Politique de Certification de l'AC KEYNECTIS-CDS ou des AC subordonnées, incorporée par renvoi dans l'Accord d'Abonnement.

La limite des dommages s'applique à la perte et aux dommages indirects de tous types, y compris, non limitativement, ceux subis par un demandeur, un destinataire ou une partie utilisatrice, par suite de la confiance accordée à un certificat ou de l'utilisation d'un certificat qui est délivré, géré, utilisé, suspendu ou révoqué par une AC ou par suite de l'expiration dudit certificat.

2.6.3 Responsabilité du demandeur vis-à-vis des parties utilisatrices

Sous réserve des autres obligations des abonnés au titre de cette PC/DPC, les abonnés sont responsables de toutes déclarations inexactes qu'ils font dans des certificats destinés à des tiers qui, après avoir vérifié une ou plusieurs signatures numériques avec le certificat, font raisonnablement confiance au contenu de ce certificat.

2.6.4 Responsabilité de l'AE

Voir section 2.2.

2.7 Responsabilité financière

2.7.1 Indemnisations

2.7.1.1 Par des abonnés

En acceptant un certificat de l'AC KEYNECTIS-CDS, l'abonné s'engage à garantir l'AC Racine à laquelle l'identifiant numérique de l'abonné est lié, l'AC KEYNECTIS-CDS et leurs sous-traitants contre tous actes ou omissions donnant lieu à une responsabilité, à un dommage ou à une perte, à des actions en justice ou à des frais de toute nature, y compris des honoraires raisonnables d'avocat, que les AC, KEYNECTIS et leurs sous-traitants peuvent encourir du fait de l'utilisation ou de la publication d'un certificat à la suite de :

- une fausse déclaration faite par l'abonné (ou par une personne agissant sur instruction de toute personne autorisée par l'abonné) ;
- la non-divulgence par l'abonné d'un fait important, si la fausse déclaration ou l'omission résulte de la négligence ou de l'intention de tromper l'AC, KEYNECTIS ou toute personne recevant le certificat ou lui faisant confiance ; ou
- le fait que l'abonné n'ait pas protégé sa clé privée, utilisé un module de sécurité matérielle ou par ailleurs, pris les précautions nécessaires pour empêcher la violation, la perte, la divulgation, la modification ou l'utilisation non autorisée de sa clé.

2.7.1.2 Par des parties utilisatrices

Outre tous accords passés avec des parties utilisatrices (y compris, non limitativement, le CLUF d'Adobe Acrobat), lorsqu'une partie utilisatrice accepte d'un abonné, un document CDS à signature numérique, l'AC KEYNECTIS-CDS doit mettre en œuvre tous les efforts raisonnables pour exiger de la partie utilisatrice qu'elle garantisse l'AC Racine et l'AC Subordonnée CDS, contre toutes pertes ou dommages causés à des tiers, par suite de toute violation d'Accords de Parties Utilisatrices, de CLUF ou d'une déclaration relative à la

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



divulgateur de l'ICP, y compris, non limitativement, tout défaut de contrôle du statut du certificat, avant de faire confiance à une signature numérique émanant d'un abonné.

2.7.2 Absence de relation fiduciaire

Les AC et KEYNECTIS ne sont pas des agents fiduciaires, des intermédiaires ou d'autres représentants d'abonnés ou de parties utilisatrices.

La relation qui existe entre les AC (ou KEYNECTIS) et les parties utilisatrices n'est pas une relation entre mandataire et mandant. Ni les abonnés ni les parties utilisatrices n'ont autorité pour obliger une AC (ou KEYNECTIS) par contrat ou autre. Les AC et KEYNECTIS ne peuvent faire aucune déclaration contraire, qu'elle soit expresse, implicite, apparente ou autre.

2.7.3 Activités dangereuses

Les services de certification électronique de KEYNECTIS ne sont pas destinés ni autorisés à la revente en tant qu'équipement de contrôle dans des conditions dangereuses ou pour des utilisations qui nécessitent un fonctionnement à sécurité intégrée (par exemple, pour des installations nucléaires, la navigation et les communications aériennes ou des systèmes de contrôle du trafic aérien) où une défaillance peut entraîner directement la mort, des blessures ou de graves dommages à l'environnement.

2.7.4 Procédure administrative

Aucune disposition.

2.8 Interprétation et mise en application

En cas de conflit entre cette PC/DPC et d'autres règles, directives ou contrats, l'abonné est lié par les dispositions de la présente PC/DPC, sauf si l'autre contrat (i) est antérieur à la première publication de cette PC/DPC ; ou (ii) prime expressément sur cette PC/DPC, auquel cas ledit contrat est opposable aux parties de ladite PC/DPC, sous réserve que les dispositions de la PC/DPC ne soient pas interdites par la loi.

2.8.1 Droit applicable

Sauf spécification contraire dans d'autres accords intervenus entre des participants de CDS, la présente PC/DPC, sa mise en œuvre, son interprétation et sa validité sont régies par le droit de la CEE, nonobstant tout autre choix d'un droit applicable stipulé au contrat ou par ailleurs, et sans qu'il soit besoin d'un établissement commercial en France. Le choix du droit de la CEE vise l'uniformité des procédures et de l'interprétation entre tous les utilisateurs, quel que soit leur lieu de résidence ou l'usage qu'ils font de leur certificat.

2.8.2 Respect des lois et réglementations en matière d'exportation

L'exportation de certains logiciels utilisés dans le cadre des services de certification de KEYNECTIS peut être subordonnée à une autorisation des instances gouvernementales concernées. Les parties se conformeront aux lois et réglementations en vigueur en matière d'exportation.

2.8.3 Règlement des litiges et procédures

Notification entre les parties en litige

Sauf spécification contraire dans d'autres accords intervenus entre des participants de CDS, avant de faire appel à un quelconque mécanisme de règlement des litiges (y compris l'arbitrage), au sujet d'un litige portant



sur tout aspect de la présente PC/DPC ou un certificat délivré par une AE, les personnes lésées aviseront KEYNECTIS, l'AC intéressée et toute autre partie concernée par le règlement du litige.

□ **Règlement officiel des litiges**

Excepté si chacune des parties directement impliquée consent à un règlement extrajudiciaire du litige (par exemple, par arbitrage), toute action visant l'application d'une disposition de la présente PC/DPC ou découlant de la PC/DPC ou de toute autre relation commerciale entre les parties concernées, doit être portée devant les tribunaux français. Chaque personne reconnaît par la présente la compétence exclusive en matière personnelle desdits tribunaux et se soumet par la présente à leur compétence exclusive en matière personnelle. Les parties renoncent par la présente à tout droit à un procès avec jury concernant toute action découlant de cette PC/DPC ou des services de certification de KEYNECTIS. Si les parties choisissent un mode de règlement extrajudiciaire, l'arbitrage et la procédure sont régis par le droit français.

□ **Succession et cession**

La présente PC/DPC s'applique au profit et à la charge des successeurs, exécuteurs, héritiers, représentants, administrateurs et cessionnaires des parties, qu'ils soient explicites, implicites ou apparents. Les droits et obligations définis dans la présente PC/DPC sont cessibles aux parties par l'effet de la loi (y compris à la suite d'une fusion ou du transfert d'une participation majoritaire dans l'actionnariat) ou autrement, sous réserve que la cession soit conforme aux dispositions de la PC/DPC en matière de cessation ou de suspension des opérations de l'AC et sous réserve, en outre, que la cession ne constitue pas une novation de toute autre dette ou obligation que la partie cédante a envers les autres parties, au moment de ladite cession.

□ **Fusion**

Aucune condition ou disposition de la présente PC/DPC concernant les droits et obligations de KEYNECTIS ou de toute AC, ne peut être amendée, abandonnée, complétée, modifiée ou annulée verbalement sans un message ou document authentifié de la partie concernée, sauf disposition contraire dans la PC/DPC.

□ **Divisibilité**

Si l'une quelconque des dispositions de la PC/DPC ou son application s'avère invalide ou inexécutable pour quelque raison ou dans quelque mesure que ce soit, les autres dispositions de la PC/DPC (et l'application de la disposition invalide ou inexécutable à d'autres personnes ou circonstances) seront interprétées de façon à respecter au mieux l'intention des parties.

Il est expressément convenu que toutes les dispositions sans exception de la présente PC/DPC qui stipulent une limite de responsabilité, une exonération, une limitation de garantie d'une autre obligation ou une exclusion de dommages, sont dissociables et indépendantes de toute autre disposition et doivent être exécutées comme telles.

2.8.4 Interprétation et traduction

Sauf stipulation contraire ou dans des circonstances exigeant une condition absolue (y compris, non limitativement, des contraintes de temps relatives à la révocation ou à la publication d'informations), la présente PC/DPC doit être interprétée conformément à ce qui est commercialement raisonnable, dans les circonstances en question. Dans l'interprétation de la PC/DPC, il doit être tenu compte de sa portée et de son application internationales, eu égard à l'uniformité de son application et au respect de la bonne foi.

Des versions traduites de la présente PC/DPC sont disponibles dans certaines langues et se trouvent dans les archives. En cas de conflit entre la version française et les autres versions, la version originale anglaise doit être retenue.



2.8.5 Abandon de droit

Le non-respect par une personne d'une disposition de la PC/DPC ne doit pas être considéré comme l'abandon du droit de faire respecter ultérieurement cette disposition ou une autre.

2.8.6 Communications

Toute partie souhaitant ou devant émettre une notification, une exigence ou une demande dans le cadre de la présente PC/DPC doit le faire moyennant un message à signature numérique conforme aux conditions de la PC/DPC ou par écrit.

Les communications électroniques prendront effet à la réception par l'expéditeur d'un accusé de réception à signature numérique de la part du destinataire. L'accusé de réception doit être reçu dans un délai de 5 (cinq) jours ; à défaut, la communication doit être effectuée par écrit.

Les communications écrites doivent être faites par courrier recommandé avec accusé de réception, à l'adresse suivante : KEYNECTIS - 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France.

2.9 Facturation des frais

KEYNECTIS peut facturer aux abonnés l'utilisation de ses services de certification électronique, conformément aux termes du contrat conclu avec KEYNECTIS.

2.10 Publication et annuaire

2.10.1 Publication d'informations de l'AC KEYNECTIS-CDS et des AC Subordonnées

KEYNECTIS gère un annuaire contenant les éléments suivants :

- une ou plusieurs des listes de certificats révoqués (LAR/LCR) délivrées par l'AC KEYNECTIS-CDS ou la Sous-AC, afin de notifier tous les identifiants numériques révoqués dans le cadre de l'ICP de CDS ;
- des copies des versions passées et actuelle de sa PC/DPC indiquant la période de validité de chaque copie de la PC/DPC.

2.10.2 Fréquence de publication

Chaque certificat peut être publié dans l'Annuaire, par l'AC KEYNECTIS-CDS ou la Sous-AC, après délivrance et acceptation dudit certificat, conformément à la section 4 de cette politique.

L'AC KEYNECTIS-CDS ou la Sous-AC doit publier une LCR dans l'Annuaire, au moins toutes les 24 heures, conformément à la section 4 de cette politique.

KEYNECTIS conserve des copies de tous les certificats délivrés pendant deux ans, mais n'archive pas ni ne conserve les LCR expirées ou obsolètes. KEYNECTIS peut procurer d'autres mécanismes de vérification d'état de certificats en ligne, tels que le protocole de vérification en ligne de l'état du certificat (OCSP, Online Certificate Status Protocol).

2.10.3 Contrôles d'accès

KEYNECTIS met en œuvre des efforts raisonnables pour rendre l'Annuaire accessible à toutes les parties, 24 heures sur 24 et sept jours sur sept, sous réserve de la maintenance périodique.

2.10.4 Annuaire

Aucune disposition.



2.11 Audit de conformité et établissement des rapports

L'AC KEYNECTIS-CDS ou sa Sous-AC est gérée dans le Bunker à haute sécurité de KEYNECTIS et régie par la politique d'audit de cette infrastructure.

2.11.1 Fréquence des audits de conformité d'entités

Les opérations de l'AC KEYNECTIS font l'objet d'audits de conformité annuels, conduits dans le cadre de la qualification de KEYNECTIS en tant que prestataire de services de certification (PSC), selon le système français qui fait observer la Directive européenne sur la signature électronique (1999/93/CE).

À cet effet, la France a mis en place un système de qualification où des PSC volontaires (tels que KEYNECTIS) sont audités par un organisme accrédité. Les audits sont conduits annuellement de la manière suivante :

- un audit initial de qualification est réalisé au cours de l'année 1 pour délivrer un certificat de conformité à KEYNECTIS ;
- des audits de maintenance sont réalisés au cours des années 2 et 3 pour s'assurer que les opérations de KEYNECTIS sont toujours conformes et, le cas échéant, que les recommandations émises lors du précédent audit ont été convenablement suivies ;
- un audit initial doit être réalisé au cours de l'année 4 pour délivrer un nouveau certificat de conformité à KEYNECTIS, et ainsi de suite.

Si les audits ne sont pas effectués de la façon prescrite, le certificat de conformité est retiré et le PSC n'est plus référencé sur le site Web de l'organisme de qualification (<http://www.lsti.fr/> option « Organismes certifiés »).

La procédure d'audit est régie par un document technique délivré par le COFRAC (comité français d'accréditation : <http://www.cofrac.fr/>) dont la référence est CEPE REF 21 « Exigences spécifiques pour la qualification des prestataires de services de confiance ».

2.11.2 Identité/qualification de l'auditeur

Les auditeurs de conformité possèdent des compétences dans le domaine des audits de conformité.

Les auditeurs sont des « lead auditors » aux termes de la norme BS7799 (formés pour la mise en œuvre de Systèmes de Management de la Sécurité de l'Information (SMSI) conformément à la norme ISO 27001 : 2005, c'est-à-dire qu'ils sont aptes à conduire des audits pour des Organismes de Certification. En outre, ils sont familiarisés avec le fonctionnement et les exigences d'une ICP similaire à celle de la présente PC/DPC.

La principale responsabilité de l'auditeur de conformité est de conduire ces audits pour le compte de l'organisme de qualification.

2.11.3 Relation de l'auditeur avec la partie auditée

L'organisme de qualification et l'auditeur de conformité sont une société privée accréditée par l'organisme français d'accréditation et totalement indépendante de KEYNECTIS.

L'organisme de qualification est : LSTI SAS - 30 bis, rue du Vieil Abrevoir 78100 Saint-Germain-en-Laye - Téléphone/Télécopie : +33 1 30 61 50 60 – www.lsti.fr

2.11.4 Thèmes abordés par l'audit

L'audit a pour objet de vérifier qu'une composante fonctionne conformément à la présente PC/DPC.

Les thèmes abordés par les audits annuels sont définis d'après la norme ETSI TS 011 456 « Exigences de sécurité pour les autorités de certification délivrant des certificats qualifiés » et comprennent :

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



- 1.2 Infrastructure à clés publiques - Cycle de vie de gestion de clés
 - 1.2.1 Génération de clés par une autorité de certification
 - 1.2.2 Stockage, sauvegarde et recouvrement de clés par l'autorité de certification
 - 1.2.3 Distribution de clés publiques par une autorité de certification
 - 1.2.4 Séquestre de clé
 - 1.2.5 Utilisation de clés par une autorité de certification
 - 1.2.6 Fin de cycle de vie d'AC
 - 1.2.7 Gestion de cycle de vie de matériel cryptographique utilisé pour signer des certificats
 - 1.2.8 Services de gestion de clés du porteur, assurés par l'AC
 - 1.2.9 Préparation de dispositif de création de signature sécurisée
- 1.3 Infrastructure à clés publiques - Cycle de vie de gestion de certificats
 - 1.3.1 Enregistrement du porteur
 - 1.3.2 Renouvellement de certificat, renouvellement de clés et mise à jour
 - 1.3.3 Génération de certificat
 - 1.3.4 Divulgateur de termes et conditions
 - 1.3.5 Divulgateur de certificat
 - 1.3.6 Révocation et suspension de certificat
- 1.4 Gestion et fonctionnement de l'AC
 - 1.4.1 Gestion de la sécurité
 - 1.4.2 Utilisation et gestion d'actifs
 - 1.4.3 Sécurité relative au personnel
 - 1.4.4 Sécurité physique et environnementale
 - 1.4.5 Gestion des opérations
 - 1.4.6 Gestion de l'accès au système
 - 1.4.7 Déploiement et maintenance de systèmes de confiance
 - 1.4.8 Gestion de la continuité des activités et traitement des incidents
 - 1.4.9 Fin de vie de l'AC
 - 1.4.10 Respect des obligations légales

2.11.5 Mesures prises suite au constat de lacunes

Lorsque l'auditeur de conformité constate une divergence par rapport aux exigences de la présente PC/DPC, les mesures suivantes doivent être prises :

- l'auditeur de conformité note la divergence ;
- l'auditeur de conformité avise KEYNECTIS de la divergence ;
- à la fin de l'audit, KEYNECTIS détermine avec l'auditeur les notifications ou les mesures complémentaires nécessaires en vertu des exigences de la PC/DPC et établit un calendrier pour la mise en œuvre de ces actions dans un délai commercialement raisonnable ;
- KEYNECTIS doit soumettre ces mesures nécessaires et le calendrier associé, à l'examen et à l'approbation de l'Autorité de Politique d'Adobe, dans les plus brefs délais.

Lorsque toutes les mesures correctives ont été mises en œuvre, KEYNECTIS doit aviser l'Autorité Politique d'Adobe que le plan correctif a été réalisé.

2.11.6 Communication des résultats

Un résumé du Rapport de l'Audit de Conformité identifiant les mesures correctives prises ou en cours de réalisation par KEYNECTIS, ainsi qu'une copie du certificat de conformité sont fournis à l'Autorité de Politique d'Adobe.

Le Rapport d'Audit de Conformité complet peut être examiné par l'Autorité de Politique d'Adobe, dans les locaux de KEYNECTIS, conformément à la politique en vigueur en matière de protection de l'information.



2.12 Confidentialité

2.12.1 Types d'informations à garder confidentielles

Les informations suivantes sont considérées comme reçues et générées de manière confidentielle par KEYNECTIS et les AC concernées et ne peuvent pas être divulguées sauf dans les cas suivants :

- enregistrements des demandes d'AC, approuvées ou rejetées ;
- accords d'abonnement et documents de demandes de certificats (excepté pour les informations placées dans un certificat ou dans les archives de référence, aux termes de la présente PC/DPC) ;
- enregistrements de transactions (enregistrements complets et journaux d'audit) ;
- enregistrements de journaux d'audit de services de certification, créés ou conservés par KEYNECTIS ou une AC ;
- rapports d'audit de services de certification, créés par KEYNECTIS, une AC, les archives de référence de KEYNECTIS (dans la mesure où ces rapports sont conservés) ou les auditeurs respectifs (internes ou publics) ;
- plans d'urgence et plans de reprise après sinistre ;
- mesures de sécurité contrôlant le fonctionnement du matériel et des logiciels des AC et l'administration des services de certification et des services désignés.

Ni les AC ni KEYNECTIS ne peuvent divulguer ou vendre les noms des demandeurs ou d'autres informations d'identification ou encore partager ces informations, sous réserve des dispositions de la présente PC/DPC. Il convient de préciser, néanmoins, que les archives de référence de KEYNECTIS contiendront des certificats, des révocations et d'autres données.

Ni les AC ni KEYNECTIS ne peuvent divulguer ou être tenus de divulguer des informations confidentielles, hormis dans les cas suivants :

- si la personne envers laquelle l'AC ou KEYNECTIS est tenu à la confidentialité a soumis une demande authentique préalable ;
- si les informations sont requises par une ordonnance de tribunal.

2.12.2 Types d'informations non considérées comme confidentielles

Aucune des informations incluses dans l'identifiant numérique n'est confidentielle.

2.12.3 Divulgateion d'informations de révocation/suspension de certificats

Aucune disposition dans la présente PC/DPC.

2.12.4 Communication aux responsables de l'application des lois

Nonobstant les dispositions qui précèdent, KEYNECTIS peut mettre ces informations à la disposition : (a) de tribunaux, d'organismes chargés de l'application de la loi ou d'autres tiers (y compris, la divulgation en réponse à la communication de documents dans le cadre d'une procédure civile), à la réception d'une ordonnance judiciaire ou d'une assignation ou sur les conseils du conseiller juridique de KEYNECTIS, (b) de responsables de l'application des lois et autres, le cas échéant, aux fins d'enquêter sur une escroquerie présumée, une fausse déclaration, un accès non autorisé ou une activité illégale potentielle de l'abonné (selon l'appréciation de KEYNECTIS) ; (c) d'un acquéreur de KEYNECTIS ou de sensiblement tous les actifs liés à une partie de son activité, dans la mesure où ces informations ont trait aux actifs ou à la/aux branche(s) d'activité faisant l'objet de l'acquisition ; et (d) de prestataires de services et vendeurs tiers dont les fonctions ont trait aux produits et services de KEYNECTIS ou selon les nécessités de KEYNECTIS pour assumer ses responsabilités aux termes du présent accord, sous réserve de l'accord de confidentialité desdits tiers concernant les informations d'abonnés personnellement identifiables.



3 Identification et authentification

L'AC KEYNECTIS-CDS délivre des certificats d'AC subordonnée. Chaque AC subordonnée peut affecter différentes utilisations de certificats à différents types de demandeurs, pour une utilisation dans le cadre de CDS.

	CDS Usage 1	CDS Usage 2	CDS Usage 3	UH/OCSP CDS
Le demandeur est un individu	Oui	Oui	Non	Non
Le demandeur est une organisation obtenant un certificat pour le compte d'un abonné individuel	Oui	Oui	Oui	Non
Le demandeur est une organisation obtenant un certificat pour le compte de l'organisation	Non	Oui	Oui	Oui

Les règles suivantes s'appliqueront à tous les demandeurs précédemment définis et seront respectées par les procédures de demande décrites à la section 4, pour chaque classe de certificats délivrés.

3.1 Enregistrement initial

3.1.1 Convention de nom

Le nom de l'abonné apparaît dans le champ « Porteur » (« Subject » en anglais), sous la rubrique CN (Common Name : nom usuel). Cette mention est obligatoire.

Pour les certificats individuels, il est constitué du prénom usuel et du nom patronymique. Ce nom est celui de l'abonné, tel qu'il figure sur les documents officiels d'état civil.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms utilisés dans le certificat doivent avoir un lien explicite avec l'entité (personne ou objet) à laquelle ils se rapportent.

Les informations portées dans le champ « Porteur » du certificat sont explicites.

- Nom de l'abonné (rubrique CN) ;
- Adresse électronique de l'abonné ;
- Raison sociale de l'organisation représentée par l'abonné, telle que figurant au K-bis ;
- Numéro de SIREN de l'organisation représentée par l'abonné, tel que figurant au K-bis ou N° d'identité donné par une pièce d'identité gouvernementale.
- Pays du siège social de l'organisation représentée par l'abonné, tel que figurant au K-bis et formulé selon la convention internationale de nommage.



Si le client modifie l'une quelconque des informations contenues dans le champ « Porteur », il doit en informer l'AC. L'AC vérifiera alors la nouvelle identité, avant la réémission d'un certificat.

En fonction des modifications apportées, il peut lui être demandé de re-certifier sa clé publique.

3.1.3 Règles d'interprétation des différentes formes de noms

Aucune interprétation particulière n'est requise pour les informations contenues dans le champ « Porteur » des certificats.

3.1.4 Unicité des noms

Chacun des certificats délivrés par l'AC possède une identité unique. L'AE assure cette unicité au moyen du processus d'enregistrement. Tout contact technique demandant un certificat à l'AC doit prouver qu'il a le droit d'utiliser le nom en question en tant qu'identité.

Il appartient à l'AC de résoudre les différends concernant l'utilisation d'un nom pour un certificat.

L'unicité d'un certificat utilisateur est établie au moyen d'un numéro de série, au sein de l'Autorité de Certification. L'AC doit veiller également à l'unicité du champ « Porteur », sur la base de l'adresse électronique de l'abonné, sauf en cas de renouvellement du certificat ou de réutilisation du champ « Porteur ».

3.1.5 Procédure de règlement des litiges portant sur les noms

L'AC doit veiller à l'unicité des noms de ses abonnés et se charger du règlement des différends portant sur la revendication d'un nom.

3.1.6 Droit de KEYNECTIS d'enquêter sur les violations

KEYNECTIS peut (sans y être légalement obligé) enquêter sur toute violation, dans les limites autorisées par la loi. En soumettant une demande d'AC ou une demande de certificat, tous les demandeurs acceptent la conduite et le champ de ces enquêtes et s'engagent à prêter leur concours dans la détermination de tous faits, circonstances et autres informations pertinentes que KEYNECTIS juge appropriés et conformes à la PC/DPC, sous réserve que lesdites enquêtes respectent toutes les lois sur le respect de la vie privée et des données.

L'enquête portant sur une AC peut comprendre, non limitativement, des entretiens, l'examen de livres, documents et procédures, ainsi que l'inspection des installations concernées. L'enquête portant sur des abonnés ou des demandeurs de certificat peut comprendre, non limitativement, des entretiens et des demandes d'examen de documents.

3.1.7 Authentification de l'identité d'organisations et de personnes

Identité d'une organisation

L'authentification est du seul ressort de l'Autorité d'Enregistrement, bien que l'AC KEYNECTIS-CDS demeure responsable vis-à-vis d'Adobe des services fournis par l'AE (voir section 2.2 de cette PC/DPC).

L'AE confirme l'existence de l'organisation mentionnée dans la demande de certificat (Raison sociale, SIREN) et son droit exclusif d'utilisation de son nom. Pour ce faire, l'AE procède à un recoupement des

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTIS_CDS_CA_FR_V1.2.doc



informations fournies avec celles qu'elle a collectées à partir des bases de données des organismes officiels ou des autorités appropriées pouvant confirmer l'existence de l'organisation.

Le contact technique du client soumet le formulaire de demande de certificat à l'AE. Les communications entre le contact technique et l'AE sont protégées, de manière à garantir l'intégrité et l'origine des données transmises. Il appartient à l'AE de vérifier que les informations contenues dans la demande de certificat sont exactes et de contrôler l'identité de l'organisation et du contact technique. L'AE procède à toutes les vérifications nécessaires à l'authentification, au moyen d'une procédure placée sous le double contrôle de deux personnes exerçant des rôles de confiance au sein de l'AE.

L'AE enregistre toutes les informations ayant servi à confirmer l'identité du client, telle qu'elle figure dans la demande de certificat et, le cas échéant, tout attribut spécifique, y compris tout numéro de référence figurant dans la documentation utilisée pour les vérifications, ainsi que toute limite de validité.

Identité d'une personne

L'AE vérifie, lors d'entretiens téléphoniques dont elle a l'initiative, que l'identité des contacts mentionnés sur les demandes de certificat est correcte. Au cours de ces entretiens, elle vérifie diverses informations fournies par le client. Ces vérifications comprennent la confirmation d'informations secrètes transmises par le client lors de la demande de certificat (voir section 4.3).

En outre, l'AE enregistre les étapes suivies pour la délivrance de chaque certificat.

Validation d'un représentant légal

Une demande de certificat faisant état d'une affiliation explicite ou implicite à une organisation ne peut être émise qu'après avoir établi que le contact technique est autorisé à agir pour le compte de cette organisation. Si le contact technique fournit des informations (confirmation d'emploi et autorisation de l'employeur, existence et identité du service cité, attribution d'une fonction, etc.), l'AE authentifie ces informations et/ou le représentant légal qui les délivre.

3.1.8 Informations non vérifiées

Aucune information non vérifiée ne figure dans les certificats.

3.1.9 Preuve de possession de clé privée

Au moment de la demande de certificat (norme PKCS#10), les demandeurs sont tenus de prouver à l'Autorité de Certification qu'ils détiennent la clé privée correspondant à la clé publique à certifier.

3.1.9.1 AC Subordonnée KEYNECTIS-CDS

Les AC Subordonnées CDS sont tenues de prouver qu'elles sont en possession de la clé privée correspondant à la clé publique incluse dans leur demande de certificat. À cet effet, il suffit de signer une demande de certificat au moyen de la clé privée d'AC subordonnée CDS et de délivrer cette demande à l'AC de délivrance. L'AC de délivrance valide alors la signature au moyen de la clé publique d'AC subordonnée CDS comprise dans la demande de certificat. Cette validation est effectuée par le Personnel de Sécurité de KEYNECTIS, au cours d'une procédure de génération des clés qui se déroule dans le Bunker de KEYNECTIS.

3.1.9.2 Abonné

Les abonnés générant leur propre clé privée doivent prouver qu'ils sont en possession de cette dernière, en l'utilisant pour signer une demande de certificat adressée à l'AC de délivrance. L'AC de délivrance valide la signature au moyen de la clé publique de l'abonné.

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



Un contrôle d'utilisation du matériel cryptographique lors du retrait est mis en œuvre pour les abonnés. Les clés privées dont la génération échappe au contrôle des abonnés (CDS Classe 1 ; CDS Classe 2) sont générées par le biais d'un matériel cryptographique et sont délivrées au porteur du certificat ou à un représentant autorisé, au moyen d'une méthode offrant des conditions de sécurité et de traçabilité (voir section 4 Demande).

3.2 Renouvellement systématique de clés

Les paires de clés sont renouvelées régulièrement, afin de minimiser les attaques cryptographiques.

3.2.1 Renouvellement des clés de l'AC subordonnée KEYNECTIS-CDS et unité d'horodatage

Les AC subordonnées KEYNECTIS-CDS peuvent utiliser leur signature en cours de validité pour signer une demande de renouvellement de clés. À la réception d'une demande valide de renouvellement de clés, l'AC KEYNECTIS-CDS délivre un nouveau certificat qui comprend la nouvelle paire de clés de l'AC subordonnée KEYNECTIS-CDS. L'ensemble de ces opérations se déroule au cours d'une procédure de génération des clés.

3.2.2 Renouvellement de clés d'abonnés

Les abonnés peuvent utiliser leur signature en cours de validité pour signer une demande de renouvellement de clés dans la même classe de certificat. À la réception d'une demande valide de renouvellement de clés, l'AC KEYNECTIS-CDS qui a délivré le certificat d'origine délivre un nouveau certificat qui comprend la nouvelle de paire de clés de l'abonné. Ce processus ne peut avoir lieu que deux fois (la troisième fois, une procédure de vérification complète doit être suivie).

3.3 Renouvellement de clés après une révocation

Le renouvellement de clés n'est pas autorisé pour les AC subordonnées KEYNECTIS-CDS, les unités d'horodatage et les certificats d'abonnés qui ont été révoqués. L'identité des AC subordonnées KEYNECTIS-CDS, de l'unité d'horodatage et de l'abonné doit être établie de nouveau, au moyen de la procédure d'enregistrement existante.

3.4 Demande de révocation

Avant d'entreprendre toute action, il est nécessaire d'authentifier les demandes de révocation, excepté pour le CDS Classe 1 qui n'est pas soumis à une procédure de révocation, du fait de la courte durée de son cycle de vie (1 à 5 minutes) mais qui fait néanmoins l'objet d'une publication de LCR.

Lorsque l'abonné est une personne, la demande de révocation est authentifiée par présentation d'un code de révocation. Ce code est connu du représentant de l'entreprise ou de l'abonné.

Pour tous les autres demandeurs, c'est l'AE qui identifie les demandes de révocation. La procédure de vérification exige le même niveau de confiance que pour l'enregistrement initial, afin de s'assurer que le client certifié a réellement fait une demande de révocation.

En conséquence, l'AE doit vérifier les identités des organisations et des personnes demandant une révocation, en suivant les étapes applicables de l'enregistrement initial.



4 EXIGENCES OPÉRATIONNELLES

4.1 Description générale du rôle de KEYNECTIS

L'AC KEYNECTIS-CDS ou ses AC subordonnées agit comme un tiers pour faciliter la confirmation du lien entre une clé publique et une entité nommée (« nommage »). Cette confirmation est représentée par un certificat, c'est-à-dire un message à signature numérique délivré par une AC.

La gestion de haut niveau de ce processus de certification comprend l'enregistrement, le nommage, l'authentification du demandeur, la délivrance, la révocation et la génération d'un état d'audit. Le nommage est principalement du ressort de KEYNECTIS, mais peut également être effectué par une autre partie. Le nommage des Autorités de Certification fait suite à un processus d'enregistrement qui est différent de celui mis en œuvre pour gérer des certificats et déterminer quand les certificats sont valides et opérationnels.

L'AC KEYNECTIS-CDS offre actuellement des niveaux distincts de services de certification électronique. À chaque niveau ou classe de certificat correspondent des fonctions et des caractéristiques de sécurité spécifiques. En fonction de leurs besoins, les demandeurs de certificat doivent opérer un choix entre ces différentes qualités de services et indiquer la classe de certificat qu'ils souhaitent. Selon la classe de certificat souhaitée, les demandeurs de certificat doivent adresser leur demande électroniquement à une AC ou la présenter en personne, en contactant une autorité d'enregistrement (AE).

En réponse à une demande de certificat et après l'authentification appropriée de l'identité du demandeur, un certificat est délivré au demandeur ou un projet de contenu du certificat est envoyé au demandeur. Le demandeur doit vérifier le certificat ou le projet, déterminer s'il répond à ses besoins et, dans l'affirmative, accepter le certificat via le processus d'enregistrement de certificat. Le nouvel abonné accepte d'être lié par les obligations permanentes de la présente PC/DPC.

La gestion des certificats comprend également la désactivation des certificats et la mise hors service des clés privées correspondantes, via un processus de révocation de certificat. D'autres services des AC peuvent comprendre l'impression, la distribution, la publication, le stockage et le retrait de certificats, en fonction de l'usage particulier envisagé pour ces derniers.

Les services de certification électronique de KEYNECTIS gèrent divers mécanismes de sécurité destinés à protéger les communications et les informations. Le certificat à lui seul ne constitue pas un mécanisme de sécurité. Les Services de Certification de KEYNECTIS offrent un cadre dans lequel les services de sécurité peuvent être utilisés par d'autres parties intervenant dans la communication. Ce cadre fait appel aux signatures numériques et à leur vérification pour faciliter la protection des communications et le commerce informatisé sur les réseaux ouverts ; il permet de déterminer si les services de sécurité procurent les assurances prévues.

Les services de sécurité reposant sur des certificats peuvent être utilisés pour parer à des menaces contre la sécurité, dans un environnement défini par l'utilisateur. Les utilisateurs sélectionnent les mécanismes de sécurité, la technologie de sécurité, les contrats de services de sécurité, ainsi que les services de certification électronique adaptés au niveau de risque prévu, afin de protéger leur environnement de communication contre la compromission.

Les Services de Certification de KEYNECTIS utilisent actuellement le système à clé publique RSA pour répondre à tous les besoins en matière de certification. Toutefois, KEYNECTIS s'engage à prendre en charge d'autres normes de signature numérique, lorsque le marché exigera des solutions alternatives.

Le processus de demande défini pour l'abonné et l'AC subordonnée dans l'ICP de CDS a été approuvé par l'Autorité de Politique d'Adobe et prévoit l'établissement et la soumission d'une demande, ainsi que l'acceptation de tout Accord d'Abonnement requis.



4.2 Classification des certificats

Dans le cadre de ses services de certification, KEYNECTIS propose actuellement cinq types distincts de certificats délivrés par l'AC KEYNECTIS-CDS ou sa Sous-Ac.

4.2.1 Certificats CDS d'usage 1 (Classe 1)

Les certificats de classe 1 ne sont délivrés qu'à des personnes, via le service K.Websign®. Les certificats de classe 1 confirment que le nom d'un utilisateur ou son alias et/ou son adresse électronique constituent un porteur. Les certificats de classe 1 sont générés par une application spécifique dénommée K.Websign® qui exerce la fonction opérationnelle d'AE pour le compte d'une organisation dont le nom est contenu dans le certificat (OU – Organization Unit – unité d'organisation). Le certificat a une durée de vie courte et n'est utilisé que pour une seule signature ou cosignature d'approbation d'un document CDS préalablement signé par un identifiant numérique CDS de classe 3 de l'organisation. Au moment de la demande de classe 1, l'application K.Websign contrôle la validité de la signature du document CDS reçu en provenance de l'AE. Le certificat est publié dans l'annuaire de KEYNECTIS et est disponible dans les archives du fichier Preuve de l'installation d'archivage externe, conformément au document de politique de gestion de preuves (PGP) portant la référence OID (1.3.6.1.4.1.22234.2.4.6.1.2). La référence de la preuve électronique est unique et restera dans la partie DN (nom distinctif) de CDS classe 1 (OU).

L'organisation joue le rôle d'une AE pour les certificats CDS de classe 1 et accepte, en tant qu'AE, la pleine responsabilité de l'identification et de l'authentification de l'abonné final, conformément à la présente PC/DPC et au contrat spécifique énonçant les obligations et les responsabilités liées à l'utilisation de l'application K.Websign.

La paire de clés CDS de classe 1 est générée par le centre de confiance KEYNECTIS Operation, à l'aide d'un module HSM FIPS 140 de niveau 2 ou supérieur.

Les certificats de classe 1 peuvent fournir une assurance significative sur l'identité du demandeur, sur la base d'un processus de vérification du nom, de l'adresse électronique du demandeur et d'autres informations fournies à l'organisation tenant lieu d'AE. Ils sont utilisés aux seules fins de signature électronique d'approbation de documents PDF CDS préalablement signés (avec un certificat de classe 3), entre l'organisation et le demandeur.

4.2.2 Certificats CDS'USAGE 2 (Classe 2)

Les certificats de classe 2 sont délivrés à des personnes au sein d'une organisation ou à un représentant de l'organisation afin d'établir de façon probante l'identité du demandeur individuel ou de l'organisation. Les certificats de classe 2 permettent de vérifier que les informations fournies par le demandeur concordent avec celles disponibles dans des bases de données déclarées, telles que la base de données des ressources humaines de l'organisation ou la base de données des clients de l'organisation (Exemple la banque), laquelle base de données est reconnue par une association agréée par le gouvernement, etc. Toute base de données de validation doit être référencée dans l'accord d'abonnement. Les certificats de classe 2 sont utilisés par les clients de KEYNECTIS qu'à des fins se rapportant exclusivement à CDS et à l'authentification forte.

Après soumission en ligne d'une demande de certificat de classe 2 à une autorité d'enregistrement (l'AE de KEYNECTIS ou l'AE de l'organisation), les informations d'enregistrement du demandeur de certificat sont vérifiées auprès de bases de données tierces (AE de KEYNECTIS) ou d'une base de données interne (AE de l'organisation). En fonction de ces informations, l'AE pourra soit approuver soit rejeter la demande. Lorsque l'AE de l'organisation est mise en œuvre, un document électronique (approbation ou rejet) signé avec un certificat CDS de classe 2 doit être utilisé par l'AE et archivé au cours de la procédure.

Certificat CDS de classe 2 pour un détenteur de certificat conforme à la PRIS V1 ou V2 française

Le programme du gouvernement français en matière de signature, dénommé PRIS, a établi des règles de délivrance de certificats spécifiques. Un demandeur de classe 2, détenteur d'un certificat valide délivré par



une AC accréditée par le gouvernement français (conformément aux réglementations PRIS V1 ou PRIS V2) peut demander un certificat CDS de classe 2. Cette demande suivra une procédure de vérification fondée sur la classe du certificat accrédité PRIS et sur la conformité du matériel utilisé .

Les certificats de classe 2 peuvent fournir une assurance significative quant à l'identité du demandeur (Personne ou organisation), sur la base d'un processus de vérification du nom, de l'adresse du demandeur et d'autres informations fournies dans la demande de certificat, et par comparaison de ces informations avec celles contenues dans des bases de données référencées. L'AE de KEYNECTIS peut également vérifier l'identité, la société, etc., du demandeur, au moyen d'appels téléphoniques directs. La confirmation repose sur des critères de correspondance de KEYNECTIS entre des bases de données tierces et les informations figurant dans la demande.

La paire de clés du certificat CDS de classe 2 est générée au moyen d'un module HSM FIPS 140 de niveau 2 ou supérieur.

Bien que KEYNECTIS mette en œuvre une méthode d'authentification évoluée pour vérifier et valider l'identité d'un demandeur de certificat de classe 2, il n'exige pas la présence physique du demandeur face à une autorité de confiance (telle qu'une AE). Par conséquent, ces avantages et ces limites doivent être pris en compte dans la décision d'obtenir, d'utiliser ou de faire confiance à un certificat de classe 2 et doivent déterminer l'utilisation de celui-ci.

4.2.3 Certificats CDS Usage 3 (classe 3)

Les certificats de classe 3 sont délivrés par le biais de différentes procédures, afin d'établir de façon probante l'identité du demandeur individuel ou de l'organisation.

Les certificats d'organisation de classe 3 sont délivrés à des organisations. Ces certificats offrent une garantie importante quant à l'identité d'un demandeur individuel ou d'un représentant légal.

Un type de certificat individuel de classe 3 est dénommé « certificat administrateur ou mandataire de classe 3 (autorité d'enregistrement) ». Il n'est délivré qu'à un administrateur autorisé, permanent et salarié de l'organisation, approuvé par une personne juridiquement reconnue de l'organisation pour exécuter des fonctions d'administrateur d'AE autorisé. Pour être habilité par l'AE de KEYNECTIS, cet administrateur d'AE ou mandataire doit se présenter physiquement face à cette dernière, avant que le certificat d'administrateur ne puisse être approuvé ou lors de la remise. La clé privée correspondant à la clé publique contenue dans un certificat administrateur de classe 3 doit être générée et stockée de manière sûre dans un dispositif cryptographique externe certifié au moins selon FIPS 140-1 de niveau 2. Après la délivrance du certificat, l'AE de l'organisation peut utiliser ce certificat pour signer un formulaire de demande PDF pour des demandes individuelles ou serveur de son organisation.

Un autre type de certificat d'organisation de classe 3 est le certificat de serveur de signature de classe 3, délivré à une organisation, par le biais d'un processus de validation multiple comprenant :

- des documents signés,
- une communication téléphonique avec l'organisation professionnelle,
- la confirmation des informations fournies au moyen d'un document juridique.

La clé privée doit être installée dans un module sécurisé HSM FIPS-140-1 de niveau 2 ou supérieur.

Les certificats de classe 3 nécessitent la **présence physique du demandeur** (personne elle même ou via représentant de l'organisation ayant un certificat administrateur ou mandataire)

4.2.4 Certificat d'horodatage

KEYNECTIS ne délivre des certificats d'horodatage qu'à sa propre organisation, via l'AC subordonnée « KEYNECTIS CDS CA » de niveau 1. Ces certificats sont délivrés exclusivement pour des services d'horodatage de KEYNECTIS hébergés dans le centre de confiance de KEYNECTIS ou dans un centre d'installation audité spécifique agissant par délégation aux services d'horodatage de KEYNECTIS.



Le certificat d'horodatage met en œuvre différentes procédures au cours d'une procédure de génération des clés, afin d'établir de façon probante l'identité du demandeur de l'organisation, y compris une communication en face à face avec l'organisation professionnelle et la confirmation des informations relatives à cette dernière, via des tiers, afin de procurer des motifs de confiance supplémentaires.

La paire de clés du certificat d'horodatage est générée au moyen d'un module HSM FIPS 140 de niveau 2 ou supérieur.

4.2.5 Certificat d'AC Subordonnée (Ac Fille)

KEYNECTIS délivre des certificats d'AC fille à des organisations. Ces certificats ne sont délivrés que pour être utilisés sous le contrôle de KEYNECTIS Operation, à l'intérieur des installations de KEYNECTIS dans le Bunker hautement sécurisé de KEYNECTIS.

La paire de clés du certificat de Sous-AC est générée au moyen d'un module HSM FIPS 140 de niveau 3 (EAL4+) situé dans la salle de procédure de génération des clés (voir section 7).

4.2.6 Certificat de test

KEYNECTIS peut délivrer des certificats de test à des fins exclusives de tests autorisés. Les certificats de test comprennent soit un OID spécifique (utilisé par la plate-forme CDS d'Adobe pour générer un message d'avertissement) soit dans l'objet, des informations spécifiques concernant l'usage et l'objectif du test, de même que dans les informations de politiques de certification. Seules des personnes autorisées peuvent utiliser des certificats de test.

4.3 Principes de validation et propriétés des classes de certificats CDS

4.3.1 Principe du processus de validation

À la réception de demandes de certificats, les AC effectuent toutes les validations requises avant de délivrer des certificats. L'AC établit que :

- le demandeur du certificat est la personne identifiée dans la demande (en accord avec la description des classes de certificats et dans les limites de celles-ci) ;
- le demandeur de certificat a le droit de détenir la clé privée correspondant à la clé publique indiquée dans le certificat ;
- les informations devant figurer sur le certificat (à l'exception des informations non vérifiées du demandeur) sont correctes ;
- toute organisation qui demande un certificat mentionnant la clé publique du demandeur de certificat (autorisé pour les certificats de classes 2 et 3) est dûment autorisée à formuler cette demande.

Une fois le certificat délivré, l'AC n'est plus tenue de surveiller ou de contrôler l'exactitude des informations du certificat, sauf si elle est avisée d'une violation du certificat, conformément à la PC/DPC.

Sous réserve des dispositions des sections 8.1 et 8.3 des présentes, KEYNECTIS se réserve le droit de mettre à jour ses procédures de validation afin d'améliorer le processus de validation. Les procédures de validation mises à jour peuvent être obtenues auprès de KEYNECTIS – 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France.

4.3.2 Propriétés des classes de certificats CDS

Le tableau ci-après énonce certaines caractéristiques de chaque classe de certificat.

	Résumé de la confirmation d'identité	Protection de la clé privée de l'AC	Protection de la clé privée du demandeur	Applications mises en œuvre ou envisagées par les utilisateurs
CDS Classe 1	Recherche automatisée et non ambiguë de noms et d'adresses électroniques	AC : matériel digne de confiance (HSM)	HSM situé dans le centre de confiance de KEYNECTIS, niveau 5 de sécurité	Application K.WebSign® pour cosigner des documents CDS préalablement signés avec des plates-formes prises en charge
CDS Classe 2	<ul style="list-style-type: none"> ▪ Recherche non ambiguë de noms, contacts et adresses électroniques ; envoi par e-mail de documents ou de registres commerciaux pour des organisations, n° de SIREN, K-bis, etc. ▪ Confirmation des informations d'enregistrement par appel téléphonique ou contrôle de certificat PrisV1 ou PrisV2 	AC : matériel digne de confiance (HSM)	Matériel cryptographique requis FIPS 140-1 niveau 2	Signature CDS au moyen de plates-formes prises en charge
CDS Classe 3	<ul style="list-style-type: none"> ▪ Recherche non ambiguë de noms, contacts, adresses physiques et envoi par e-mail de documents ou de registres commerciaux pour des organisations, n° de SIREN, K-bis, etc. ▪ Confirmation des informations d'enregistrement par appel téléphonique ▪ Délivrance en face à face en personne ou à représentant 	AC : matériel digne de confiance (HSM)	Matériel cryptographique requis. Certifié FIPS 140-1 niveau 2 ou supérieur	Signature CDS au moyen de plates-formes prises en charge,



	administrateur /mandataire			
UH CDS	<ul style="list-style-type: none"> ▪ Procédure de génération des clés de KEYNECTIS 	AC : matériel digne de confiance (MSM)	Matériel cryptographique requis. FIPS 140-1 niveau 2	Application K.Stamp® de KEYNECTIS

4.3.3 Confirmation par des tiers des informations d'une entreprise

Lorsque c'est nécessaire (certificats de classe 2 et de classe 3), un tiers désigné dans l'accord d'abonnement confirme la raison sociale, l'adresse et d'autres coordonnées de la société, en les comparant à sa base de données et en consultant les organismes officiels appropriés. La confirmation des informations relatives à des sociétés et à des banques nécessite certaines procédures personnalisées (et éventuellement localisées) axées sur des critères juridiques (tels que la preuve de l'inscription au Registre du Commerce). Le tiers communique également des numéros de téléphone utilisés pour des communications hors bande avec la société, afin de confirmer certaines informations (par exemple, pour vérifier la fonction d'un agent au sein de la société ou pour confirmer que la personne figurant dans la demande est bien le demandeur). Si la base de données ne contient pas la totalité des informations requises, le tiers peut conduire une enquête à la demande de l'AC ou le demandeur de certificat peut être invité à fournir des informations et des preuves complémentaires.

4.3.4 Confirmation de l'adresse postale

Lors de la délivrance des certificats de classe 2 & 3, l'AC envoie un courrier de confirmation ou de livraison (courrier postal recommandé pour classe 2 avec accusé de réception pour classe 3 (Postal ou porteur)) à l'adresse postale indiquée dans la demande de certificat et confirmée au moyen de bases de données tierces. Cette procédure de confirmation fournit une preuve supplémentaire garantissant que le demandeur est celui qu'il prétend être et que l'adresse indiquée dans la demande de certificat est correcte. En France, le service postal dénommé « lettre recommandée avec accusé de réception » ainsi que les sociétés dites de porteurs Physiques (DHL etc..) garantissent l'identité de l'organisation

4.3.5 Confirmation du détenteur d'un certificat français PRIS V1 ou PRIS V2

Au cours de la procédure de validation d'un certificat CDS de classe 2, une procédure simplifiée pour la vérification d'identité par un tiers repose sur la vérification de la signature électronique d'un document, au moyen de ce certificat.

4.4 Exigences en matière de demande d'un certificat CDS de classe 1

4.4.1 Inscription de l'organisation

Avant la délivrance d'un certificat CDS de classe 1, l'organisation chargée d'identifier le demandeur doit être en possession d'un certificat de classe 3 pour cette organisation et doit avoir souscrit un contrat de licence K.WebSign. L'organisation exerce la fonction d'AE dans le modèle de délivrance de certificat CDS de classe 1.

4.4.2 Enregistrement des demandeurs

Il appartient à l'organisation de déterminer et de vérifier les informations requises pour générer le contenu du DN. Toutes les informations doivent être complètes et seront transmises à l'aide de données signées et chiffrées constituant un moyen pour l'AC KEYNECTIS-CDS ou la Sous-AC de vérifier l'identité de l'organisation et l'intégrité des informations.



4.4.3 Informations de certification

Voir section 7.

4.4.4 Procédure de traitement des demandes de certificat

La plate-forme K.WebSign de KEYNECTIS reçoit en provenance de l'organisation les informations d'un demandeur en ligne, ainsi qu'un document CDS PDF. La plate-forme K.WebSign vérifie les points suivants :

- l'état complet et l'intégrité de la demande ;
- la validité de la signature CDS du document.

La plate-forme K.WebSign génère ensuite une paire de clés, à l'intérieur du Bunker d'opérations hautement sécurisées, au moyen d'un dispositif cryptographique certifié FIPS 140-1 niveau 2, crée une DSC comprenant un DN avec une référence unique du document CDS reçu (TransNUM) et l'envoi à l'AC KEYNECTIS-CDS, à l'aide de données XML signées et chiffrées.

4.5 Délivrance d'un certificat CDS de classe 1

À la réception d'une demande issue de la plate-forme K.WebSign, l'AC KEYNECTIS-CDS délivre un certificat CDS de classe 1 comprenant des informations uniques (identité et TransNUM) dans le ND.

4.6 Acceptation d'un certificat CDS de classe 1

Une fois que le demandeur a reçu et approuvé le certificat CDS, la plate-forme K.WebSign ajoute une signature d'approbation au document CDS et l'archive pour une durée d'au moins trois ans.

4.7 Suspension et révocation d'un certificat CDS de classe 1

En raison du cycle de vie court du certificat CDS de classe 1, aucun processus de révocation n'est stipulé.

4.7.1 Motifs d'une révocation

Aucune disposition.

4.7.2 Origine de la demande de révocation

Aucune disposition.

4.7.3 Procédure de demande de révocation

Aucune disposition.

4.7.4 Période de grâce d'une demande de révocation

Aucune disposition.

4.7.5 Motifs d'une suspension

Aucune disposition.

4.7.6 Origine de la demande de suspension

Aucune disposition.



4.7.7 Procédure d'une demande de suspension

Aucune disposition.

4.7.8 Limites relatives à la période de suspension

Aucune disposition.

4.7.9 Fréquence de publication des LCR

Afin de permettre à toute partie utilisatrice de vérifier la validité d'un certificat, les LCR font l'objet d'une publication quotidienne, avec une période de validité de sept jours.

4.7.10 Exigence de contrôle des AR/LCR

Les parties utilisatrices doivent récupérer les AR/LCR au moins toutes les 24 heures, avant de faire confiance à un document signé à l'aide d'un identifiant numérique CDS, excepté pour les identifiants numériques CDS délivrés aux fins des services d'horodatage.

4.7.11 Contrôle en ligne du statut de révocation

L'OCSP est un protocole permettant d'obtenir des renseignements opportuns au sujet du statut de révocation d'un certificat CDS, lorsque la signature et/ou la validation en ligne sont effectuées via certains produits Adobe. Les demandes OCSP contiennent les données suivantes :

- la version du protocole ;
- la demande de service ;
- l'identifiant du certificat cible.

Si un certificat CDS contient une extension OCSP, certains produits Adobe peuvent établir une demande OCSP en utilisant l'OID : 1.2.840.113583.1.1.9.2 qui est contenu dans le certificat CDS.

4.7.12 Exigences de vérification en ligne des révocations

Le message de réponse OCSP définitif comprend les données suivantes :

- la version de la syntaxe de réponse ;
- le nom de l'appelé ;
- les réponses à chacun des certificats d'une demande ;
- la signature calculée par hachage de la réponse.

L'adresse de l'appelé OCSP est précisé dans le certificat. Le certificat utilisé pour signer la réponse OCSP est délivré par l'AC KEYNECTIS-CDS ou une AC subordonnée.

Lorsque l'AC retourne un message d'erreur en réponse à une demande de statut de certificat, le message d'erreur n'est pas signé numériquement.

4.7.13 Autres moyens disponibles d'information sur les révocations

Aucune disposition.

4.7.14 Exigences de vérification d'autres moyens d'information sur les révocations

Aucune disposition.

4.7.15 Exigences spécifiques en cas de compromission de la clé

En cas de compromission de la clé privée de l'AC KEYNECTIS-CDS, utilisée pour signer un certificat CDS, KEYNECTIS informera par e-mail, dans les plus brefs délais possibles, tous les abonnés en possession de



certificats CDS délivrés à partir de cette clé privée, que les certificats CDS seront révoqués le jour ouvrable suivant et que cette révocation et sa publication dans la LCR appropriée vaudront notification à l'abonné de la révocation de son certificat CDS.

4.8 Exigences en matière de demande d'un certificat CDS de classe 2

Le processus suivant s'applique aux demandeurs sollicitant des certificats CDS de classe 2, en vue d'une utilisation dans leur rôle pour le compte de l'organisation, soit à titre individuel, soit en rapport avec une fonction assurée par un serveur.

4.8.1 Inscription d'une personne représentant une organisation (Mandataire)

Avant que tout demandeur affilié à une organisation puisse demander un certificat CDS, l'organisation doit avoir souscrit un contrat de services CDS (Bon de commande). Le représentant de l'organisation, agissant pour le compte de cette dernière, doit remplir à cet effet un formulaire d'inscription auprès de KEYNECTIS-CDS, sous un format prescrit par KEYNECTIS. Tous les formulaires d'inscription sont soumis à l'examen, à l'approbation et à l'acceptation de KEYNECTIS.

Le service client de KEYNECTIS-CDS procède aux vérifications suivantes :

- établissement de l'identité de l'organisation (contrat commercial et Inscription au registre du commerce (France) ou auprès d'un organisme tiers international DUNS) ;
- confirmation du droit de la future AE de représenter la société, via la soumission d'une déclaration de preuve de droit signé par un représentant autorisé de l'organisation, ou par utilisation de signature électronique via le portail spécifique de signature de KEYNECTIS

4.8.2 Enregistrement de demandeurs appartenant à une organisation ou représentant l'Organisation

Les demandeurs de certificats individuels ou organisation au sein de l'organisation doivent remplir un formulaire KEYNECTIS qui sera validé par l'AE autorisée de l'organisation, via la signature électronique du document en format PDF. Les demandeurs peuvent demander un certificat pour usage Personnel (Clef USB) ou serveur dans la mesure où les bibles sont générés sur HSM fips 140-1 level 02.

Le mandataire désigné (titulaire d'un certificat CDS de classe 2 ou 3 ou d'un niveau équivalent d'une AC accepté par Keynectis) pour le compte de l'organisation exécutera les étapes de vérification au sein de l'organisation, afin de valider l'habilitation du demandeur à solliciter un certificat CDS ou vérifiera l'exactitude des informations contenues dans la demande de certificat CDS ou s'assurera par ailleurs de l'absence d'erreurs ou d'omissions. L'AE désignée procède ensuite à une signature CDS de la demande et la télécharge vers KEYNECTIS.

Le suivi de la demande de certificat doit être effectué par l'AE, au moyen d'un document signé CDS.

4.8.3 Inscription d'une personne appartenant à une petite organisation (individuelle)

Les informations à fournir sont celles qui sont envoyées dans le fichier de demande de certificat. Une petite organisation est une structure de travail indépendant et le processus de vérification peut se fonder sur des informations officielles disponibles dans la base de données du Registre du Commerce en France.

La demande de certificat s'effectue en trois étapes :

- Étape 1 : Le demandeur transmet le fichier de demande de certificat et envoie par la poste la pièce d'identité officielle ci-dessous.
- Étape 2 : Les documents et le fichier de demande reçus sont validés par l'AE de KEYNECTIS-CDS.
- Étape 3 : L'abonné retire le certificat.

L'AE de KEYNECTIS ne traitera les demandes de certificat que si elles sont soumises sous la forme d'un fichier de demande de certificat, accompagné de tous les justificatifs d'identité suivants :

Document 1 : lettre signée du représentant de l'organisation. Il s'agit de la demande écrite (et signée) du représentant légal. Cette lettre désigne la personne à laquelle le certificat sera délivré. La lettre doit comporter :



- la cosignature d'acceptation de la personne destinataire (demandeur) ou mandataire,;
- l'adresse électronique du représentant pour l'informer de la révocation du certificat.

Document 2 : extrait de K-bis de la société. Le document original envoyé doit être daté de moins de trois mois et doit mentionner le numéro de SIREN et l'adresse de la société (Optionnel en France).

Document 3 : un justificatif d'identité du demandeur autorisé. Les justificatifs d'identité de la personne autorisée prennent la forme de copies conformes selon les règles de la législation française ou européenne relatives aux copies certifiées conformes. En France, une copie conforme est à choisir parmi les quatre justificatifs suivants : extrait de K-bis, photocopie de la carte nationale d'identité, photocopie du passeport ou du permis de conduire.

Document 4 : lettre (Formulaie) du demandeur autorisé. La lettre de la personne autorisée doit contenir les informations suivantes :

- le numéro de téléphone professionnel ;
- le numéro de téléphone mobile (personnel ou professionnel) ;
- le code personnel de retrait et de révocation (ci-après dénommé « code de révocation et de retrait ») ;
- l'adresse électronique ;
- la déclaration d'acceptation des conditions générales de vente et des obligations stipulées par l'AC.

Document 5 : bon de commande et mode de paiement. Ce document est établi par l'organisation du demandeur aux fins de la délivrance d'un ou de plusieurs certificats, et indique le mode de paiement souhaité (un chèque rempli et signé sera joint si nécessaire).

L'AE de KEYNECTIS-CDS doit procéder aux vérifications suivantes :

- établir l'identité du futur abonné (sur la base de la validation du document 3) ;
- vérifier le droit du futur abonné de représenter la société (sur la base du document 1) ;
- confirmer la relation entre la clé publique à certifier et le futur abonné ;
- s'assurer que le futur abonné a eu connaissance des termes et conditions d'utilisation du certificat (entretien téléphonique avec le demandeur et le représentant légal).

4.8.4 Enregistrement des demandeurs

L'AE de KEYNECTIS-CDS exécute les étapes d'authentification énumérées ci-dessous (et s'assure, d'une manière générale, de l'absence d'erreurs et d'omissions se rapportant aux étapes d'authentification).

KEYNECTIS ne fera figurer aucun nom individuel sur un certificat CDS de petite organisation, sans avoir vérifié premièrement la concordance entre le nom de la personne, le pays et la localité mentionnés sur le formulaire d'inscription et ceux de l'identification, et deuxièmement la validité de l'identification de la petite organisation.

Afin d'éviter les erreurs et la délivrance frauduleuse de certificats, le processus repose sur le principe de « séparation des tâches ». La personne qui vérifie le document établissant l'identité de l'organisation ne peut pas vérifier l'identité du demandeur par téléphone et vice-versa.

Le processus fonctionne donc sur la base d'un « binôme » (personne n° 1 / personne n° 2) qui se répartit les tâches de la manière suivante :

- validation de la réception du bon de commande et du formulaire (personne n° 1) ;
- vérification de l'existence de la société et de ses coordonnées (personne n° 1) ;
- vérification du numéro de téléphone (personne n° 2).

Pour ce qui concerne le nom de l'organisation, l'objectif est de vérifier que :

- l'organisation existe bien (d'après son numéro de SIREN ou son numéro de DUNS pour les sociétés implantées à l'étranger).

Pour les sociétés françaises, le nom de l'organisation peut être vérifié sur des sites officiels tels que www.dnb.com.



S'il ressort de la vérification sur les sites de référence que le numéro de SIREN (ou de DUNS pour les sociétés établies hors du territoire français) correspond à l'O (Organisation) figurant sur la demande, le service client peut valider cette étape et poursuivre la vérification.

Si, au contraire, le numéro de SIREN ou de DUNS ne correspond pas à l'organisation, le service client doit demander au client de lui fournir ce que l'on appelle un « Document de Preuve de Droit » - document officiel prouvant l'existence de la société (par exemple, extrait de K-bis, Journal Officiel, etc.).

Ce document doit comporter impérativement :

- le nom de l'organisation ;
- sa marque officielle (cachet, logo, etc.) ;
- son numéro de société (ou d'enregistrement) ;
- le nom du service ayant émis le document ;
- la signature de l'agent administratif ayant émis le document.

La procédure de vérification téléphonique permet de s'assurer :

- que la personne travaille bien pour la société qui a fait la demande ;
- qu'elle a connaissance de la demande ;
- qu'elle confirme les adresses électroniques ;
- qu'elle est autorisée à demander un certificat, à le recevoir et à l'installer.

Le numéro de téléphone peut être vérifié sur des sites officiels (opérateur français et annuaire public pour le téléphone filaire) ou via les renseignements téléphoniques.

Lorsque le numéro de téléphone spécifié est celui d'un téléphone portable : le contact du demandeur doit fournir la preuve légale qu'il existe un lien entre lui-même et l'organisation mentionnée sur le document 1 cosigné par le représentant de l'organisation).

Lors de l'entretien téléphonique, le service client pose un certain nombre de questions visant à valider le bien-fondé de la demande établie en ligne :

- Si le service client obtient la totalité des réponses, il valide cette étape de vérification et délivre le certificat.
- Si certaines des informations sont manquantes, le client doit corriger sa demande.

Le demandeur est déjà titulaire d'un certificat PrisV1 ou PrisV2 ou RGS 2*

Le gouvernement français a déjà accrédité et référencé des AC pour la délivrance de certificats conformément aux protocoles PrisV1 ou PrisV2. Si le demandeur est titulaire d'un tel certificat, il fera l'objet d'un processus de vérification simplifié, sur la base de la validation du certificat utilisé au moment de la transmission de la demande. Dans ce cas, le CN du certificat CDS sera identique au CN sous PrisV1 ou PrisV2.

4.8.5 Informations de certification

Voir section 7.

4.8.6 Procédure de traitement des demandes de certificats

Le demandeur se connecte au site Web public de KEYNECTIS-CDS et remplit un formulaire de demande puis procède à la signature de la demande.

Les AE de KEYNECTIS-CDS ou l'AE Déléguée sont avisées de la demande et exécutent les étapes de validation décrites dans la section précédente.

L'AE de KEYNECTIS-CDS ou l'AE Déléguée se connecte à un site d'administrateur au moyen d'un certificat individuel délivré par une AC KEYNECTIS différente (contrôle d'accès et de rôle) et peut accepter la demande ou la rejeter si elle ne passe pas le processus de vérification avec succès. À l'issue de la validation, un e-mail est envoyé au demandeur, en vue de la délivrance du certificat.

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



4.9 Délivrance d'un certificat CDS de classe 2

Si l'AE KEYNECTIS constate que le formulaire d'inscription du certificat CDS du demandeur a été vérifié, le certificat du demandeur est signé par la Sous-AC KEYNECTIS-CDS.

Pour délivrer le certificat CDS pour une personne Physique (Personnel ou représentant une Organisation, KEYNECTIS génère une paire de clés publique et privée au moyen d'un dispositif HSM Fips 140-1 level 02 (minimum) de type cle USB.

Pour délivrer le certificat CDS pour une machine représentant une Organisation, les documents relatifs à la clé publique (CSR) seront envoyés à KEYNECTIS pour signature et le certificat CDS du demandeur sera signé par KEYNECTIS et renvoyé au demandeur.

Le demandeur peut utiliser son propre dispositif cryptographique approuvé et certifié FIPS 140-1 niveau 2 ou, s'il n'en possède pas encore, peut en acquérir un auprès de KEYNECTIS.

Si le demandeur ou l'organisation agissant pour le compte du demandeur se procure un dispositif matériel approuvé **auprès de KEYNECTIS**, le demandeur aura la possibilité de demander à KEYNECTIS de générer une paire de clés publique et privée sur le dispositif matériel approuvé, dans les locaux de KEYNECTIS et de fournir à l'abonné le dispositif matériel approuvé contenant le certificat. Dans ce cas, le dispositif matériel approuvé sera envoyé à l'abonné par la poste, via un autre service de livraison, par coursier ou au moyen d'un autre mode de remise en main propre et pourra nécessiter une signature à la livraison. KEYNECTIS doit recueillir et conserver tous les récépissés de livraison. Dans certaines circonstances, le numéro de téléphone du représentant du service client de KEYNECTIS et son adresse électronique peuvent être communiqués au client au moment de la livraison, pour tout problème technique ou relevant du service client. KEYNECTIS peut, à sa seule discrétion, fournir cette assistance technique ou commerciale aux demandeurs/abonnés.

4.10 Acceptation d'un certificat CDS de classe 2

Le demandeur peut expressément signifier l'acceptation d'un certificat CDS en utilisant ce certificat.

4.11 Suspension et révocation d'un certificat CDS de classe 2

Le processus de révocation marque la fin anticipée de la période d'utilisation d'un certificat CDS.

4.11.1 Causes de révocation

Un certificat CDS de classe 2 doit être révoqué et son numéro de série doit être inscrit sur une liste de certificats révoqués (LCR), si l'une des circonstances suivantes est identifiée :

- les informations de l'abonné figurant dans son certificat ont changé, avant l'expiration « normale » du certificat ;
- les règles d'utilisation du certificat ne sont pas respectées ;
- la clé privée de l'abonné est suspectée de compromission, de perte ou de vol ;
- l'organisation a demandé la révocation, au moyen du code de révocation ;
- le certificat de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats signés par la clé privée correspondante) ;
- l'organisation a cessé son activité.

4.11.2 Origine de la demande de révocation

Les seules entités habilitées à demander une révocation ou à révoquer un certificat CDS délivré par KEYNECTIS sont :

- le représentant de l'organisation ou le mandataire ;
- l'Autorité d'Enregistrement ;
- KEYNECTIS et l'Autorité de Politique d'Adobe.



4.11.3 Procédure de traitement de la demande de révocation

Le représentant de l'organisation émet la demande de révocation :

- en utilisant le code de révocation utilisé au moment de l'inscription ou
- en contactant l'AE de KEYNECTIS-CDS, par e-mail, service postal national/régional, télécopie ou service de messagerie de 24 heures, pour demander la révocation du certificat CDS, en motivant sa demande.

À la réception d'une demande de révocation, KEYNECTIS doit aviser le représentant de l'organisation de la demande, par e-mail. KEYNECTIS adressera un e-mail à l'abonné pour obtenir confirmation de la demande. Ce message signalera que KEYNECTIS est sur le point de révoquer le certificat CDS et que la publication de la révocation dans la LCR appropriée vaudra notification à l'abonné et aux parties utilisatrices de la révocation du certificat CDS. Seul l'abonné recevra cette notification.

4.11.4 Période de grâce d'une demande de révocation

Il n'est accordé aucune période de grâce à l'abonné avant la révocation et KEYNECTIS procédera à la révocation du certificat CDS le jour ouvrable suivant, en annonçant la révocation dans la prochaine LCR publiée.

4.11.5 Causes de suspension

Il n'existe pas de suspension.

4.11.6 Origine de la demande de suspension

Aucune disposition.

4.11.7 Procédure de la demande de suspension

Aucune disposition.

4.11.8 Limites relatives à la période de suspension

Aucune disposition.

4.11.9 Fréquence de publication des LCR

Les LCR font l'objet d'une publication quotidienne, avec une période de validité de sept jours.

4.11.10 Exigence de contrôle des AR/LCR

Les parties utilisatrices doivent récupérer les LAR/LCR au moins toutes les 24 heures, avant de faire confiance à un document signé à l'aide d'un identifiant numérique CDS, excepté pour les identifiants numériques CDS délivrés aux fins des services d'horodatage.

4.11.11 Contrôle en ligne du statut de révocation

L'OCSP est un protocole permettant d'obtenir des renseignements opportuns au sujet du statut de révocation d'un certificat CDS, lorsque la signature et/ou la validation en ligne sont effectuées via certains produits Adobe. Les demandes OCSP contiennent les données suivantes :

- la version du protocole ;
- la demande de service ;
- l'identifiant du certificat cible ;

Si un certificat CDS contient une extension OCSP, certains produits Adobe peuvent établir une demande OCSP en utilisant l'OID : 1.2.840.113583.1.1.9.2 qui est contenu dans le certificat CDS.



4.11.12 Exigences de vérification en ligne des révocations

Le message de réponse OCSP définitif comprend les données suivantes :

- la version de la syntaxe de réponse ;
- le nom de l'appelé ;
- les réponses à chacun des certificats d'une demande ;
- la signature calculée par hachage de la réponse.

L'adresse de l'appelé OCSP est URL = <http://k-valid.keynectis.com/ds-server/process>. Le certificat utilisé pour signer la réponse OCSP est délivré par l'AC KEYNECTIS-CDS ou une AC subordonnée.

Lorsque l'AC retourne un message d'erreur en réponse à une demande de statut de certificat, le message d'erreur n'est pas signé numériquement.

4.11.13 Autres moyens disponibles d'information sur les révocations

Aucune disposition.

4.11.14 Exigences de vérification d'autres moyens d'information sur les révocations

Aucune disposition.

4.11.15 Exigences spécifiques en cas de compromission de la clé

En cas de compromission de la clé privée de l'AC KEYNECTIS-CDS, utilisée pour signer un certificat CDS, KEYNECTIS informera par e-mail, dans les plus brefs délais possibles, tous les abonnés en possession de certificats CDS délivrés à partir de cette clé privée, que les certificats CDS seront révoqués le jour ouvrable suivant et que la publication de cette révocation dans la LCR appropriée vaudra notification aux abonnés de la révocation de leur certificat CDS.

4.12 Exigences en matière de demande d'un certificat CDS de classe 3

Les certificats CDS de classe 3 sont délivrés lorsque les demandeurs sont des organisations obtenant et gérant une identité numérique pour le compte d'un abonné individuel (en ayant un rôle d'AE vis-à-vis de celui-ci) et pour le compte de l'organisation elle-même, afin de l'utiliser sur un serveur. Les certificats CDS de classe 3 sont délivrés lors d'un processus **en face à face** entre l'AE de KEYNECTIS et l'organisation ou son représentant.

4.12.1 Inscription

Le représentant de l'organisation remet tous les documents d'identité à l'AE de KEYNECTIS qui vérifie la validité de l'identité de l'organisation, auprès du Registre du Commerce et/ou de la base de données Dun and Bradstreet. Le représentant de l'organisation, agissant pour le compte de celle-ci, remplit un formulaire d'inscription de certificat KEYNECTIS-CDS, sous un format prescrit par KEYNECTIS. Tous les formulaires d'inscription sont soumis à l'examen, à l'approbation et à l'acceptation de KEYNECTIS. Les formulaires d'inscription spécifient le module matériel cryptographique utilisé pour la génération de la paire de clés.

4.12.2 Enregistrement des demandeurs

KEYNECTIS demande tout d'abord les justificatifs d'identité suivants :

Document 1 : lettre de l'organisation. Il s'agit de la demande écrite (et signée) de l'abonné. Cette lettre désigne la personne (AE ou contact technique pour le serveur) à laquelle le certificat doit être délivré. La lettre doit comporter :

- la cosignature d'acceptation de la personne destinataire (futur abonné) ;



- un code de révocation (composé d'une chaîne alphanumérique) connu du représentant de la société, afin que celui-ci puisse révoquer le certificat du demandeur, lorsque le mandat n'a plus cours ou pour une raison quelconque ;
- l'adresse électronique du client s'il souhaite être informé de la révocation du certificat.

Document 2 : extrait de K-bis de la société. Le document original envoyé doit être daté de moins de trois mois et doit mentionner le numéro de SIREN et l'adresse de la société.

Document 3 : lettre d'autorisation pour le certificat d'enregistrement de l'AE. La lettre d'autorisation est signée par un représentant de l'organisation et comporte : les noms d'AE et le titre ou nom du contact technique (serveur), ainsi qu'une déclaration attestant que les demandeurs désignés sont des membres de l'organisation et sont autorisés à demander un certificat CDS pour l'AE ou à l'usage du serveur.

Document 4 : lettre de l'AE du demandeur (ou du contact technique). La lettre de l'intéressé doit comporter les informations suivantes :

- le numéro de téléphone professionnel ;
- le numéro de téléphone mobile (personnel ou professionnel) ;
- le code personnel de retrait et de révocation (ci-après dénommé « code de révocation et de retrait ») ;
- l'adresse électronique ;
- la déclaration d'acceptation des conditions générales de vente et des obligations stipulées par l'AC.

Document 5 : bon de commande et Mode de paiement. Ce document est établi par la société aux fins de la délivrance d'un ou de plusieurs certificats, et indique le mode de paiement souhaité (un chèque rempli et signé sera joint si nécessaire).

L'AE de KEYNECTIS doit procéder aux vérifications suivantes :

- établir l'identité du futur abonné et de l'organisation ;
- confirmer le droit du futur abonné de représenter la société ;
- confirmer la relation entre la clé publique à certifier et le futur abonné ;
- s'assurer que le futur abonné a eu connaissance des termes et conditions d'utilisation du certificat.

4.12.3 Procédure d'enregistrement de certificats CDS de classe 3

La demande de certificat CDS de classe 3 doit contenir les informations suivantes :

- identification personnelle du contact technique : nom, prénom, adresse électronique, fonction, adresse postale complète, numéros de téléphone (standard et ligne directe) ;
- identification de l'organisation : nom, prénoms et statut juridique, ainsi que d'autres informations nécessaires à l'enregistrement (par exemple, le numéro de SIREN de la société) ;
- clé publique selon la norme PKCS#10 ;
- période de validité du certificat ;
- informations « secrètes » du client pour le processus d'authentification lors de la vérification d'identité (fourniture d'un couple de question-réponse) ou utilisation d'échange cryptés par des certificats ou secrets partagés.

Avant la délivrance d'un certificat d'AE ou de serveur et l'indication du nom de l'organisation sur un certificat CDS destiné à l'organisation, KEYNECTIS vérifie la validité de l'identification de l'organisation.

Afin d'éviter les erreurs et la délivrance frauduleuse de certificats, le processus repose sur le principe de « séparation des tâches ». La personne qui procède à l'authentification ne peut pas procéder à la vérification et vice-versa.

Le processus fonctionne donc sur la base d'un « binôme » (personne n° 1 / personne n° 2) qui se répartit les tâches de la manière suivante :

- validation de la réception du bon de commande et du formulaire (personne n° 1) ;



- vérification de l'existence de la société et de ses coordonnées (personne n° 1) ;
- vérification du numéro de téléphone du demandeur de l'AE ou du serveur (personne n° 2) ;

Pour le module cryptographique matériel, la vérification porte sur la conformité du module à la norme FIPS 140-1 niveau 2.

Pour ce qui concerne le nom de l'organisation, l'objectif est de vérifier que : l'organisation existe bien (d'après son numéro de SIREN ou son numéro de DUNS pour les sociétés implantées à l'étranger).

Pour les sociétés françaises, le nom de l'organisation peut être vérifié sur des sites officiels, tels que : www.dnb.com.

S'il ressort de la vérification sur les sites de référence que le numéro de SIREN (ou de DUNS pour les sociétés établies hors du territoire français) correspond à l'O (Organisation) figurant sur la demande, le service client peut valider cette étape et poursuivre la vérification.

Si, au contraire, le numéro de SIREN ou de DUNS ne correspond pas à l'organisation, le service client doit demander au client de lui fournir ce que l'on appelle un « Document de Preuve de Droit » - document officiel prouvant l'existence de la société (par exemple, extrait de K-bis, Journal Officiel, etc.).

Ce document doit comporter impérativement :

- le nom de l'organisation ;
 - sa marque officielle (cachet, logo, etc.) ;
 - son numéro de société (ou d'enregistrement) ;
 - le nom du service ayant émis le document ;
 - la signature de l'agent administratif ayant émis le document.
- La vérification en face à face permet d'établir la preuve de l'identité du demandeur ou du contact technique.

4.12.4 Confirmation des contrôles d'exportation

En complément des vérifications effectuées pour les certificats de classe 3, KEYNECTIS doit procéder aux contrôles suivants pour délivrer des certificats de contrôle d'exportation à installer sur un serveur.

KEYNECTIS invitera le demandeur de certificat à indiquer le pays dans lequel le serveur sera installé. Cette information fournie par le demandeur dans le cadre de l'accord d'abonnement garantit que le serveur sera installé dans le pays indiqué.

Si le demandeur de certificat garantit que le serveur doit être installé en France, KEYNECTIS doit s'assurer que le champ « Country » (pays) inclus dans la demande de certificat contient bien la valeur « FR » (norme ISO). KEYNECTIS doit vérifier auprès d'une base de données tierce que l'entité mentionnée dans le champ « Contact Information » (informations sur le contact) est située en France. KEYNECTIS doit s'assurer, en outre, que le code d'activité mentionné dans la demande de certificat identifie le demandeur de certificat comme étant une banque, une institution financière, une compagnie d'assurance ou un organisme médical ou de santé. Dans le cas contraire, le demandeur de certificat doit fournir les justificatifs l'autorisant à exercer les activités d'une banque, d'une institution financière, d'une compagnie d'assurance ou d'un organisme médical ou de santé.

4.12.5 Informations de certification

Voir section 7.



4.12.6 Procédure de traitement des demandes de certificats

Le demandeur ou son représentant Administrateur AE porteur d'un certificat se connecte au site Web public de KEYNECTIS-CDS télécharge ou remplit un formulaire de demande. Si la demande concerne le serveur d'une organisation, la DSC (PKCS#10) sera transmise en même temps que les informations se rapportant au module matériel utilisé et à sa conformité à la norme FIPS 140-1 niveau 2 ou supérieur.

Les AE de KEYNECTIS-CDS sont avisées de la demande et exécutent les étapes de validation décrites dans la section précédente.

L'AE de KEYNECTIS-CDS se connecte à un site d'administrateur au moyen d'un certificat individuel délivré par une AC KEYNECTIS spécifique (contrôle d'accès et de rôle) et peut accepter la demande ou la rejeter si elle ne passe pas le processus de vérification avec succès. À l'issue de la validation, un e-mail est envoyé au demandeur, en vue de la délivrance du certificat dans le cadre d'un processus en face à face.

4.13 Délivrance d'un certificat CDS de classe 3

Si KEYNECTIS constate que le formulaire d'inscription du certificat CDS du demandeur a été vérifié, le certificat du demandeur est signé par la Sous-AC KEYNECTIS-CDS. KEYNECTIS doit délivrer le certificat CDS en procédant de la manière suivante :

- en appelant le navigateur Web du demandeur, afin de générer une paire de clés publique et privée au moyen d'un dispositif matériel approuvé, tout en soumettant à des restrictions les modules de prestataires de services cryptographiques disponibles (« PSC ») qui permettent au demandeur de générer une paire de clés ;
- en copiant une CSR (PKCS#10) contenant la clé publique.

La délivrance fait l'objet d'une procédure en face à face avec l'AE ou le contact technique du demandeur, en présence du personnel de KEYNECTIS (le lieu géographique de la rencontre peut être le site du demandeur ou celui de KEYNECTIS).

4.14 Acceptation d'un certificat CDS de classe 3

Le demandeur signifie expressément son acceptation d'un certificat CDS en utilisant ce dernier et en signant l'accord d'abonnement.

4.15 Suspension et révocation d'un certificat CDS de classe 3

Le processus de révocation marque la fin anticipée de la période d'utilisation d'un certificat CDS.

4.15.1 Causes de révocation

Un certificat CDS de classe 3 doit être révoqué et son numéro de série doit être inscrit sur une liste de certificats révoqués (LCR), si l'une des circonstances suivantes est identifiée :

- les informations de l'abonné figurant dans son certificat ont changé, avant l'expiration « normale » du certificat ;
- les règles d'utilisation du certificat ne sont pas respectées ;
- la clé privée de l'abonné est suspectée de compromission, de perte ou de vol ;
- l'abonné en fait lui-même la demande ;
- le certificat de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats signés par la clé privée correspondante) ;
- l'organisation a cessé son activité ;
- une modification de longueur de clé ou d'algorithme (signature et/ou hachage) est demandée à la suite d'une recommandation d'une organisation nationale ou internationale appropriée ;
- du fait de la modification du nom de l'organisation, le contact technique n'est plus autorisé à utiliser le nom de domaine ;
- le ND figurant sur le certificat est erroné ;
- le contact technique a utilisé un ND erroné dans la demande initiale ;
- la fin de la relation entre l'AC et le client.



4.15.2 Origine de la demande de révocation

Les seules entités habilitées à demander une révocation ou à révoquer un certificat CDS délivré par KEYNECTIS sont :

- le représentant de l'organisation ;
- le contact technique ;
- l'Autorité d'Enregistrement ;
- KEYNECTIS et l'Autorité de Politique d'Adobe.

4.15.3 Procédure et traitement d'une demande de révocation de certificat en ligne

Le service en ligne est mis à la disposition du demandeur 24 heures sur 24 et sept jours sur sept pour lui permettre de révoquer son certificat dans les meilleurs délais. Les abonnés se connectent au site de l'AC et peuvent révoquer leur certificat en spécifiant leur adresse électronique et le code de retrait et de révocation qui leur a été communiqué au moment de la signature d'une révocation. Les demandes doivent contenir des informations d'identification du certificat et de son titulaire.

4.15.4 Procédure et traitement d'une demande de révocation de certificat hors ligne

Le service hors ligne est mis à la disposition des abonnés ou de leur représentant, tous les jours ouvrés, de 9h à 17h. La révocation se fait à l'aide du code de retrait et de révocation de l'abonné ou du code de révocation du représentant.

Le contact technique ou l'AE envoie une demande de révocation à l'AE de KEYNECTIS-CDS, en indiquant au moins les informations suivantes :

- son identification personnelle ;
- les données « secrètes » qu'il a envoyées lors de la demande du certificat qu'il souhaite révoquer.

L'AE de KEYNECTIS-CDS authentifie la demande de révocation autorisée et la transmet à l'AC. L'AC authentifie l'AE et révoque le certificat en activant sa clé de signature privée.

À des fins de protection, les informations émanant de l'AE sont envoyées à l'AC via une ligne sécurisée. Toutes les opérations de révocation de certificats sont protégées de façon à garantir l'intégrité, la confidentialité (si nécessaire) et l'origine des données envoyées et traitées.

Le contact technique est avisé du changement d'état de validité de son certificat. Une fois révoqué, le certificat n'est pas re-certifié.

4.15.5 Période de grâce d'une demande de révocation

Il n'est accordé aucune période de grâce à l'abonné avant la révocation et KEYNECTIS procédera à la révocation du certificat CDS le jour ouvrable suivant, en annonçant la révocation dans la prochaine LCR publiée.

4.15.6 Causes de suspension

Il n'existe pas de suspension.

4.15.7 Origine de la demande de suspension

Aucune disposition.

4.15.8 Procédure de la demande de suspension

Aucune disposition.



4.15.9 Limites relatives à la période de suspension

Aucune disposition.

4.15.10 Fréquence de publication des LCR

Les LCR font l'objet d'une publication quotidienne, avec une période de validité de sept jours.

4.15.11 Exigence de contrôle des AR/LCR

Les parties utilisatrices doivent récupérer les LAR/LCR au moins toutes les 24 heures, avant de faire confiance à un document signé à l'aide d'un identifiant numérique CDS, excepté pour les identifiants numériques CDS délivrés aux fins des services d'horodatage.

4.15.12 Vérification en ligne du statut de révocation

L'OCSP est un protocole permettant d'obtenir des renseignements opportuns au sujet du statut de révocation d'un certificat CDS, lorsque la signature et/ou la validation en ligne sont effectuées via certains produits Adobe. Les demandes OCSP contiennent les données suivantes :

- la version du protocole ;
- la demande de service ;
- l'identifiant du certificat cible.

Si un certificat CDS contient une extension OCSP, certains produits Adobe peuvent établir une demande OCSP en utilisant l'OID : 1.2.840.113583.1.1.9.2 qui est contenu dans le certificat CDS.

4.15.13 Exigences de vérification en ligne des révocations

Le message de réponse OCSP définitif comprend les données suivantes :

- la version de la syntaxe de réponse ;
- le nom de l'appelé ;
- les réponses à chacun des certificats d'une demande ;
- la signature calculée par hachage de la réponse.

L'adresse de l'appelé OCSP est URL = <http://k-valid.keynectis.com/ds-server/process>. Le certificat utilisé pour signer la réponse OCSP est délivré par la Sous-AC KEYNECTIS-CDS.

Lorsque l'AC retourne un message d'erreur en réponse à une demande de statut de certificat, le message d'erreur n'est pas signé numériquement.

4.15.14 Autres moyens disponibles d'information sur les révocations

Aucune disposition.

4.15.15 Exigences de vérification d'autres moyens d'information sur les révocations

Aucune disposition.

4.15.16 Exigences spécifiques en cas de compromission de la clé

En cas de compromission de la clé privée de l'AC KEYNECTIS-CDS, utilisée pour signer un certificat CDS, KEYNECTIS informera par e-mail, dans les plus brefs délais possibles, tous les abonnés en possession de certificats CDS délivrés à partir de cette clé privée, que les certificats CDS seront révoqués le jour ouvrable suivant et que la publication de cette révocation dans la LCR appropriée vaudra notification à l'abonné de la révocation de son certificat CDS.



4.16 Exigences en matière de demande de certificats CDS d'UH et d'AC subordonnée (Sous AC)

Les certificats CDS d'UH (Unité d'Horodatage) et d'AC fille ou AC subordonnée sont délivrés lors d'une procédure de génération des clés, à l'intérieur du Bunker de KEYNECTIS.

4.16.1 Inscription d'une organisation

Elle se déroule de la même manière que la création d'une AC, au moyen des éléments suivants :

- un document de nommage ;
- un script de procédure de génération des clés ;
- un témoin physique et l'authentification des détenteurs de parts de secret ;
- une notariation juridique.

4.16.2 Enregistrement des demandeurs

Au moyen du document de nommage et de la procédure de génération des clés.

4.16.3 Informations de certification

Non précisées

4.16.4 Procédure de traitement des demandes de certificat

Au cours de la procédure de génération des clés.

4.17 Délivrance d'un certificat CDS d'UH et de Sous-AC

La génération de paire de clés et la certification ont lieu dans la salle de sécurité de niveau 5, au moyen d'un ordinateur non connecté au réseau, d'un module cryptographique FIPS 140 niveau 3 (Eal4+), selon le principe de la part de secret M sur n, tel qu'expliqué à la section 6.

4.18 Acceptation d'un certificat CDS d'UH et de Sous-AC

Notariation juridique avec des témoins, à la fin de la procédure de génération des clés.

4.19 Suspension et révocation d'un certificat d'UH et de Sous-AC

Pendant leur cycle de vie, la paire de clés et le certificat sont stockés dans le Bunker hautement sécurisé de KEYNECTIS. L'accès à ces éléments et leur contrôle relèvent de la responsabilité de l'équipe régissant la politique de sécurité, ainsi qu'il est décrit à la section 5.

Le processus de révocation marque la fin anticipée de la période d'utilisation d'un certificat d'UH ou de Sous-AC.

4.19.1 Causes de révocation

Un certificat CDS d'UH ou de Sous-AC doit être révoqué et son numéro de série doit être inscrit sur une liste de certificats révoqués (LCR/LAR), si l'une des circonstances suivantes est identifiée :

- les règles d'utilisation du certificat ne sont pas respectées ;
- la clé privée est suspectée de compromission, de perte ou de vol ;
- le certificat de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats signés par la clé privée correspondante) ;
- l'organisation de KEYNECTIS a cessé son activité ;
- une modification de longueur de clé ou d'algorithme (signature et/ou hachage) est recommandée par une organisation nationale ou internationale appropriée ;
- la fin de la relation entre l'AC et le client.

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTIS_CDS_CA_FR_V1.2.doc



4.19.2 Origine de la demande de révocation

Les seules entités habilitées à demander une révocation ou à révoquer un certificat CDS d'UH ou de Sous-AC délivré par KEYNECTIS sont :

- le représentant de l'organisation ;
- l'Autorité d'Enregistrement ;
- KEYNECTIS et l'Autorité de Politique d'Adobe.

4.19.3 Procédure et traitement d'une demande de révocation de certificat

Au cours d'une procédure de génération de clés.

4.19.4 Période de grâce d'une demande de révocation

Il n'est accordé aucune période de grâce à l'abonné avant la révocation et KEYNECTIS procédera à la révocation du certificat CDS le jour ouvrable suivant, en annonçant la révocation dans la prochaine LCR publiée.

4.19.5 Causes de suspension

Il n'existe pas de suspension.

4.19.6 Origine de la demande de suspension

Aucune disposition.

4.19.7 Procédure de la demande de suspension

Aucune disposition.

4.19.8 Limites relatives à la période de suspension

Aucune disposition.

4.19.9 Fréquence de publication des LCR

Les LCR font l'objet d'une publication quotidienne, avec une période de validité de sept jours pour le certificat d'UH.

KEYNECTIS-CDS délivre des LAR systématiques pour la Sous-AC CDS une fois par an et des LCR au moins une fois par jour. En cas de révocation d'un identifiant numérique consécutive à une compromission de clé privée, la Sous-AC KEYNECTIS-CDS délivre une LAR/LCR mise à jour dans les 24 heures de la révocation.

4.19.10 Exigence de contrôle des AR/LCR

Les parties utilisatrices doivent récupérer les AR/LCR au moins toutes les 24 heures, avant de faire confiance à un document signé à l'aide d'un identifiant numérique CDS, excepté pour les identifiants numériques CDS délivrés aux fins des services d'horodatage.

4.19.11 Vérification en ligne du statut de révocation d'un certificat d'UH et de Sous-AC

Pour le certificat d'UH, la vérification est identique à celle effectuée pour le certificat CDS de classe 1, 2 ou 3.



Aucune disposition pour le certificat de Sous-AC.

4.19.12 Exigences de vérification en ligne des révocations

Les exigences relatives au certificat d'UH sont les mêmes que celles relatives au certificat CDS de classe 1, 2 ou 3.

Aucune disposition pour le certificat de Sous-AC.

4.19.13 Autres moyens disponibles d'information sur les révocations

Aucune disposition.

4.19.14 Exigences de vérification d'autres moyens d'information sur les révocations

Aucune disposition.

4.19.15 Exigences spécifiques en cas de compromission de la clé

En cas de compromission de la clé privée de l'AC KEYNECTIS-CDS, utilisée pour signer un certificat CDS, KEYNECTIS informera par e-mail, dans les délais les plus brefs possibles, tous les abonnés en possession de certificats CDS délivrés à partir de cette clé privée, que les certificats CDS seront révoqués le jour ouvrable suivant et que la publication de cette révocation dans la LCR appropriée vaudra notification à l'abonné de la révocation de son certificat CDS.

4.20 Procédures d'audit de la sécurité

4.20.1 Systèmes de confiance

Les AC et les AE de KEYNECTIS-CDS, ainsi que les archives de référence de KEYNECTIS n'utilisent que des systèmes de confiance dans le cadre de leurs services respectifs.

4.20.2 Horodatage

L'horodatage est destiné à améliorer les services de certification électronique de KEYNECTIS et la fiabilité des certificats. Il contribue également à la non-répudiation des messages à signature numérique. L'horodatage crée une notation qui fait apparaître (au moins) la date et l'heure exactes d'une action (explicitement ou implicitement), ainsi que l'identité de la personne ou du système qui a créé la notation. Tous les horodatages adoptent l'heure GMT (Greenwich Meridian Time) et l'UTC (Universal Time Convention). Pour les besoins de la présente PC/DPC, toute année exprimée dans la plage de valeurs de 00 à 69 désigne une année comprise entre 2000 et 2069 et toute année exprimée dans la plage de 70 à 99 désigne une année comprise entre 1970 et 1999.

L'horodatage des données suivantes par l'AC KEYNECTIS-CDS ou sa Sous-AC, s'effectue soit directement dans les données elles-mêmes, soit dans un rapport d'audit digne de confiance :

- les certificats ;
- la LCR ou d'autres informations des bases de données de suspension et de révocation ;
- chaque version de la PC/DPC ;
- les messages du service client ;
- d'autres informations, conformément aux dispositions de la présente PC/DPC.

Remarque : l'horodatage cryptographique sera mis en œuvre de manière incrémentale par l'AC pour tous les messages concernés.



4.20.3 Types d'événements enregistrés

L'AC KEYNECTIS-CDS ou sa Sous-AC générera automatiquement des enregistrements fiables, ainsi que certains documents, tels que :

- des documents prouvant le respect des règles de la PC/DPC ;
- des documents relatifs aux actions et informations se rapportant à chaque demande de certificat, ainsi qu'à la création, la délivrance, l'utilisation, la révocation, l'expiration et le renouvellement de chaque certificat délivré.

Ces enregistrements contiendront toutes les informations en possession de l'AC concernant :

- l'identité de l'abonné désigné dans chaque certificat (excepté pour les certificats CDS de classe 1, pour lesquels seuls le nom non ambigu de l'abonné et le nom de référence du document sont conservés) ;
- l'identité des personnes demandant la révocation d'un certificat (excepté pour les certificats CDS de classe 1, pour lesquels seul le nom non ambigu de l'abonné est conservé) ;
- d'autres faits indiqués dans le certificat ;
- les horodatages ;
- certains faits importants et prévisibles relatifs à la délivrance du certificat.

Les documents peuvent être conservés soit sous la forme de messages informatiques, soit sur papier, pourvu que leur indexation, leur stockage, leur conservation et leur reproduction soient exacts et complets. L'AC peut demander à un abonné ou à son agent de produire les documents qui permettront à l'AC de se conformer aux dispositions de la présente section.

4.20.4 Durées de conservation des documents

Les AC KEYNECTIS-CDS conserveront de manière fiable tous les enregistrements de classe 2 et de classe 3, ainsi que les documents s'y rapportant, pendant au moins 3 (trois) ans après la date de révocation ou d'expiration du certificat. Ces documents seront conservés sous forme électronique ou sur papier. Pour les certificats de classe 1, les documents électroniques seront conservés pendant au moins 3 (trois) ans à compter de leur délivrance.

4.20.5 Fréquence de journalisation

Les journaux d'accès sont examinés selon une fréquence quotidienne (pendant les jours ouvrables) ou si un événement quelconque le nécessite.

4.20.6 Période de conservation des journaux d'audit

Les journaux d'audit sont conservés sur site, pendant un an au maximum, après l'événement. Conformément à la législation française, les journaux d'accès physiques et les enregistrements de vidéosurveillance ne sont pas conservés pendant plus d'un mois.

4.20.7 Protection des journaux d'audit

Les journaux d'audit et les informations enregistrées sont stockés dans des zones sécurisées, conformément à la politique de stockage des éléments sensibles. L'accès à ces zones est réservé aux employés autorisés de KEYNECTIS, selon une procédure de double contrôle.

4.20.8 Procédures de sauvegarde des journaux d'audit

Tous les journaux générés automatiquement sont dupliqués avant la collecte des journaux d'audit.

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

Tous les journaux d'audit sont collectés manuellement par un/des employé(s) de confiance de KEYNECTIS.



4.20.10 Notification au responsable d'un événement

Les notifications au responsable d'un événement sont transmises automatiquement, par SMS ou par e-mail, au personnel de KEYNECTIS chargé de veiller au bon fonctionnement du système pendant les heures d'ouverture et en dehors de ces heures.

4.20.11 Analyse des vulnérabilités

Toutes les politiques de sécurité et les procédures opérationnelles font l'objet d'une vérification annuelle.

4.20.12 Audit relatif aux Sous-AC

KEYNECTIS met en place et gère des systèmes de confiance pour conserver un journal d'audit de tous les événements importants, tels que la génération de clés, ainsi que la demande, la validation et la révocation de certificats. Afin d'évaluer sa conformité avec la présente PC/DPC et d'autres accords, directives, procédures et normes applicables, l'audit à périodicité annuelle doit se conformer au programme d'audit Webtrust pour AC du moment, tel que publié par l'AICPA ou aux critères de certification appropriés pour des audits équivalents approuvés par l'Autorité de Politique d'Adobe.

La réception par KEYNECTIS de rapports d'audit de tiers ne vaut pas acceptation ou approbation par KEYNECTIS du contenu, des conclusions ou des recommandations de ces rapports. KEYNECTIS peut vérifier ces rapports pour protéger ses services de certification électronique. N'étant pas l'auteur de ces rapports d'audit, KEYNECTIS n'est pas responsable de leur contenu. KEYNECTIS n'exprime aucune opinion quant à ces rapports d'audit et sa responsabilité n'est nullement engagée au titre de dommages éventuels pouvant découler de la confiance accordée par KEYNECTIS à ces rapports d'audit.

4.21 Archivage des enregistrements

4.21.1 Types d'événements enregistrés

L'AC KEYNECTIS-CDS ou sa Sous-AC archive les enregistrements suivants, de manière suffisamment détaillée afin de pouvoir justifier le bon fonctionnement de l'AC.

Document/données à archiver	Requis (oui/non)
Politique de Certification	Oui
Politique et Déclaration des Pratiques de Certification	Oui
Obligations contractuelles	Oui
Configurations du système et de l'équipement	Oui
Modifications et mises à jour du système ou des configurations (scripts)	Oui
Demandes de révocation	Oui
Authentification de l'identité de l'abonné (suivant section 3.1.9)	Oui
Documents de réception et d'acceptation de certificats	Oui
Documents de réception de jetons	Oui
Tous les certificats délivrés ou publiés	Oui
Liste complète de tous les certificats révoqués	Oui
Tous les journaux d'audit	Oui



Autres données ou demandes nécessaires à la vérification du contenu des archives	Oui
Documents requis par les auditeurs de conformité	Oui

4.21.2 Période de conservation des archives

Les données archivées doivent être conservées pendant 10 ans.

4.21.3 Protection des archives

Les journaux d'audit et les informations enregistrées sont stockés dans des zones sécurisées, conformément à la politique de stockage des éléments sensibles. L'accès à ces zones est réservé aux employés autorisés de KEYNECTIS, selon une procédure de double contrôle.

4.21.4 Procédure de sauvegarde des archives

Les journaux d'audit sont dupliqués avant leur collecte. Un jeu de journaux d'audit est ensuite prêt à être transféré vers l'archivage.

4.21.5 Exigences en matière d'horodatage des enregistrements

Les enregistrements sont horodatés sur la base d'une synchronisation d'horloge à sources multiples externes.

4.21.6 Système de collecte des archives (interne ou externe)

Tous les journaux d'audit sont collectés manuellement et manipulés par un/des employé(s) de confiance de KEYNECTIS.

4.21.7 Procédure de récupération et de vérification des archives

Les données d'archives sont soumises à la politique de protection de l'information de KEYNECTIS. Pour pouvoir accéder aux données d'archives, les personnes extérieures doivent en faire la demande par écrit et obtenir une autorisation au niveau du Directeur opérationnel de KEYNECTIS.

Les données d'archives sont accessibles aux personnes autorisées, dans les locaux de KEYNECTIS.

4.22 Renouvellement de clés

L'AC KEYNECTIS-CDS ou sa Sous-AC exécute la procédure de renouvellement de clés qui décrit la procédure de sécurité et le script mis en œuvre.

4.23 Compromission et reprise après sinistre

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

Si l'équipement de l'AC KEYNECTIS-CDS ou de sa Sous-AC est endommagé ou n'est plus opérationnel, son bon fonctionnement doit être rétabli dans les meilleurs délais, la priorité étant donnée à l'aptitude à générer des informations sur l'état des certificats).

4.23.2 En cas de révocation de la clé publique d'une entité

L'AC KEYNECTIS-CDS ou sa Sous-AC exécute une nouvelle procédure de génération des clés, afin de rétablir un environnement sécurisé, après la révocation de la clé publique. Ces procédures sont similaires à la procédure initiale de génération de la paire de clés et à la soumission de la clé publique au niveau



supérieur pour re-certification. Cette procédure de révocation sera exécutée sous le contrôle de l'AC Racine Adobe, avant l'élaboration de toute procédure spécifique concernant la notification aux utilisateurs finals.

4.23.3 En cas de compromission de la clé d'une entité

Si la clé de signature de l'AC KEYNECTIS-CDS ou de sa Sous-AC est compromise, KEYNECTIS en informera immédiatement l'Autorité de Politique d'Adobe.

4.23.4 Plans d'urgence et reprise après sinistre

L'AC KEYNECTIS-CDS ou sa Sous-AC mettra en place, documentera et testera périodiquement les fonctions et procédures d'urgence et de reprise après sinistre, en conformité avec la PC/DPC et les procédures de sécurité de KEYNECTIS.

4.24 Fin de vie de l'AC

4.24.1 Fin de vie ou des activités de l'AC

Les obligations suivantes sont destinées à limiter l'impact de la cessation du service, par le biais d'une notification rapide, d'un transfert des responsabilités aux entités succédant à l'AC, du maintien des enregistrements et de certains dédommagements.

Pour l'AC KEYNECTIS-CDS, la procédure est décrite dans la Politique de Certification CDS et pour la Sous-AC KEYNECTIS-CDS, la procédure mise en œuvre est décrite ci-dessous.

4.24.2 Exigences avant la fin de vie

Avant de cesser ses activités d'AC, KEYNECTIS-CDS doit :

- notifier à son AC de niveau supérieur (c'est-à-dire Adobe) son intention de cesser ses activités d'AC. Cette notification doit être délivrée au moins 90 (quatre-vingt-dix) jours avant la cessation. L'AC de niveau supérieur peut demander des déclarations complémentaires, afin de vérifier le respect de cette disposition ;
- donner à l'abonné en possession d'un certificat non révoqué ou non expiré qu'elle a délivré, un préavis de 90 (quatre-vingt-dix) jours de son intention de cesser ses activités d'AE ;
- révoquer tous les certificats qui restent non révoqués ou non expirés à la fin de la période de préavis de 90 (quatre-vingt-dix) jours, que l'abonné ait demandé ou non la révocation ;
- notifier la révocation à chaque abonné concerné ;
- faire ce qui est raisonnablement en son pouvoir pour que la cessation de ses services de certification occasionne le moins d'inconvénients possible aux abonnés et aux personnes qui doivent vérifier les signatures numériques par référence à la clé publique contenue dans les certificats encore ouverts ;
- prendre des dispositions raisonnables pour la conservation de ses archives ;
- dédommager les abonnés dans une mesure raisonnable (sans dépasser le prix d'achat du certificat) pour la révocation de leurs certificats non expirés.

4.24.3 Réémission des certificats par l'AC successeur

Afin d'assurer la continuité des services d'AC aux demandeurs de certificats, les AC cessant leurs activités doivent prendre des dispositions avec une autre autorité similaire, sous réserve de l'accord écrit de l'autre AC et de l'approbation d'Adobe, en vue de la réémission des certificats encore ouverts des demandeurs. En réémettant un certificat d'AC, l'AC successeur assume les droits et les interdictions de l'AC en cessation, ainsi que, dans la mesure convenue par écrit entre les deux autorités et approuvée par Adobe, les obligations et responsabilités liées aux certificats non expirés. Sauf accord contraire entre l'AC en cessation et le demandeur, et sous réserve de l'accord écrit de l'AC successeur, la PC/DPC restera applicable à l'AC successeur, comme elle l'était à l'AC d'origine.



Les exigences énoncées ici peuvent varier d'un contrat à l'autre, pourvu que (a) les changements n'affectent que les parties contractantes et (b) Adobe approuve la totalité de ces changements.

5 MESURES DE SECURITE PHYSIQUES, PROCEDURALES ET RELATIVES AU PERSONNEL

5.1 Mesures de sécurité physiques

5.1.1 Situation géographique et construction de sites

Les installations de traitement des informations sensibles et essentielles de l'AC KEYNECTIS ou de sa Sous-AC sont hébergées dans des zones sécurisées, protégées par des périmètres de sécurité clairement définis et équipées de barrières de sécurité et de contrôles d'accès appropriés. Elles sont physiquement protégées contre 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 ou de la Sous-AC KEYNECTIS-C.

L'AC ou la Sous-AC KEYNECTIS-CDS se situe dans le Centre de Confiance de KEYNECTIS. Les installations de reprise après sinistre, en tant que centre de confiance principal, bénéficient du même ensemble de mesures de sécurité et de protection.

5.1.2 Accès physique

Tous les contrôles d'accès sont mis en œuvre de manière fiable, conformément à la politique de sécurité physique de KEYNECTIS.

L'accès aux salles de production est soumis à une procédure d'authentification reposant sur un double contrôle et sur une authentification rigoureuse faisant appel à une combinaison de badges et de biométrie (ce que l'on a et ce que l'on est).

Tous les employés de KEYNECTIS possèdent des badges qui leur permettent d'entrer dans le périmètre de sécurité, en fonction de leurs privilèges.

Tous les droits d'accès physique sont définis de telle sorte qu'une personne seule ne peut pas avoir accès à des données sensibles ni exécuter une opération sensible.

La politique de sécurité physique de KEYNECTIS est décrite dans le document désigné [DSQ_NT_KEYNECTIS Physical Security Policy_Tier 7].

5.1.3 Alimentation électrique et climatisation

KEYNECTIS garantit que les installations électriques et de climatisation sont suffisantes pour assurer le bon fonctionnement des systèmes de l'AC ou de la Sous-AC KEYNECTIS-CDS et qu'elles se composent d'installations principales et de secours, conformément à sa politique de sécurité physique.

5.1.4 Expositions à l'eau

KEYNECTIS garantit que les systèmes de l'AC ou de la Sous-AC KEYNECTIS-CDS bénéficient d'une protection qui minimise les dégâts des eaux, conformément à sa politique de sécurité physique.

5.1.5 Prévention et protection contre les incendies

KEYNECTIS garantit que les systèmes de l'AC ou de la Sous-AC KEYNECTIS-CDS sont protégés par des systèmes de détection et d'extinction des incendies, conformément à sa politique de sécurité physique.

5.1.6 Stockage des supports

Les supports utilisés au sein de KEYNECTIS pour l'AC ou la Sous-AC KEYNECTIS-CDS font l'objet d'une gestion sécurisée visant à les protéger contre tout dommage, vol et accès non autorisé. Des procédures de

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



gestion des supports sont mises en œuvre pour protéger les supports contre l'obsolescence et la détérioration pendant la période où les enregistrements doivent être conservés.

Tous les supports sont gérés de manière sécurisée conformément à la politique de gestion des éléments sensibles et au programme de protection des informations.

Les supports comportant des informations sensibles sont mis au rebut conformément à la politique de stockage des éléments sensibles.

KEYNECTIS transfère régulièrement des copies ou des sauvegardes d'éléments sensibles vers un lieu de stockage hors site qui met en œuvre des mesures de sécurité équivalentes aux siennes, dans ses locaux principaux.

5.1.7 Traitement des déchets

Tous les supports utilisés pour le stockage d'informations sensibles, telles que les clés, les données d'activation ou les fichiers de l'AC KEYNECTIS-CDS ou de sa Sous-AC sont effacés ou détruits avant d'être mis au rebut, conformément à la politique de gestion des éléments sensibles de KEYNECTIS et à sa politique de destruction [DSQ_NT_Destruction des supports d'information].

Les jetons de sauvegarde qui ont contenu des données de clé privée de l'AC ou de la Sous-AC KEYNECTIS-CDS sont détruits physiquement dès qu'ils ne sont plus utilisés.

5.1.8 Sauvegarde hors site

Des sauvegardes complètes du système de l'AC KEYNECTIS-CDS, suffisantes pour permettre la reprise suite à une panne du système, sont effectuées périodiquement. Des copies de sauvegarde des informations et des logiciels essentiels à l'entreprise sont effectuées régulièrement. Des équipements de sauvegarde adéquats sont prévus pour garantir la récupération de toutes les informations et des logiciels essentiels à l'entreprise après un sinistre ou une défaillance des supports de stockage. Au moins une copie de sauvegarde complète de la clé privée est stockée hors site (en un lieu distinct de celui où se trouvent les équipements de l'AC ou de la Sous-AC KEYNECTIS-CDS).

Cette copie de sauvegarde est conservée sur un site où les contrôles physiques et de procédure sont équivalents à ceux mis en œuvre sur le site opérationnel de l'AC ou de la Sous-AC KEYNECTIS-CDS, conformément à la politique de sécurité physique de KEYNECTIS.

5.2 Mesures de sécurité en termes de procédures

5.2.1 Rôle de confiance

Tous les salariés, entrepreneurs et consultants (dénommés collectivement le « personnel ») qui ont accès à ou qui contrôlent des opérations cryptographiques pouvant affecter de façon significative la délivrance, l'utilisation ou la révocation de certificats par l'AC, y compris l'accès aux opérations restreintes des archives de référence de KEYNECTIS, seront considérés, pour les besoins de la présente PC/DPC, comme occupant un poste de confiance. Ce personnel inclut, non limitativement, le personnel du service client, le personnel d'administration du système, le personnel technique désigné et les cadres chargés de superviser le système de confiance de l'infrastructure de l'AC.

5.2.2 Nombre de personnes requises par tâche

Les opérations sensibles de l'AC ou de la Sous-AC KEYNECTIS-CDS qui nécessitent un contrôle par plusieurs personnes relèvent toutes, d'un point de vue opérationnel, de la gestion du cycle de vie des clés privées de l'AC. Ces opérations comprennent :

- la génération de clés par l'AC ;
- la révocation de clés par l'AC ;
- la génération de certificats par l'AC ;
- le renouvellement de certificats par l'AC ;
- l'activation de clés par l'AC ;
- la désactivation de clés par l'AC ;
- la destruction de clés par l'AC ;



- les opérations effectuées sur toutes les données d'activation, de la création à la destruction.

Toutes ces opérations sont réalisées et enregistrées, conformément aux procédures de l'AC KEYNECTIS-CDS, par des personnes occupant des rôles de confiance.

5.2.3 Identification et authentification de chaque rôle

L'identification et l'authentification de toutes les personnes concernées lors d'une procédure de génération des clés sont conduites par les employés de KEYNECTIS. Le personnel d'identification et d'authentification qui détient des privilèges sur les MSM de l'AC KEYNECTIS-CDS est muni de dispositifs physiques (clés PED) limitant leur accès. Ces dispositifs sont requis pour activer les MSM. Seules les personnes autorisées peuvent pénétrer dans la salle de génération des clés pour activer le MSM contenant la clé privée de l'AC ou de la Sous-AC KEYNECTIS-CDS.

La liste des personnes autorisées à accéder au périmètre de sécurité de KEYNECTIS et des droits associés figure dans le document [DSQ_NT_Droits d'accès zones KEYNECTIS].

5.3 Mesures de sécurité en termes de personnel

5.3.1 Procédures de gestion du personnel

Les AC KEYNECTIS-CDS mettent en place et suivent des procédures de gestion du personnel qui permettent d'assurer raisonnablement la crédibilité et les compétences de leurs salariés, ainsi que l'accomplissement satisfaisant de leurs obligations.

5.3.1.1 Personnel à des postes de confiance

Le personnel n'aura pas accès aux fonctions de confiance tant que les vérifications nécessaires n'auront pas été effectuées. Toutes les personnes postulant à des rôles de confiance sont sélectionnées sur la base de critères de loyauté, de fiabilité et d'intégrité et font l'objet d'une vérification d'antécédents, conformément à la politique [DSQ_NT_KEYNECTIS trusted employee policy].

La procédure de vérification des antécédents porte au moins sur les points suivants :

- *l'identité personnelle ;*
- *le lieu de résidence ;*
- *le numéro de sécurité sociale ;*
- *le casier judiciaire ;*
- *les références bancaires ;*
- *l'emploi précédent ;*
- *les références professionnelles ;*
- *la formation.*

Cette mesure ne s'applique pas aux membres du conseil d'administration de KEYNECTIS ou des AC, à moins qu'ils n'occupent un poste opérationnel dans les services de certification électronique.

5.3.1.2 Renvoi de personnes à des postes de confiance

Toute personne qui échoue à l'enquête initiale ou périodique sera renvoyée de son poste de confiance. Le renvoi d'une personne occupant un poste de confiance est laissé à la discrétion exclusive de l'AC concernée (ou de KEYNECTIS, dans le cas du personnel de KEYNECTIS).

5.3.1.3 Exigences et fréquence des formations

Les salariés de KEYNECTIS sont régulièrement informés et sensibilisés au sujet des procédures de sécurité, conformément à la procédure [DSQ_NT_KEYNECTIS_Trusted Employee Policy]. En outre, ils suivent une formation annuelle, dans le cadre du plan de formation interne de l'entreprise.

5.3.1.4 Séquence et fréquence de rotation des emplois

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



Aucune disposition.

5.3.1.5 Sanctions en cas d'actions non autorisées

Tous les salariés de KEYNECTIS exécutant des actions non autorisées sont passibles de sanctions aux termes de l'article 22 « Sanctions disciplinaires » de la déclaration du règlement interne de KEYNECTIS.

5.3.1.6 Exigences en matière de recrutement de personnel

Les AC KEYNECTIS-CDS conduisent une enquête initiale sur toutes les personnes postulant à des postes de confiance, afin d'établir aussi raisonnablement que possible leur loyauté et leurs compétences. Par la suite, les AC KEYNECTIS-CDS conduisent une enquête périodique sur tous les membres du personnel qui occupent un poste de confiance, afin de vérifier s'ils continuent de satisfaire les critères de loyauté et de compétence, en conformité avec les pratiques de KEYNECTIS en matière de personnel ou leur équivalent.

5.3.1.7 Documentation fournie au personnel

KEYNECTIS fournit à son personnel de confiance des documents relatifs à la tâche ou aux tâches qu'il doit accomplir pendant le fonctionnement de l'AC ou de la Sous-AC KEYNECTIS-CDS. Cette documentation est fournie au personnel soit lors de la formation, via le réseau d'entreprise de KEYNECTIS, soit sur la base du principe de connaissance sélective.

6 MESURES DE SÉCURITÉ TECHNIQUES

6.1 Approbation des logiciels et équipements matériels

Tous les logiciels et matériels se rapportant aux services de certification électronique doivent être approuvés par KEYNECTIS, par un consultant autorisé de KEYNECTIS ou par d'autres autorités reconnues (désignées périodiquement par KEYNECTIS), en fonction des besoins, conformément à la présente PC/DPC.

6.2 Génération, installation et protection d'une paire de clés

6.2.1 Génération d'une paire de clés par l'AC et la Sous-AC KEYNECTIS-CDS

Les AC KEYNECTIS-CDS généreront et protégeront de façon fiable leurs propres clés privées, au moyen d'un module de sécurité matérielle digne de confiance et supérieur à la norme FIPS 140-1 niveau 3 et elles prendront des précautions nécessaires pour éviter la perte, la divulgation, la modification ou l'usage abusif. KEYNECTIS utilise actuellement la carte Luna CA 3 de Chrysalis-ITS (critères communs EAL4+ et FIPS 140-1 niveaux 2 et 3).

Afin de pouvoir proposer une solution faisant appel à plusieurs fournisseurs, KEYNECTIS utilise le dispositif MSM de Bull Trustway (EAL4+ et FIPS 140-3), en tant qu'unité matérielle de signature cryptographique. Tous les jetons ont été développés au moyen d'un logiciel personnalisé afin d'obtenir des jetons infalsifiables.

La génération des clés privées de l'AC et de la Sous-AC a lieu au cours d'une **procédure officielle de génération des clés** :

- à l'aide d'un matériel cryptographique approuvé ;
- à l'aide d'ordinateurs spécialisés hors ligne ;
- sous double contrôle ;
- dans une salle spécialisée et sécurisée, située dans les locaux de KEYNECTIS, sous surveillance/enregistrement vidéo et avec des services de notaire public.

6.2.2 Délivrance de la paire de clés privées

L'AC et la Sous-AC KEYNECTIS-CDS génèrent leurs propres clés privées, de sorte qu'aucune délivrance n'est nécessaire à l'extérieur du Bunker de KEYNECTIS.

Les clés privées d'abonnés sont délivrées aux abonnés ou aux représentants autorisés, en fonction de la section Exigences Opérationnelles ci-dessus.

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

Les clés publiques sont délivrées à l'émetteur d'identifiants numériques, par le biais de demandes PKCS#10. La demande PKCS#10 est signée à l'aide de la clé privée de l'abonné. La signature de l'abonné est authentifiée par l'AC émettrice, avant la délivrance d'un identifiant numérique à l'abonné.



6.2.4 Tailles des clés

L'AC et la Sous-AC KEYNECTIS-CDS utilisent une paire de clés RSA d'une longueur de 2048 bits. L'identifiant numérique de l'abonné CDS doit utiliser une paire de clés RSA d'au moins 2048 bits.

6.3 Protection des clés privées

6.3.1 Protection à l'aide d'un module cryptographique

Les AC KEYNECTIS-CDS font appel à des modules matériels cryptographiques dignes de confiance pour toutes les opérations nécessitant l'utilisation de leur clé privée. La procédure de création de clés privées est publiée dans les archives de référence de KEYNECTIS.

Tous les jetons cryptographiques et autres dispositifs matériels liés à la procédure de délivrance de certificats sont conservés dans des salles sécurisées, protégées à la fois par un mode d'accès par clés électroniques et par des lecteurs biométriques. Toutes les salles sécurisées relèvent d'une zone de sécurité de niveau 4 sur 7 (sécurité physique), sont protégées contre les incendies au moyen de systèmes d'extinction automatique et les privilèges d'accès sont réservés aux salariés de confiance ayant des responsabilités inhérentes à leur poste à l'intérieur des salles.

6.3.2 Partage de secret

Les AC KEYNECTIS-CDS font appel au partage de secret, par le biais de détenteurs de parts de secret, autorisés, pour améliorer la fiabilité de leur(s) clé(s) privée(s) et assurer le recouvrement des clés, suivant le tableau 2 Distribution de parts de secret ci-dessous.

Entité	Part de secret nécessaire pour permettre à la clé privée de l'AC de signer des certificats d'utilisateur final	Part de secret nécessaire pour générer un certificat d'AC à l'aide de la paire de clés	Total des parts de secret distribuées	Parts récupérées en cas de sinistre	
				Nécessaires	Total
AC KEYNECTIS-CDS (ACR)	2	3	5	3	5
AC SOUS-AC KEYNECTIS-CDS (ACR)	2	3	5	3	5
UH KEYNECTIS-CDS	2	3	5	3	5

Tableau 2 – Distribution des parts de secret

□ Protection de la part de secret

Le détenteur de part de secret doit utiliser des systèmes de confiance pour protéger sa part de secret contre les violations. Sauf disposition contraire dans la présente PC/DPC, le détenteur de part de secret s'engage à ne pas :

- divulguer, publier, copier, partager avec des tiers ou prendre part à tout usage abusif de la part de secret ;
- révéler (explicitement ou implicitement) à l'extérieur de l'entreprise qu'il est ou que quelqu'un d'autre est détenteur d'une part de secret ;
- conserver la part de secret en un lieu où elle ne pourra pas être récupérée en cas d'incapacité ou d'indisponibilité du détenteur de part de secret (excepté si la part de secret est utilisée à d'autres fins).



□ **Disponibilité et communication des parts de secret**

Le détenteur de part de secret doit mettre sa part de secret à la disposition des entités autorisées (dont la liste figure sur le formulaire d'acceptation de part de secret), seulement après l'obtention d'une autorisation appropriée, par le biais d'un enregistrement authentifié (voir paragraphe suivant).

En cas d'accident (déclaré par l'émetteur de part de secret), le détenteur de part de secret doit contacter un site de recouvrement, conformément aux instructions de l'émetteur de part de secret.

Avant de se rendre sur un site d'urgence ou de recouvrement et de communiquer sa part de secret, le détenteur de part de secret doit authentifier la déclaration de l'émetteur de part de secret, conformément aux instructions figurant sur le formulaire d'acceptation de part de secret (sauf en cas d'interdiction légale ou judiciaire, par exemple, dans le cadre d'une enquête criminelle).

La procédure comportera l'utilisation d'une phrase challenge (communiquée par l'émetteur de part de secret au détenteur de part de secret) pour s'assurer que le détenteur de part de secret n'est pas incité frauduleusement à se rendre sur un mauvais site, pour empêcher ainsi le recouvrement de la part de secret par l'émetteur. Sur le site de recouvrement, le détenteur de part de secret délivrera (personnellement) la part de secret dans le cadre de sa participation à la procédure de recouvrement consécutive à l'accident.

Le détenteur de part de secret peut faire confiance à tout(e) instruction, document, message, enregistrement, instrument ou signature qu'il estime authentique, avec une certitude raisonnable, pourvu qu'il authentifie la déclaration de l'émetteur de part de secret, conformément au paragraphe précédent. L'émetteur de part de secret fournira au détenteur de part de secret un exemplaire de toutes les signatures servant à authentifier les instructions de l'émetteur de part de secret.

□ **Enregistrements à conserver par les émetteurs et détenteurs de parts de secret**

Les émetteurs et les détenteurs de parts de secret conserveront des enregistrements de leurs activités concernant les parts de secret. Sur demande authentifiée, le détenteur de part de secret fournira à l'émetteur de part de secret ou à son représentant désigné, des informations concernant l'état de la part de secret.

6.3.3 Séquestre des clés privées

Les clés privées de KEYNECTIS-CDS sont mises en main tierce pendant la procédure de génération des clés et sont conservées selon une procédure manuelle dans la zone de sécurité de niveau 7 du Bunker de KEYNECTIS.

Les clés privées de KEYNECTIS-CDS destinées à l'UH sont mises en main tierce pendant la procédure de génération des clés et sont conservées selon une procédure manuelle dans la zone de sécurité de niveau 7 du Bunker de KEYNECTIS.

Les clés privées de l'abonné CDS ne font pas l'objet d'une procédure de séquestre.

6.3.4 Sauvegarde des clés privées

Les clés privées des abonnés ne font pas l'objet de sauvegarde.

La sauvegarde des clés privées de l'AC et de la Sous-AC KEYNECTIS-CDS est décrite ci-dessous.

6.3.5 Archivage des clés privées

Les parts de secret et les sauvegardes de clés privées d'AC sont conservées dans une zone de sécurité de niveau 7 qui met en œuvre des procédures d'accès sous double contrôle :

- Le personnel autorisé accompagne les détenteurs de parts de secret dans une salle sécurisée spécialisée (personnes de confiance détenant des privilèges d'accès contrôlé par des lecteurs biométriques/clés électroniques).
- Situé dans une salle sécurisée, un coffre-fort de supports résistant au feu pendant une heure, permet le stockage protégé dans des compartiments se trouvant à l'intérieur du coffre-fort. Ces compartiments sont placés sous double contrôle et constituent des emplacements individuels de stockage, réservés à chaque détenteur de part de secret.

Remarque : des clés de reprise après sinistre sont conservées hors site dans des compartiments de coffre-fort de la chambre forte d'une banque, sous le contrôle de deux personnes de confiance.



6.3.6 Introduction des clés privées dans le module cryptographique

Les clés privées des AC KEYNECTIS-CDS sont générées exclusivement par le module cryptographique. Les clés privées des abonnés sont soit générées par le module cryptographique, soit importées vers celui-ci.

6.3.7 Méthode d'activation des clés privées

Pour activer une clé privée, les abonnés ou des rôles de confiance doivent s'authentifier sur le support hébergeant la clé privée. Les types d'authentification comprennent, non limitativement, des mots de passe, des PIN, des expressions de passe et la biométrie.

6.3.8 Méthode de désactivation des clés privées

La désactivation des modules cryptographiques contenant la clé privée de l'AC s'effectue automatiquement, à chaque fois qu'ils sont déconnectés de leurs lecteurs de cartes système. La réactivation de la clé privée stockée dans le MSM nécessite six personnes sous double contrôle.

6.3.9 Méthode de destruction des clés privées

La destruction des clés privées de l'AC et de la Sous-AC KEYNECTIS-CDS peut être effectuée au moyen de différents mécanismes, dont l'effacement de la clé privée de l'AC au moyen des fonctions de réinitialisation et/ou de suppression du module cryptographique ou la destruction physique du module cryptographique.

6.4 Autre aspect de la gestion des paires de clés privées

6.4.1 Archivage des clés publiques

Aucune disposition.

6.4.2 Périodes d'utilisation des clés publiques et privées

Le certificat CDS de classe 1 peut imposer des périodes d'utilisation de clés privées.

Aucune disposition pour les autres classes.

6.5 Données d'activation

6.5.1 Génération et installation des données d'activation

Les données d'activation de KEYNECTIS-CDS permettant de déverrouiller les clés privées dans le module cryptographique, sont générées lors de la procédure de génération des clés.

Les parts de secret permettant d'activer la clé privée de l'AC au moyen de six personnes sous double contrôle, sont générées à l'aide des modules cryptographiques matériels contenant la clé privée, lors de la procédure de génération de clés. L'activation de modules cryptographiques contenant la clé privée de l'AC des clients nécessite la disponibilité constante de ces parts de secret.

6.5.2 Protection des données d'activation

Les données d'activation sont protégées contre la divulgation et mettent en œuvre un principe de partage de secret manuel n sur m.

6.6 Mesures de sécurité des systèmes informatiques

6.6.1 Sécurité des communications

Toutes les communications entre KEYNECTIS et d'autres entités concernées par des services de certification électronique, en vertu de la présente PC/DPC, doivent faire appel à une application procurant les mécanismes de sécurité appropriés avec un risque mesuré. Sans que leur portée soit limitée, les avis informatiques, les accusés de réception de ces avis et toute autre communication affectant la sécurité des services de certification feront également l'objet d'une protection appropriée.

6.6.2 Sécurité des installations

Les AC KEYNECTIS-CDS mettent en œuvre des installations qui sont sensiblement conformes aux procédures de sécurité de KEYNECTIS ou à des normes équivalentes.



6.7 Mesures de sécurité techniques du cycle de vie

6.7.1 Mesures de sécurité liées au développement des systèmes

Le développement et la modification des systèmes et des logiciels sont documentés et contrôlés par le département Qualité de KEYNECTIS.

6.7.2 Mesures liées à la gestion de la sécurité

Le développement et les modifications des systèmes initiaux des AC (matériel, application, système d'exploitation) sont documentés et contrôlés par le département Qualité de KEYNECTIS.

6.7.3 Evaluation de la sécurité du cycle de vie

Tous les composants logiciels des AC KEYNECTIS-CDS présents dans le centre de confiance de KEYNECTIS, ont été développés conformément aux exigences du document CEN CWA 14167-1 « Exigence de sécurité des systèmes de confiance gérant des certificats numériques de signature électronique ».

6.8 Mesures de sécurité réseau

Les composantes de l'ICP accessibles par réseau sont connectées à Internet via des protections de limite de système et assurent un service continu (excepté, si nécessaire, pendant de courtes périodes de maintenance ou de sauvegarde).

Les composantes de l'AC KEYNECTIS-CDS 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. L'ensemble des principes et mesures de sécurité applicable est identifié dans la politique de sécurité du système d'information de KEYNECTIS.

6.9 Mesures de sécurité liées à la conception des modules cryptographiques

Les MSM utilisés pour les besoins de l'AC KEYNECTIS-CDS sont soit conformes à la norme FIPS...

7 PROFILS DES CERTIFICATS ET DES LCR

7.1 Extensions et règles de nommage

7.1.1 Mécanismes d'extension et cadre d'authentification

Les services de certification facilitent l'utilisation des certificats X.509 v3. Les certificats X.509 v3 étendent les capacités des v1 et v2 et permettent d'ajouter des extensions au certificat. Cette capacité, composant standard des services de certification de KEYNECTIS, complète le modèle des services d'authentification standard.

7.1.2 Extensions standard et spécifiques

Le document « X.509 Amendment 1 to ISO/IEC 9594-8:1995 » définit une série d'extensions. Ces extensions permettent des contrôles de gestion et d'administration utiles pour une authentification à grande échelle et à usages multiples. Les services de certification de KEYNECTIS font appel à plusieurs de ces contrôles à des fins identifiées dans le document X.509. (Remarque : les logiciels d'utilisateurs conformes à X.509 sont supposés appliquer les règles de validation de la PC/DPC.)

Par ailleurs, la PC/DPC permet à l'utilisateur de définir des extensions « privées » supplémentaires dans des buts ou sous des modes propres à l'environnement de son application. La définition d'extensions axées sur un service et les pratiques de traitement de ces informations lors de la demande de certification, de l'approbation et de la délivrance du certificat sont spécifiées dans les procédures de sécurité de

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDS_CA_FR_V1.2.doc



KEYNECTIS, ainsi que dans des documents accessibles au public auprès des organisations proposant ces extensions.

7.1.3 Identification et criticité des extensions spécifiques

La fonction de chaque extension est indiquée par une valeur standard OID (identifiant d'objet). En outre, à chaque extension de certificat est attribuée une valeur de criticité « vraie » ou « fausse ». Cette valeur est déterminée par l'AC, le cas échéant, sur la base d'informations fournies par le demandeur dans sa demande de certificat. Cette valeur doit respecter certaines contraintes imposées par l'organisation chargée de la définition de l'extension.

La présence d'une valeur de criticité « vraie » dans une extension donnée exige que toutes les personnes qui valident le certificat considèrent celui-ci comme non valable si elles ne connaissent pas le but et les exigences d'une extension spécifique quelconque dont la valeur de criticité est « vraie ». Si cette valeur est « fausse », lors de la validation, soit ces personnes traiteront l'extension conformément à la définition applicable, soit elles ne la prendront pas en compte.

7.1.4 Chaînes de certificats et types d'AC

Les services de certification électronique de KEYNECTIS utilisent des chaînes de certificats. Chaque AC d'une chaîne de certificats KEYNECTIS exécute des procédures particulières en fonction du rôle qui lui est attribué dans la hiérarchie ADOBE. Une même AC peut exercer deux rôles différents :

- « Sous-AC de l'Autorité de Certification Racine Adobe » et
- AC d'une autre AC.

7.1.5 Extensions de certificats des utilisateurs finals

Les AC peuvent délivrer aux utilisateurs finals des certificats contenant des extensions définies dans le document « X.509 Amendment 1 to ISO/IEC 9594-8:1995 ». Les extensions ISO qui sont utilisées dans les services de certification de KEYNECTIS et dont le contenu est attribué par l'AC concernée, sont actuellement limitées aux suivantes :

- Contraintes de base
- Utilisation de la clé
- Utilisation étendue de la clé
- Politique de certification
- AKI (identifiant de la clé de l'autorité) / SKI (identifiant de la clé du porteur)

L'utilisation de ces extensions régit le processus de délivrance et de validation des certificats.

7.1.6 Extensions ISO « Contraintes de base »

L'extension de contraintes de base sert à délimiter le rôle et la position de l'AC ou du certificat d'utilisateur final dans une chaîne de certificats. Par exemple, les certificats délivrés à des AC et à des AC subordonnées contiennent une extension de contraintes de base qui les identifie comme des certificats d'AC. Les certificats d'utilisateurs finals comportent une extension qui fait qu'ils ne peuvent pas être des certificats d'AC.

7.1.7 Extensions ISO « Utilisation de la clé » et « Utilisation étendue de la clé »

L'extension « Utilisation de la clé » limite les finalités techniques pour lesquelles une clé publique figurant dans un certificat valable peut être utilisée dans le cadre des services de certification électronique de KEYNECTIS. Les certificats d'AC peuvent contenir une extension « Utilisation de la clé » qui limite l'usage de la clé à la signature des certificats, d'une liste de certificats révoqués et d'autres données.



7.1.8 Extension ISO « Politique de certification »

L'extension « Politique de certification » limite un certificat aux pratiques requises par des parties de confiance (ou indiquées à celles-ci). L'extension « Politique de certification » telle qu'elle est mise en œuvre dans les services de certification renvoie les utilisateurs à la PC/DPC et indique les usages appropriés.

Les extensions et le nommage amélioré sont spécifiés dans le certificat soit en totalité, soit partiellement auquel cas, le reste figure dans un document externe inclus par référence dans le certificat.

L'information contenue dans le champ « Organizational Unit » (unité d'organisation) se trouve également dans l'extension « Politique de certification », si cette dernière figure dans le certificat. La présente PC/DPC constitue une « politique de certification » selon les termes du document « X.509 Amendment 1 to ISO/IEC 9594-8:1995 ». Une AC agissant en tant qu'autorité habilitée à formuler des politiques, attribuée à la PC/DPC une valeur d'identifiant d'objet (OID) qui est incluse dans l'extension « Politique de certification ».

7.1.8.1 Pointeurs vers la PC/DPC

Il est fait appel à du texte (lisible par l'utilisateur) et à des pointeurs informatiques (à base d'URL ou d'autres identifiants et mécanismes) pour permettre aux utilisateurs de certificats de localiser facilement la PC/DPC et d'autres informations pertinentes et d'y accéder.

7.1.8.2 Avertissements, limitations de responsabilité et limitations de garantie

Chaque certificat peut contenir une brève déclaration énonçant les limitations applicables en matière de responsabilité et de garantie, ainsi qu'un pointeur vers le texte complet de ces avertissements, exonérations et limitations, dans la PC/DPC.

Ces informations peuvent également être affichées au moyen d'une fonction de visualisation de certificat, le cas échéant, via un lien hypertexte vers un message accessible aux utilisateurs ou agents, au lieu d'être incorporées dans le certificat. La méthode mise en œuvre pour partager des informations (à présenter aux utilisateurs) consiste en un qualificateur d'AC désignant une politique de certification enregistrée auprès de KEYNECTIS (à l'aide d'une extension v3 standard).



8 ADMINISTRATION DES SPÉCIFICATIONS

8.1 Procédures de modification de la PC/DPC

La PC/DPC de l'AC KEYNECTIS-CDS doit être soumise à l'examen et à l'approbation de l'Autorité de Politique d'Adobe, avant d'être appliquée et publiée. KEYNECTIS doit également :

- proposer toute nouvelle version de la PC/DPC avec mise en évidence de ses modifications ;
- attendre l'approbation de la nouvelle PC/DPC ;
- publier et appliquer la nouvelle PC/DPC.

8.2 Politique de publication et de notification

L'Autorité de Politique de KEYNECTIS doit mettre en œuvre cette politique. Toutes les propositions de modifications de cette politique doivent être communiquées à toutes les AC CDS subordonnées, 90 (quatre-vingt-dix) jours avant leur adoption. L'Autorité de Politique de KEYNECTIS examinera les commentaires pour ou contre les modifications proposées, sous réserve qu'ils soient formulés par écrit, dans un délai de 30 jours à compter de la publication des modifications proposées.

8.3 Procédure d'approbation de la PC/DPC

La présente PC/DPC de l'AC KEYNECTIS-CDS a été approuvée par l'Autorité de Politique d'Adobe, avant la réception du certificat d'AC Racine Adobe, conformément à la politique de CDS d'Adobe.

9 ANNEXE

Ce document contient différents acronymes et abréviations. Vous trouverez une définition des termes les plus couramment utilisés dans le glossaire ci-dessous.

A / B

Abonné

Personne à laquelle un certificat a été délivré, qui est le porteur de et est capable d'utiliser (et y a été autorisé) la clé privée qui correspond à la clé publique indiquée dans le certificat.

Accord d'abonnement

Accord conclu entre le demandeur et l'AC pour la fourniture de services de certification électronique précis, conformément à la présente PC/DPC.

AC Racine Adobe

Autorité de Certification Racine d'Adobe.

AC Subordonnée CDS

Toute Autorité de Certification autorisée liée à une AC Racine intégrée à Acrobat par Adobe.

Accepter (un certificat)

Les demandeurs de certificat font état de leur approbation d'un certificat tout en ayant pris connaissance et bonne note des informations qu'il contient, conformément à la PC/DPC.

Accès

Type spécifique d'interaction entre une demande et des sources de communication ou d'information, entraînant un flux d'information, une prise de contrôle ou l'activation d'un processus.

Accréditation / Accrédité



Déclaration formelle formulée par un représentant KEYNECTIS autorisé, selon laquelle un système informatique, un professionnel, un employé, un sous-traitant ou une société est habilité à effectuer certaines opérations et à opérer dans un cadre de sécurité spécifique, en ayant recours à un ensemble défini de mesures de sécurité.

Administrateur de l'Autorité d'Enregistrement

Employé d'une AE, responsable de l'exécution des fonctions d'une AE.

AE

Cf Autorité d'enregistrement .

AE non KEYNECTIS

AE n'appartenant pas à KEYNECTIS et dont les fonctions se limitent à celles d'une AE.

Affirmer / Affirmation

Reconnaître ou indiquer l'exactitude de données ou la véracité d'informations.

Archives de référence

Base de données de certificats contenant également des informations connexes.

Algorithme cryptographique

Processus de calcul clairement spécifié permettant de résoudre un problème. Ensemble de règles conduisant au résultat prescrit.

Alias

Synonyme de pseudonyme.

Archiver

Conserver des enregistrements et les journaux correspondants pendant une période donnée à des fins de sécurité, de sauvegarde et d'audit.

ARL/LAR

Liste des Autorités de certification Révoquées ou Liste des Certificats Révoqués.

Annuaire

Ensemble d'enregistrement organisés (classés)

Audits

Procédure permettant de certifier la présence de contrôles et leur adéquation à leur objectif. Un audit permet d'enregistrer et d'analyser des opérations afin de surveiller les intrusions ou les utilisations dans un système d'information. Les anomalies détectées au cours d'un audit sont signalées au département approprié.

Autorité de Certification (AC)

Entité chargée de délivrer des certificats numériques. Elle définit les termes et conditions relatifs à la gestion du cycle de vie d'un certificat (délivrance, renouvellement, révocation, etc.) À cette fin, l'autorité de certification est chargée de rédiger une Politique de Certification (PC) détaillant ces termes et conditions.

Autorité de Certification Racine (ACR)

Autorité de Certification suprême.

Autorité d'Enregistrement (AE)

Entité responsable de l'identification et de l'authentification de demandeurs de certificats électroniques au nom d'une AC, mais non responsable de la délivrance de certificats électroniques.

Autorité de nommage

Entité mettant en œuvre des procédures et politiques de nommage et contrôlant l'enregistrement et l'attribution de noms de base à des objets d'une classe donnée.

**Autorité de nommage KEYNECTIS**

Autorité de nommage chargée d'établir, de contrôler et de gérer l'attribution de noms distinctifs relatifs pour toutes les AE.

Autorité de Politique d'Adobe

Panel de membres de la direction d'Adobe, chargé de définir, de revoir et d'approuver les politiques relatives à l'ICP Adobe.

Authentification

Processus mis en œuvre pour confirmer l'identité d'un individu ou l'intégrité d'une information. L'authentification d'un message consiste à déterminer son origine et à vérifier qu'il n'a pas été modifié ni remplacé pendant son acheminement.

Authentifier

Voir Authentification.

Auteur

Personne ou mandataire de cette personne à l'origine de la génération, du stockage ou de la communication d'un message de données. Une personne agissant en tant qu'intermédiaire n'est pas considérée comme l'auteur.

Autorisation

Attribution de droits, notamment d'accès à des informations ou à des ressources spécifiques.

Avis

Résultat d'une notification, conformément à la présente PC/DPC.

Base de données

Ensemble d'informations connexes créées, stockées ou manipulées par un système de gestion informatisé.

Base de données digne de confiance

Base de données créée sous le contrôle et/ou avec l'approbation du gouvernement. Ces bases de données peuvent être créées en accord avec des programmes gouvernementaux (par ex. programme PRIS ou de santé) ou avec des groupes d'organisations approuvées (par ex., secteur bancaire, groupe industriel de membres identifiés).

C**Canal sécurisé**

Moyen de communication reposant sur un système cryptographique qui protège les messages des menaces observées.

Caractère commercial raisonnable

Dans le contexte du commerce électronique, cette expression fait référence à la mise en œuvre et à l'utilisation de technologies, de contrôles et de procédures administratives et opérationnelles assurant de manière raisonnable la fiabilité des systèmes et des messages.

Carte à puce

Dispositif de sécurité contenant le certificat d'un utilisateur et la clé privée connexe.

CDS

Certified Document Services.

Certificat

Message contenant au minimum les informations suivantes : le nom ou des données d'identification du demandeur, la clé publique du demandeur, la période de validité du certificat, le numéro de série du certificat



et la signature numérique de l'AC. Toute référence à un « certificat de classe » (1, 2, 3, etc.) sans autre qualificateur se rapporte à un certificat « normal » ou « provisoire », à moins que le contexte indique une interprétation différente. Toute référence à un certificat se rapporte exclusivement aux certificats délivrés par une AC.

Certificat à clé publique

Voir Certificat.

Certificat d'AC

Certificat délivré par une AC à une AC subordonnée.

Certificat CDS

Certificat délivré dans le cadre de l'ICP de CDS pour la signature numérique de documents PDF.

Certificats de classe 1, 2 et 3

Certificat correspondant à un niveau de confiance défini.

Certificat électronique

Un certificat est un fichier électronique qui représente un document d'identification numérique, par l'établissement d'un lien avec l'entité qui lui est associée.

Certificat d'authenticité

Document délivré par une autorité officielle autorisée appartenant à la juridiction dans laquelle la reconnaissance par un notaire a eu lieu, afin d'authentifier le statut d'un notaire.

Certificat gratuit

Certificat délivré par une Autorité d'Enregistrement sans frais.

Certificat de test

Certificat délivré par une AC à des fins de tests techniques uniquement. Seules des personnes autorisées peuvent utiliser des certificats de test.

Certification / Certifier

Processus de délivrance d'un certificat par une Autorité d'Enregistrement.

Certification croisée

Situation dans laquelle une AC KEYNECTIS et/ou une AE non KEYNECTIS (représentant un autre domaine de certification) délivre un certificat dont le porteur est l'autre AC ou AE.

Certified Document Services

Service offert par les partenaires Adobe, autorisant la signature numérique d'un document PDF Adobe par son auteur, à l'aide d'un identifiant numérique généré dans le cadre de l'ICP de CDS.

Chaîne de certificats

Liste ordonnée de certificats contenant un demandeur de certificat (utilisateur final) et des certificats d'AC.

Chiffrement

Processus permettant la transformation d'informations intelligibles en informations inintelligibles afin d'en protéger la confidentialité.

Clé privée

Clé mathématique tenue secrète par son détenteur. Elle permet de signer des informations électroniquement et de déchiffrer des données chiffrées à l'aide de la clé publique correspondante.

Clé publique



Clé mathématique pouvant être rendue publique et utilisée pour vérifier les signatures électroniques créées par la clé privée correspondante. Une clé publique permet également de chiffrer des données qui peuvent être déchiffrées par la clé privée correspondante.

Clé publique auto-signée

Structure de données conçue comme un certificat, mais signée par son propre porteur. À la différence d'un certificat, une clé publique auto-signée ne peut pas être utilisée pour authentifier une clé publique à d'autres parties.

Confidentialité

État des données importantes tenues secrètes et uniquement divulguées aux parties autorisées.

Confiance / Faire confiance

Accepter une signature numérique et effectuer des actions qui pourraient être dommageables si la signature numérique s'avérait non valide.

Confirmer

Déclarer ou indiquer par le biais d'une action (examen, enquête) que des données sont exactes et que des informations sont correctes.

Correspondre

Appartenir à la même paire de clés.

Cosigner

Signer avec un certificat CDS un document PDF Adobe précédemment signé.

Compromission

Violation (ou violation présumée) d'une mesure de sécurité, entraînant la divulgation d'informations confidentielles ou la perte de contrôle sur de telles informations (voir Intégrité des données).

Contrôles

Mesures prises pour veiller à l'intégrité et à la qualité d'un processus.

Cryptographie

Il existe deux types de cryptographie : la cryptographie symétrique dite à clé partagée et la cryptographie asymétrique dite à clés publique/privée.

Cryptographie à clé publique

Méthode cryptographique reposant sur une paire de clés mathématiques liées. La clé publique peut être transmise à toute personne souhaitant l'utiliser. Elle permet de chiffrer des informations ou de vérifier une signature numérique. La clé privée est tenue secrète pas son détenteur et permet de déchiffrer des informations ou de générer une signature numérique.

D

Délivrance de certificat

Action exécutée par une CA lorsqu'elle crée un certificat et en informe le demandeur (qui deviendra alors un abonné) défini dans le certificat.

Demandeur de certificat

Personne ou agent autorisé demandant la délivrance d'un certificat à clé publique à une AC.

Demande de certificat

Demande de délivrance d'un certificat émise par un demandeur de certificat à l'attention d'une AC.

Demande de certificat d'AC



Demande envoyée par une entité non KEYNECTIS aux services de certification électronique KEYNECTIS pour devenir une AC et pour recevoir un certificat d'AC.

Demande de Signature de Certificat (DSC)

Formulaire de demande de certificat pouvant être lu par une machine.

Dépositaire d'une part de secret

Détenteur autorisé d'un jeton physique contenant une donnée secrète.

Destinataire (d'une signature numérique)

Personne recevant une signature numérique et en position de lui faire confiance, que cette confiance soit accordée ou non.

Disponibilité

Mesure dans laquelle une entité habilitée peut raisonnablement accéder à ou utiliser des informations ou des processus, sur demande. La disponibilité rend possible l'accès contrôlé aux ressources et assure la prompte exécution d'opérations urgentes.

Distinguished Name (DN)

Ensemble de données identifiant une entité réelle, telle qu'une personne dans un environnement informatisé (CN = Common Name, nom usuel) (C = Country, pays) (S = State, état) (O = Organization, organisation) (OU = Organization Unit, département).

Document CDS

Document Acrobat signé à l'aide d'un certificat CDS.

Données

Programmes, fichiers et toute autre information stockés dans un ordinateur, transmis via celui-ci ou gérés par celui-ci.

Dongle

Dispositif cryptographique permettant la fabrication et le stockage sécurisés d'un certificat électronique. Il peut être utilisé sans lecteur et se connecte sur le port USB d'un ordinateur.

E / F

E-mail

Message envoyé, reçu ou transmis au format numérique via un système de communication informatisé (courrier électronique).

Émetteur de part de secret

Personne désignée par une AE pour créer et distribuer des données secrètes.

Employé permanent

Employé embauché pour une durée indéterminée, n'ayant pas été renvoyé ni suspendu, et qui ne fait actuellement l'objet d'aucune action disciplinaire de la part de son employeur.

Enregistrement

Information écrite sur un support matériel (un document) ou enregistrée sur un support électronique ou tout autre support, susceptible d'être récupérée sous une forme lisible. Le terme « enregistrement » s'applique à la fois à « document » et « message » (voir Document, Message).

Enregistrement

Processus de demande de certificat.

Entité finale

Voir Personne.



Expiration du certificat

Date et heure indiquées dans un certificat, indiquant la fin de la période de validité, sans que soit mentionnée la possibilité d'une révocation antérieure.

Extension de certificat

Champ additionnel d'un certificat, pouvant contenir des informations supplémentaires sur la clé publique certifiée, l'abonné, l'émetteur du certificat et/ou le processus de certification. Les extensions standard sont définies dans l'amendement 1 de la norme ISO/IEC 9594-8: 1995 (X.509).

Écriture

Informations d'un enregistrement accessibles et utilisables pour une référence ultérieure.

File Transfer Protocol (FTP)

Protocole d'application offrant un système de transfert des fichiers dans un environnement Internet.

G / H

Génération de clés

Processus de confiance de création d'une paire de clés (privée / publique).

Générer une paire de clés

Créer, dans un environnement de confiance, lors d'une demande de certificat, des clés privées dont les clés publiques correspondantes sont soumises à l'AC dans le cadre d'un processus prouvant la capacité du demandeur à utiliser la clé privée.

Hachage (fonction de hachage)

Fonction mathématique selon laquelle :

- un message permet d'obtenir le même résultat à chaque fois que l'algorithme est appliqué à ce même message ;
- il est mathématiquement impossible de déduire ou de reconstituer le message à partir du résultat produit par l'algorithme ;
- il est mathématiquement impossible d'identifier deux messages différents produisant le même résultat de hachage en utilisant le même algorithme.

Hiérarchie des certificats

Au sein des services de certification électronique, toutes les AC sont classées par catégorie en fonction de leur rôle dans la structure arborescente des AC. Une AC délivre et gère les certificats d'abonnés (utilisateurs finals) et/ou d'une ou plusieurs AC subordonnées. Une AC appartenant à une hiérarchie de confiance doit respecter des procédures uniformes, notamment en termes de nommage, de nombre maximum de niveaux, etc., afin d'assurer l'intégrité du domaine et ainsi de veiller à l'uniformité des processus de responsabilité, de vérifiabilité et de gestion via des processus opérationnels de confiance.

Hiérarchie d'ICP

Ensemble d'AC dont les fonctions sont organisées selon le principe de délégation de l'autorité, et entre elles en tant que subordonnées ou supérieures.

HSM

Module de Sécurité Matérielle voir MSM

Horodatage

Service indiquant la date et l'heure correctes d'un événement de manière fiable.

I / J

ICP de CDS



Politique, processus et technologie requis pour gérer, utiliser et faire confiance aux certificats liés à une AC Racine, intégrée dans les produits Acrobat, Reader et LiveCycle et utilisée parallèlement à la solution Certified Document Services.

ICP Adobe

Politique, processus et technologie requis pour gérer, utiliser et faire confiance aux certificats liés à l'AC Racine Adobe.

Identification

Processus de vérification de l'identité d'une personne. L'identification est facilitée par les certificats dans la cryptographie à clé publique.

Intégrité des données

Condition de données n'ayant subi aucune modification ni destruction non autorisée.

Identification numérique

Nom donné à un certificat.

Informations de champ d'enregistrement

Pays, code postal, âge et type des données incluses dans un certificat donné, en fonction des options sélectionnées par le demandeur.

Infrastructure à Clé Publique (ICP)

Ensemble de moyens techniques, humains, documentaires et contractuelles mis à la disposition des utilisateurs, ainsi que des systèmes cryptographiques asymétriques, pour assurer un environnement sécurisé pour les communications électroniques.

Information non vérifiée

Information d'un certificat envoyée par un demandeur à une AC qui n'a pas été confirmée par l'AC et pour laquelle l'AC n'offre aucune garantie hormis le fait qu'elle a été envoyée par le demandeur du certificat. Les informations sur les titres, les diplômes, les accréditations et les informations de champ d'enregistrement sont autant d'informations considérées comme non vérifiées, hormis mention contraire.

Intégrité

Voir Intégrité des données.

Jeton

Dispositif utilisé pour stocker la paire de clés d'un abonné ou d'une autorité de certification et la chaîne de certificats, ainsi que pour générer une signature.

K/L

Lien

Confirmation par une Autorité d'Enregistrement de la relation entre l'entité nommée et sa clé publique.

Liste des Certificats Révoqués (LCR)

Liste publiée régulièrement, portant la signature numérique d'une AC et contenant les certificats suspendus ou révoqués avant leur date d'expiration. Elle inclut généralement le nom de l'émetteur de la LCR, la date de publication, la date de la prochaine publication, le numéro de série des certificats révoqués, la date et l'heure précises de révocation et les motifs justifiant la révocation.

M

Matériel cryptographique

Dispositifs de sécurité contenant la clé privée de l'utilisateur, le certificat à clé publique et pouvant contenir une mémoire cache d'autres certificats, notamment tous ceux de la chaîne de certification de l'utilisateur.

**Menace**

Circonstance ou événement susceptible d'endommager un système. Citons notamment la destruction, la divulgation non autorisée, la modification de données et le déni de service.

Message

Représentation numérique d'informations ; enregistrement informatisé.

MSM

Module de Sécurité Matérielle voir HSM

Module cryptographique

Mise en œuvre fiable d'un système cryptographique, permettant le chiffrement et le déchiffrement des données en toute sécurité.

Mot de passe

Information d'authentification confidentielle, composée d'une chaîne de caractères utilisée pour accéder à une ressource.

N / O**Nom**

Ensemble d'attributs d'identification utilisés pour décrire un certain type d'entité.

Nom du porteur

Valeur sans équivoque contenue dans le champ du nom du porteur lié à la clé publique.

Nom Distinctif

Nom caractéristique. Voir Distinguished Name.

Nom distinctif relatif (RDN, Relative Distinguished Name)

Ensemble d'attributs, notamment le nom distinctif d'une entité, permettant de distinguer cette entité des autres de même type.

Nommage de l'identité

Utilisation de la section d'extension « Organization Unit » (OU =) dans un certificat X.509 v3.

Nommage

Attribution d'identifiants descriptifs à des objets d'un type particulier. Cette opération est effectuée par une autorité, qui respecte des procédures d'attribution spécifiques et qui conserve des enregistrements spécifiques en rapport avec les procédures d'enregistrement identifiées.

Nom sans équivoque

Voir Nom distinctif.

Non-répudiation

Apporte la preuve de l'origine ou de la transmission de données afin de protéger l'émetteur contre toute fausse déclaration de non-réception par le destinataire, et de protéger le destinataire contre toute fausse déclaration de non-transmission par l'émetteur. Apporte une preuve en cas de désaccord.

Notifier

Communiquer des informations spécifiques à une autre personne, conformément à la présente PC/DPC et à la législation applicable.

Numéro de série

Voir Numéro de série du certificat.

Numéro de série du certificat



Valeur permettant d'identifier sans aucune ambiguïté un certificat délivré par une AC.

Organisation

Entité à laquelle un utilisateur est affilié. L'organisation elle-même peut être un utilisateur.

P / Q

Paire de clés

Clé privée et clé publique correspondante. Une clé publique permet d'authentifier une signature numérique créée par l'utilisation de la clé privée correspondante. Par ailleurs, selon le type d'algorithme utilisé, les composantes d'une paire de clés peuvent également chiffrer et déchiffrer des informations à des fins de confidentialité, auquel cas seule la clé privée autorise la lecture des informations chiffrées à l'aide de la clé publique correspondante.

Part de secret

Partie d'un secret chiffré distribué entre un certain nombre de jetons physiques.

Partage de secret

Processus de distribution de parts de secret d'une clé privée à un certain nombre de dépositaires, en fonction de la tolérance du partage de la clé.

Parties

Entités dont les droits et les obligations doivent être régis par une PC/DPC. Il peut s'agir d'abonnés, d'AC ou de tierces parties de confiance.

Partie utilisatrice

Individu utilisant un produit Adobe Acrobat pour valider un document certifié.

Personne

Être humain ou organisation (ou dispositif sous le contrôle d'un être humain ou d'une organisation) capable de signer ou de vérifier un message.

Phrase challenge

Ensemble de chiffres et/ou de lettres choisi par un demandeur de certificat, envoyé à l'Autorité d'Enregistrement avec une demande de certificat et utilisé par cette AE pour authentifier le demandeur, conformément aux exigences définies dans la présente PC/DPC.

Plates-formes prises en charge.

Logiciels de signature de document au format PDF ISO mettant en oeuvre l'ensemble des contrôles et éléments constituant la signature électronique permettant aux produits Adobe de vérifier de signature de réaliser le contrôle de validité du certificat (OCSPet CRL) et de l'horodatage en mode non connecté.

Politique de Certification (PC)

Également appelée Déclaration des Pratiques de Certification. Définit les procédures de génération et de gestion de certificats, ainsi que la relation de confiance établie entre l'utilisateur final et le porteur du certificat.

Politique et Déclaration des Pratiques de Certification (PC/DPC)

Document, révisé régulièrement, énonçant les pratiques utilisées par une AC pour la délivrance de certificats.

Politique de sécurité

Document regroupant les besoins et meilleures pratiques en termes de processus de sécurité et de protection assurés par un système de confiance, venant renforcer la PC/DPC.

Présence physique

© KEYNECTIS Tous droits réservés.

Réf. CPS_KEYNECTISCDSCA_FR_V1.2.doc



Acte d'apparition (physique, plutôt que virtuelle ou figurative) devant une AE ou son représentant pour prouver son identité, prérequis à la délivrance d'un certificat sous certaines conditions.

Promesse

Accord ou conduite dont l'objectif est d'indiquer l'intention générale d'une Autorité d'Enregistrement, et s'accompagnant d'un effort de bonne foi, d'offrir un service spécifique et d'assurer sa gestion. Une promesse n'est pas nécessairement assortie de la garantie selon laquelle les services seront pleinement dispensés et donneront satisfaction. Les promesses sont distinctes de l'assurance et des garanties, à moins que cela ne soit expressément indiqué.

Publier

Enregistrer et classer des informations dans les archives de référence afin de divulguer et de rendre publiques certaines informations conformément à la présente PC/DPC et à la législation applicable.

Parties utilisatrices

Destinataires qui agissent en faisant confiance à un certificat ou à une signature numérique.

Période de validité

Période commençant à la date et à l'heure de délivrance d'un certificat (ou plus tard si cela est spécifié dans le certificat) et se terminant à la date et à l'heure d'expiration ou de révocation du certificat.

Plates-formes prises en charge:

Logiciels sous licence Adobe (Adobe reader 6+, Adobe Acrobat 7+, livec Cycle ES Digital Signature) permettant de signer et de vérifier les signatures des documents PDF avec les certificats CDS

Porteur

Détenteur d'une clé privée correspondant à une clé publique. Le terme « porteur » fait référence à la fois à l'équipement et au dispositif contenant la clé privée et à la personne, le cas échéant, qui contrôle cet équipement ou ce dispositif. Le porteur est désigné par un nom sans équivoque lié à une clé publique contenue dans le certificat du porteur.

Qualificateur

Syntaxe de données facilitant la représentation d'un ensemble de données qui limite la signification de la présente PC/DPC. La valeur d'un qualificateur accroît l'extension de la Politique de Certification de tous les certificats, conformément aux règles définies par la norme X.509.

R

Racine

AC qui délivre le premier certificat dans la chaîne de certification. La clé publique de l'AC racine doit être préalablement connue de l'utilisateur du certificat afin que soit validée la chaîne de certification.

Révocation de certificat

Voir Révoquer un certificat.

Ressource cryptographique

Ressource matérielle dans laquelle sont stockées les clés privées.

Renouvellement

Processus d'obtention d'un nouveau certificat de classe et type identiques que le certificat antérieur après l'expiration de celui-ci.

Répudiation

Refus ou tentative de refus de la part d'une entité impliquée dans une communication de reconnaître sa participation dans tout ou partie de cette communication.

Révoquer un certificat



Processus d'interruption définitive de la validité d'un certificat à partir d'un moment précis (par exemple, à la suite de la compromission d'une clé privée).

Racine de confiance

Une racine de confiance est une clé publique dont le lien à une AC a été confirmé par un utilisateur ou un administrateur système. Les logiciels et systèmes effectuant des tâches d'authentification à l'aide d'un processus cryptographique et de certificats à clé publique supposent que la valeur de la clé a été obtenue correctement. La confiance est garantie par un accès constant de la racine depuis une base d'archives de confiance, qui ne peut être modifiée que par des administrateurs de confiance identifiés.

Rapport d'audit de confiance

Rapport électronique horodaté électroniquement

Rôle de confiance

Un rôle de confiance est détenu par une personne qui a accès à ou contrôle des opérations cryptographiques susceptibles d'affecter la délivrance, l'utilisation ou la révocation de certificats par l'AC, notamment qui a accès à des opérations faisant l'objet de restrictions sur les archives de référence KEYNECTIS. Des règles de sécurité supplémentaires, définies par le service de sécurité KEYNECTIS complètent la définition du rôle de confiance (par ex. : dépositaire du secret).

RSA

Système cryptographique à clé publique inventé par Rivest, Shamir et Adelman.

S

Services de certification électronique

Services fournis par un prestataire de services de certification (électronique). Citons par exemple la délivrance de certificats électroniques, l'offre de services d'annuaire de certification, la publication de LCR, la fourniture de jetons d'horodatage, l'archivage, etc.

Signature numérique

Transformation d'un message à l'aide d'un système de chiffrement asymétrique permettant au détenteur du message initial et de la clé publique du signataire de déterminer précisément si la transformation a été effectuée à l'aide de la clé privée correspondant à la clé publique du signataire et si le message a été modifié depuis la transformation.

S/MIME

Spécification de courrier électronique protégé exploitant une syntaxe de message cryptographique dans un environnement Internet.

Sécurité

État de ce qui est protégé contre tout accès non autorisé ou toute perte ou tout événement incontrôlé. Dans la pratique, il est impossible de parvenir à une sécurité absolue et la sécurité de tout système est relative.

Services de sécurité

Services fournis par un ensemble de mécanismes de sécurité. Citons notamment le contrôle d'accès, la confidentialité et l'intégrité des données.

Serveur

Système informatisé répondant aux requêtes de systèmes clients.

Signer

Créer une signature numérique pour un message ou apposer une signature sur un document.

Signature

Méthode adoptée ou utilisée par l'auteur d'un document pour s'identifier. Cette méthode peut être acceptée par le destinataire ou être utilisée systématiquement en fonction des circonstances.

**Signataire**

Personne qui crée une signature numérique afin de signer un message ou un document.

Système de confiance

Matériel informatique, logiciels et procédures protégés contre toute intrusion ou mauvais usage ; offre un niveau raisonnable de disponibilité ; apte à exécuter les fonctions qui lui ont été dévolues ; renforce la politique de sécurité applicable.

T / U**Tierce partie de confiance**

Tierce partie indépendante et impartiale qui contribue à la sécurité et à la fiabilité ultime des transferts d'informations informatisés.

Transaction

Transfert d'informations professionnelles par voie informatique, qui consiste en des processus spéciaux facilitant la communication sur des réseaux mondiaux.

Type de certificat

Propriétés définies d'un certificat limitant son rôle aux applications associées à ce type exact.

UH

Unité d'Horodatage. Entité chargée de la signature de jetons d'horodatage à l'aide d'un certificat.

Universal Resource Locator (URL)

Dispositif standard d'identification et de localisation de certains enregistrements et d'autres ressources se trouvant sur le Web.

Utilisateur

Entité autorisée qui utilise un certificat en tant que demandeur, destinataire ou tierce partie de confiance. N'inclut pas l'AC qui délivre le certificat.

V**Validation d'un certificat**

Processus effectué par un destinataire ou une tierce partie de confiance pour confirmer la validité d'un certificat et pour confirmer la validité de celui-ci à la date et à l'heure de la création d'une signature numérique.

Validation d'une demande de certificat

Processus exécuté par l'AC à la suite de la soumission d'une demande de certification. Il s'agit d'une condition préalable à l'approbation de la demande et à la délivrance d'un certificat.

Validation d'une chaîne de certificats

Pour chaque certificat de la chaîne, processus exécuté par le destinataire ou la tierce partie de confiance pour :

- authentifier la clé publique (de chaque certificat) ;
- confirmer la validité de chaque certificat ;
- s'assurer que le certificat a été délivré pendant sa période de validité et que toutes les parties de confiance ont agi conformément à la PC/DPC

Vérifier (une signature numérique)

Déterminer de manière précise que :

- la signature numérique a été créée pendant la période de validité du certificat par la clé privée correspondant à la clé publique contenue dans le certificat ;
- le message n'a pas été modifié depuis la création de la signature numérique.

**Violation**

Violation (ou violation présumée) d'une mesure de sécurité (par ex. divulgation ou divulgation présumée d'informations confidentielles, perte de contrôle sur ce type d'informations).

W/X/Y/Z**World Wide Web (WWW)**

Système d'information distribué reposant sur des structures hypertextes, permettant à l'utilisateur de créer, de modifier ou de parcourir des documents hypertextes. Support de publication graphique et de visualisation de documents.

X.509

Norme UIT-T (Union Internationale des Télécommunications-T) relative aux certificats. Désigne des certificats contenant ou pouvant contenir des extensions.

