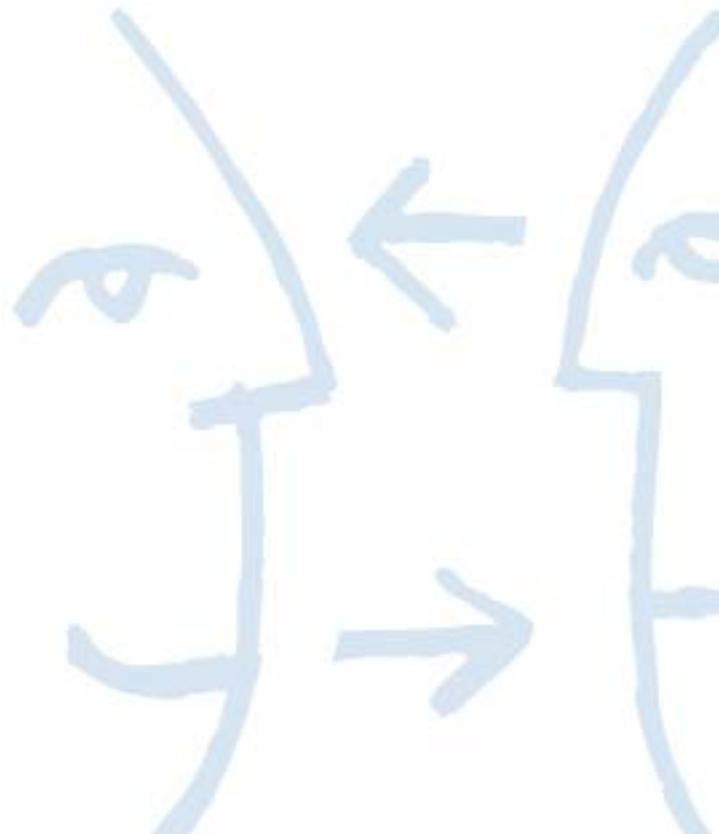




**KEYNECTIS**

■ **POLITIQUE DE CERTIFICATION  
DE L'AC KEYNECTIS SHARED**

Date : 02/04/2009





## POLITIQUE DE CERTIFICATION

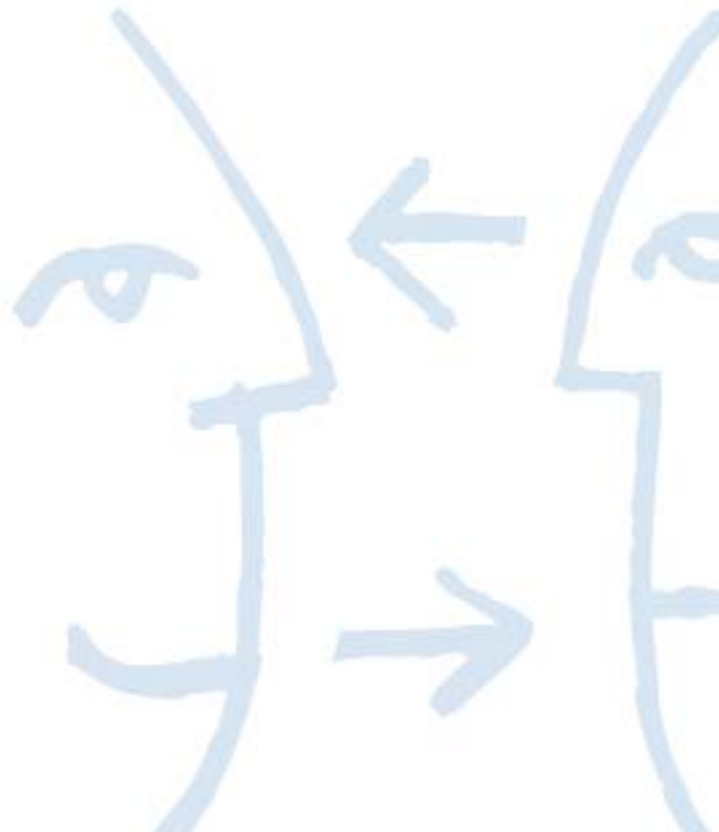
---

<b>Objet:</b>	Ce document consiste en la politique de certification de l'AC KEYNECTIS SHARED
---------------	--

<b>Numéro de version:</b>	0.4	<b>Nombre de pages:</b>	44
<b>Etat du document:</b>	<input checked="" type="checkbox"/> Projet	<input type="checkbox"/> Version finale	
<b>Rédacteur :</b>	Emmanuel Montacutelli	KEYNECTIS	

<b>Diffusion:</b>	<input checked="" type="checkbox"/> Externe	<input checked="" type="checkbox"/> Interne KEYNECTIS	
Utilisateurs des certificats délivrés par l'AC KEYNECTIS SHARED			KEYNECTIS

<b>Historique:</b>				
Date	Version	Rédacteur	Commentaires	Validé par
02/04/2009	0.4	RPI	Compléments	JYF
01/04/2009	0.3	MLAB	Compléments	
24/03/2009	0.2	JYF	Compléments	
23/02/2009	0.1	EM	Création du document	JYF



## SOMMAIRE

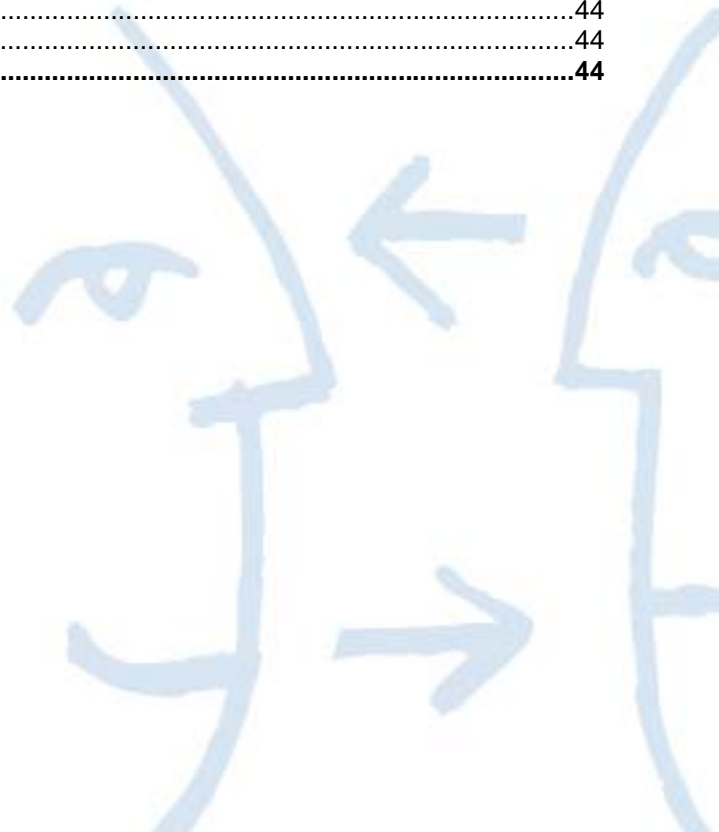
<b>AVERTISSEMENT</b>	<b>8</b>
<b>1 INTRODUCTION</b>	<b>9</b>
1.1 Généralités	9
1.2 Nom du Document et Identification	9
1.3 Les composantes de l'IGC	9
1.3.1 Autorité Administrative de KEYNECTIS (AAK)	10
1.3.2 Autorité de Certification (AC)	10
1.3.3 Autorité d'Enregistrement (AE)	10
1.3.4 Service de Publication (SP)	10
1.3.5 Opérateur de Service de Certification (OSC)	10
1.3.6 Porteur	10
1.3.7 Autres participants	11
1.3.7.1 Client	11
1.3.7.2 Utilisateur de certificat (UC)	11
1.3.7.3 Communauté d'utilisateurs	11
1.4 Utilisation des certificats	11
1.4.1.1 Certificat de l'AC	11
1.4.1.2 Certificat Porteur	11
1.4.2 Utilisation interdite des certificats	11
1.5 Application de la politique	12
1.5.1 Organisme responsable de la présente politique	12
1.5.2 Personne responsable	12
1.5.3 Personne déterminant la conformité de l'implémentation de la présente PC/DPC	12
1.5.4 Procédure d'approbation du présent document	12
1.6 Définitions et Acronymes	12
1.6.1 Définitions	12
1.6.2 Acronymes	14
<b>2 ANNUAIRES ET SERVICES DE PUBLICATION</b>	<b>16</b>
2.1 Service de publication	16
2.2 Informations publiées	16
2.3 Heure et fréquence de publication	16
2.4 Contrôle d'accès au service de publication	16
<b>3 IDENTIFICATION ET AUTHENTIFICATION</b>	<b>17</b>
3.1 Nommage	17
3.1.1 Types de noms	17
3.1.1.1 Certificat AC	17
3.1.1.2 Certificat Porteur	17
3.1.2 Utilisation de noms explicites	17
3.1.3 Anonymat ou utilisation de pseudonyme	17
3.1.4 Règles d'interprétations des différentes formes de noms	17
3.1.5 Unicité des noms	17
3.1.6 Reconnaissance, vérification, et rôle des noms de marques déposées	18
3.2 Vérification initiale d'identité	18
3.2.1 Preuve de possession de la clé privée	18
3.2.2 Vérification de l'identité des organisations	18
3.2.2.1 Client	18
3.2.2.2 Porteur	18
3.2.3 Vérification de l'identité des personnes	18
3.2.4 Informations non vérifiées	18
3.2.5 Validation de l'autorité d'un porteur	18
3.2.6 Critères de reconnaissance	18
3.3 Vérifications aux fins de renouvellement de clés	18

3.3.1	Vérifications aux fins de renouvellement de clés en situation normale .....	18
3.3.2	Vérifications aux fins de renouvellement de clés après révocation du certificat .....	18
<b>3.4</b>	<b>Vérifications aux fins de révocation.....</b>	<b>19</b>
<b>4</b>	<b>EXIGENCES OPERATIONNELLES .....</b>	<b>20</b>
<b>4.1</b>	<b>Types de certificat.....</b>	<b>20</b>
4.1.1	Origine de la demande de certificat .....	20
4.1.2	Procédure d'enregistrement et responsabilités .....	20
<b>4.2</b>	<b>Traitement d'une demande de certificat.....</b>	<b>20</b>
4.2.1	Identification et authentification.....	20
4.2.2	Approbation ou rejet d'une demande de certificat .....	20
4.2.3	Durée de traitement d'une demande de certificat.....	20
<b>4.3</b>	<b>Emission d'un certificat .....</b>	<b>20</b>
4.3.1	Actions effectuées par l'AC pendant l'émission d'un certificat.....	20
4.3.2	Notification de l'émission d'un certificat .....	20
<b>4.4</b>	<b>Acceptation d'un certificat .....</b>	<b>20</b>
4.4.1	Procédure d'acceptation d'un certificat .....	20
4.4.2	Publication d'un certificat par l'AC.....	20
4.4.3	Notification de l'émission d'un certificat par l'AC à d'autres entités .....	20
<b>4.5</b>	<b>Utilisation des bi-clés et des certificats .....</b>	<b>20</b>
4.5.1	Utilisation des bi-clés et des certificats .....	20
4.5.2	Utilisation des clés publiques et des certificats par les tierces parties .....	21
<b>4.6</b>	<b>Demande d'un nouveau certificat.....</b>	<b>21</b>
<b>4.7</b>	<b>Changement de clés (ou certification d'une nouvelle clé publique).....</b>	<b>21</b>
<b>4.8</b>	<b>Modification d'un certificat.....</b>	<b>21</b>
<b>4.9</b>	<b>Révocation d'un certificat.....</b>	<b>21</b>
4.9.1	Motif de révocation d'un certificat .....	21
4.9.2	Origine d'une demande de révocation .....	21
4.9.3	Procédure de demande de révocation.....	22
4.9.4	Délai accordé au porteur pour formuler la demande de révocation .....	22
4.9.5	Délai de traitement d'une révocation .....	22
4.9.6	Exigences de vérification de révocation pour les tierces parties .....	22
4.9.7	Fréquences de publication des LCR.....	22
<b>4.10</b>	<b>Service d'état des certificats .....</b>	<b>22</b>
4.10.1	Caractéristiques opérationnelles.....	22
<b>4.11</b>	<b>Fin de la relation entre Le porteur et l'AC.....</b>	<b>22</b>
<b>4.12</b>	<b>Séquestre et recouvrement de clés.....</b>	<b>23</b>
<b>5</b>	<b>MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN ŒUVRE .....</b>	<b>24</b>
<b>5.1</b>	<b>Sécurité physique.....</b>	<b>24</b>
5.1.1	Situation géographique .....	24
5.1.2	Accès physique.....	24
5.1.3	Energie et air conditionné .....	24
5.1.4	Exposition aux liquides .....	24
5.1.5	Prévention et protection incendie.....	24
5.1.6	Mise hors service des supports .....	24
5.1.7	Sauvegardes hors site .....	24
<b>5.2</b>	<b>Mesures de sécurité procédurales .....</b>	<b>24</b>
5.2.1	Rôles de confiance .....	24
5.2.2	Nombre de personnes nécessaires à l'exécution de tâches sensibles .....	25
5.2.3	Identification et authentification des rôles.....	25
<b>5.3</b>	<b>Mesures de sécurité vis-à-vis du personnel.....</b>	<b>25</b>
5.3.1	Qualifications, compétence et habilitations requises .....	25
5.3.2	Procédures de vérification des antécédents.....	25
5.3.3	Exigences en matière de formation initiale .....	25
5.3.4	Exigences et fréquence en matière de formation continue .....	25
5.3.5	Gestion des métiers .....	25
5.3.6	Sanctions en cas d'actions non autorisées.....	25
5.3.7	Exigences vis-à-vis du personnel des prestataires externes.....	25
5.3.8	Documentation fournie au personnel.....	26

<b>5.4</b>	<b>Procédures de constitution des données d'audit</b>	<b>26</b>
5.4.1	Type d'événements à enregistrer	26
5.4.2	Processus de journalisation	27
5.4.3	Protection des journaux d'événements	27
5.4.4	Procédures de sauvegarde des journaux d'événements	27
5.4.5	Système de collecte des journaux d'événements	27
5.4.6	Evaluation des vulnérabilités	27
<b>5.5</b>	<b>Archivage des données</b>	<b>27</b>
5.5.1	Type de données archivées	27
5.5.2	Période de conservation des archives	27
5.5.3	Protection des archives	27
5.5.4	Exigences d'horodatage des données	28
5.5.5	Système de collecte des archives	28
5.5.6	Procédures de récupération et de vérification des archives	28
<b>5.6</b>	<b>Renouvellement de bi-clé</b>	<b>28</b>
5.6.1	Certificat d'AC	28
5.6.2	Certificat de Porteur	28
<b>5.7</b>	<b>Compromission et plan de reprise</b>	<b>28</b>
5.7.1	Procédures en cas d'incident et de compromission	28
5.7.2	Corruption des ressources informatiques, des logiciels, et/ou des données	29
5.7.3	Procédures en cas de compromission de la clé privée d'une entité	29
5.7.4	Capacités de reprise d'activité à la suite d'un sinistre	29
<b>5.8</b>	<b>Fin de vie d'AC</b>	<b>29</b>
<b>6</b>	<b>MESURES TECHNIQUES DE SECURITE</b>	<b>30</b>
<b>6.1</b>	<b>Génération et installation des bi-clés</b>	<b>30</b>
6.1.1	Génération des bi-clés	30
6.1.1.1	Bi-clé d'AC	30
6.1.1.2	Bi-clé de Porteur	30
6.1.2	Fourniture de la clé privée au porteur	30
6.1.3	Fourniture de la clé publique à l'AC	30
6.1.4	Fourniture de la clé publique d'AC aux tierces parties	30
6.1.5	Taille de clés	30
6.1.6	Production des paramètres des clés publiques et contrôle de qualité	30
6.1.7	Utilisation de la clé (selon le champ "key usage" du certificat X 509 V3)	30
<b>6.2</b>	<b>Protection des clés privées et normes relatives au module cryptographique</b>	<b>31</b>
6.2.1	Normes applicables aux ressources cryptographiques et contrôles	31
6.2.2	Contrôle de la clé privée par de multiples personnes	31
6.2.3	Séquestre de clé privée	31
6.2.4	Sauvegarde de clé privée	31
6.2.4.1	AC	31
6.2.4.2	Porteur	31
6.2.5	Archivage de clé privée	31
6.2.6	Importation / exportation d'une clé privée	31
6.2.7	Stockage d'une clé privée dans un module cryptographique	31
6.2.8	Méthode d'activation d'une clé privée	31
6.2.8.1	AC	31
6.2.8.2	Porteur	31
6.2.9	Méthode de désactivation d'une clé privée	31
6.2.9.1	AC	32
6.2.9.2	Porteur	32
6.2.10	Méthode de destruction d'une clé privée	32
6.2.10.1	AC	32
6.2.10.2	Porteur	32
6.2.11	Certification des ressources cryptographiques	32
<b>6.3</b>	<b>Autres aspects de la gestion des bi-clés</b>	<b>32</b>
6.3.1	Archivage des clés publiques	32
6.3.2	Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés	32
6.3.2.1	AC	32
6.3.2.2	Porteur	32
<b>6.4</b>	<b>Données d'activation</b>	<b>32</b>

6.4.1	Génération et installation des données d'activation .....	32
6.4.1.1	AC.....	32
6.4.1.2	Porteur.....	32
6.4.2	Protection des données d'activation .....	33
6.4.2.1	AC.....	33
6.4.2.2	Certificat porteur .....	33
6.4.3	Autres aspects touchant aux données d'activation.....	33
<b>6.5</b>	<b>Mécanismes de sécurité des systèmes informatiques .....</b>	<b>33</b>
6.5.1	Exigences techniques de sécurité des ressources informatiques .....	33
6.5.2	Indice de sécurité informatique .....	33
<b>6.6</b>	<b>Contrôles techniques du système pendant son cycle de vie .....</b>	<b>33</b>
6.6.1	Contrôle des développements des systèmes .....	33
6.6.2	Contrôles de gestion de la sécurité .....	34
6.6.3	Contrôle de sécurité du système pendant son cycle de vie .....	34
<b>6.7</b>	<b>Mécanismes de sécurité du réseau .....</b>	<b>34</b>
<b>6.8</b>	<b>Horodatage/Système de datation .....</b>	<b>34</b>
<b>7</b>	<b>CERTIFICATS, CRL, ET PROFILS OCSP .....</b>	<b>35</b>
<b>7.1</b>	<b>Profil de Certificats.....</b>	<b>35</b>
7.1.1	Extensions de Certificats .....	35
7.1.1.1	Certificat AC .....	35
7.1.1.2	Champs de base du certificat.....	35
7.1.1.3	Extension du certificat .....	35
7.1.1.4	Certificat Porteur.....	35
7.1.1.5	Extension du certificat .....	36
7.1.2	Identifiant d'algorithmes .....	36
7.1.3	Formes de noms .....	36
7.1.4	Identifiant d'objet (OID) de la Politique de Certification .....	36
7.1.5	Extensions propres à l'usage de la Politique .....	36
7.1.6	Syntaxe et Sémantique des qualificatifs de politique .....	36
7.1.7	Interprétation sémantique de l'extension critique "Certificate Policies" .....	36
<b>7.2</b>	<b>Profil de LCR.....</b>	<b>36</b>
7.2.1	LCR et champs d'extensions des LCR .....	36
<b>8</b>	<b>CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS .....</b>	<b>37</b>
<b>8.1</b>	<b>Fréquence et motifs des audits .....</b>	<b>37</b>
<b>8.2</b>	<b>Identité / Qualification des auditeurs .....</b>	<b>37</b>
<b>8.3</b>	<b>Lien entre l'auditeur et l'entité contrôlée .....</b>	<b>37</b>
<b>8.4</b>	<b>Points couverts par l'évaluation .....</b>	<b>37</b>
<b>8.5</b>	<b>Mesures prises en cas de non-conformité .....</b>	<b>37</b>
<b>8.6</b>	<b>Communication des résultats .....</b>	<b>37</b>
<b>9</b>	<b>AUTRES QUESTIONS COMMERCIALES ET JURIDIQUES .....</b>	<b>38</b>
<b>9.1</b>	<b>Tarifs.....</b>	<b>38</b>
9.1.1	Frais d'émission et de renouvellement de certificats.....	38
9.1.2	Frais d'accès aux certificats.....	38
9.1.3	Frais d'accès aux LCR et aux informations d'état des certificats .....	38
9.1.4	Frais pour d'autres services.....	38
9.1.5	Politique de remboursement.....	38
<b>9.2</b>	<b>Responsabilité financière .....</b>	<b>38</b>
9.2.1	Couverture par les assurances .....	38
9.2.2	Autres ressources .....	38
9.2.3	Couverture et garantie concernant les entités utilisatrices .....	38
<b>9.3</b>	<b>Confidentialité des informations .....</b>	<b>38</b>
9.3.1	Informations confidentielles .....	38
9.3.2	Information considérées comme non confidentielles.....	38
9.3.3	Obligation de protection des informations confidentielles .....	38
<b>9.4</b>	<b>Confidentialité des informations à caractère personnel .....</b>	<b>39</b>
9.4.1	Plan de confidentialité .....	39
9.4.2	Information considérées comme personnelles .....	39

9.4.3	Information non considérées comme n'étant pas à caractère personnel .....	39
9.4.4	Obligation de protection des informations à caractère personnel .....	39
9.4.5	Consentement exprès et préalable à l'utilisation de données à caractère personnel .....	39
9.4.6	Divulgaration due à un processus judiciaire ou administratif .....	39
9.4.7	Autres motifs de divulgation de données à caractère personnel .....	40
<b>9.5</b>	<b>Droits relatifs à la propriété intellectuelle .....</b>	<b>40</b>
<b>9.6</b>	<b>Obligations et garanties .....</b>	<b>40</b>
9.6.1	Obligations communes .....	40
9.6.2	Obligations et garanties de l'AAK .....	40
9.6.3	Obligations et garanties de l'AC .....	40
9.6.4	Obligations de l'AE .....	41
9.6.5	Obligations et garanties du porteur .....	41
9.6.6	Obligations et garanties du SP .....	41
9.6.7	Obligations et garanties des autres participants .....	41
9.6.7.1	Obligations et garanties du Client .....	41
<b>9.7</b>	<b>Déni de garanties .....</b>	<b>41</b>
<b>9.8</b>	<b>Limites de responsabilité .....</b>	<b>42</b>
<b>9.9</b>	<b>Indemnités .....</b>	<b>43</b>
<b>9.10</b>	<b>Durée et fin anticipée de validité de la PC .....</b>	<b>43</b>
9.10.1	Durée .....	43
9.10.2	Résiliation .....	43
9.10.3	Effets de la résiliation et survie .....	43
<b>9.11</b>	<b>Amendements .....</b>	<b>43</b>
9.11.1	Procédure pour apporter un amendement .....	43
9.11.2	Mécanisme et délais des notifications .....	43
9.11.3	Motifs selon lesquels un OID doit être changé .....	43
<b>9.12</b>	<b>Règlement des différends .....</b>	<b>43</b>
<b>9.13</b>	<b>Droit applicable .....</b>	<b>44</b>
<b>9.14</b>	<b>Conformité au droit applicable .....</b>	<b>44</b>
<b>9.15</b>	<b>Divers .....</b>	<b>44</b>
9.15.1	Totalité de l'entente .....	44
9.15.2	Affectation .....	44
9.15.3	Divisibilité .....	44
9.15.4	Exonération des droits .....	44
9.15.5	Force majeure .....	44
<b>9.16</b>	<b>Autres dispositions .....</b>	<b>44</b>



## AVERTISSEMENT

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

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

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

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

L'utilisation de la présente politique de certification, propriété de la société KEYNECTIS, a été concédée au Client dans la cadre du contrat de service conclu avec KEYNECTIS pour la mise en œuvre du service de certification électronique associé à l'utilisation de l'AC SHARED mis à disposition par KEYNECTIS.

## 1 INTRODUCTION

### 1.1 Généralités

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

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

KEYNECTIS dispose d'une Autorité de Certification, nommée Autorité de Certification KEYNECTIS Shared et notée AC dans la suite de ce document qui certifie des porteurs conformément à la présente Politique de Certification (PC) pour le compte de Clients de KEYNECTIS.

<b>KEYNECTIS SHARED CA</b>
--------------------------------

La présente PC est appliquée par l'AC et les Clients de KEYNECTIS dans le cadre de la gestion du cycle de vie des certificats électroniques délivrés par l'Autorité de Certification KEYNECTIS Shared. Chaque Client de KEYNECTIS a la responsabilité d'identifier et de définir un ensemble de porteurs et d'utilisateurs auxquels s'appliquera la présente PC. Chaque Client définit sa communauté d'utilisateurs qui agissent suivant des règles qui lui sont propres.

La présente Politique de Certification (PC) est conforme au RFC 3647 « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF).

### 1.2 Nom du Document et Identification

La présente PC appelée : « PC\_AC\_SHARED » est la propriété de KEYNECTIS. Cette PC est enregistrée par un numéro d'identifiant d'objet (OID) qui est : 1.3.6.1.4.1.22234.2.1.3.2.

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

### 1.3 Les composantes de l'IGC

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

- Service d'enregistrement et de demande de certificat : ce service récupère et vérifie les informations d'identification du porteur, avant de transmettre la demande de certificat au service de génération de certificat. Ce service est mise en œuvre par l'Autorité d'enregistrement (noté AE) ;
- Service de génération de certificat : ce service génère les certificats électroniques des porteurs à partir des informations transmises par le service de service d'enregistrement et de demande de certificat. Ce service est mise en œuvre par l'OSC ;
- Service de retrait de certificat : ce service permet au porteur ou au Client de retirer les certificats. Ce service est mise en œuvre par l'Autorité d'enregistrement (noté AE) et l'opérateur de service de certification (noté OSC) ;
- Service de révocation de certificats : ce service traite les demandes de révocation des certificats de porteurs et détermine les actions à mener, dont la génération des Liste de Certificats Révoqués (LCR). Ce service est mise en œuvre à la fois par l'AE et l'OSC ;

- Service de Publication : ce service met à disposition les informations nécessaires à l'utilisation des certificats émis par l'AC (PC publiée par l'AC, ...), ainsi que les résultats des traitements du service de gestion des révocations (LCR). Ce service est mise en œuvre par l'OSC.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus afin de délivrer des certificats aux porteurs. La Déclaration des Pratiques de Certification (noté DPC) donnera les détails des pratiques de l'AC et de l'AE dans cette perspective.

Chaque Client complète la DPC générique de KEYNECTIS avec les procédures d'enregistrement qui sont dédiées à la communauté d'utilisateurs qu'il définit.

### **1.3.1 Autorité Administrative de KEYNECTIS (AAK)**

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

### **1.3.2 Autorité de Certification (AC)**

L'AC génère des certificats et révoque des certificats à partir de demandes qui lui sont envoyées par les AE des Clients. Elle s'appuie sur un Opérateur de Service de Certification (OSC) afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie d'un certificat.

L'AC agit conformément à la présente PC et la DPC associée.

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

### **1.3.3 Autorité d'Enregistrement (AE)**

L'ensemble des services d'enregistrement est délégué à des entités liées contractuellement à KEYNECTIS dans le cadre de la présente Politique, ces entités sont ci-après appelés Clients.

L'Autorité d'Enregistrement (AE) est utilisée pour la mise en œuvre des services d'enregistrement des demandes de certificats, de retrait et de révocation des certificats. L'AE est chargée d'authentifier et d'identifier les porteurs.

Le Client est AE au sens de la responsabilité pour les opérations d'identification et d'authentification des porteurs de certificats pour les services d'AE qu'il met en œuvre.

L'AE agit conformément à la présente PC et à la DPC associée qui sont établies par l'AAK et aux procédures spécifiques élaborées par le Client.

### **1.3.4 Service de Publication (SP)**

Le SP est utilisé pour la mise en œuvre du service de publication.

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

### **1.3.5 Opérateur de Service de Certification (OSC)**

L'OSC assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC. L'OSC est techniquement dépositaire de la clé privée de l'AC utilisée pour la signature des certificats. Sa responsabilité se limite au respect des procédures que l'AC définit afin de répondre aux exigences de la présente PC.

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

### **1.3.6 Porteur**

Un porteur est une personne physique qui met en œuvre une clé privée correspondant à une clé publique certifiée par l'AC, afin de réaliser des fonctions de sécurité (signature, authentification, ...) dans le cadre d'applications métier identifiées par le Client.

### **1.3.7 Autres participants**

#### **1.3.7.1 Client**

Le Client définit une communauté d'utilisateurs dans le cadre unique d'applications qui lui sont propres et dont il a la responsabilité. Le Client ne peut pas définir de communauté d'utilisateurs pour des applications qui ne sont pas de sa responsabilité directe.

Le client est l'entité qui identifie et authentifie un ensemble de porteurs et d'utilisateurs de certificat (UC) pour ses besoins d'applications métiers. Le Client est AE uniquement pour cet ensemble de porteur et d'UC. Le Client s'organise et définit ses propres procédures d'enregistrement (authentification et identification) pour les services qu'il met en œuvre et complète ainsi la DPC générique élaborée par l'AAK. Il peut déléguer tout ou partie des procédures qu'il utilise.

#### **1.3.7.2 Utilisateur de certificat (UC)**

L'utilisateur de certificat appartient à la même communauté d'utilisateurs que le porteur et qui est définie par le Client. L'utilisateur de certificat est une machine ou une personne qui valide le certificat d'un porteur dans le cadre des applications métiers identifiés par le Client.

#### **1.3.7.3 Communauté d'utilisateurs**

Une communauté d'utilisateurs est définie par l'ensemble des porteurs et d'UC comme identifié par un Client. Une communauté d'utilisateurs utilise les certificats conformément à la présente PC, et à la DPC associée, et aux procédures complémentaires définies par le Client. Une communauté d'utilisateurs utilise les certificats dans le cadre d'application(s) du Client.

## **1.4 Utilisation des certificats**

### **1.4.1 Utilisation appropriée des certificats**

#### **1.4.1.1 Certificat de l'AC**

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

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

#### **1.4.1.2 Certificat Porteur**

Les certificats délivrés aux porteurs ne sont utilisés que dans le cadre des applications métiers identifiées par le Client pour sa communauté d'utilisateurs. Les certificats sont utilisés par les UC afin d'authentifier les porteurs lors de la mise en œuvre des fonctions de sécurité (signature, contrôle d'accès et/ou chiffrement).

#### **1.4.2 Utilisation interdite des certificats**

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

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

## 1.5 Application de la politique

### 1.5.1 Organisme responsable de la présente politique

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

### 1.5.2 Personne responsable

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

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

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

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

### 1.5.4 Procédure d'approbation du présent document

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

## 1.6 Définitions et Acronymes

### 1.6.1 Définitions

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

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

**Autorité de Certification (AC) :** Se reporter au § 1.3.2.

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

**Client :** Se reporter au § 1.3.7.1.

**Communauté de l'utilisateur :** Se reporter au § 1.3.7.3.

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

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

**Certificat :** clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

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

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

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

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

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

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

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

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

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

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

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

**Fonction de hachage** : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux deux propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1];
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

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

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

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

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

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

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

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

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

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

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

**Politique de sécurité** : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

**Porteur** : Se reporter au § 1.3.6.

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

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

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

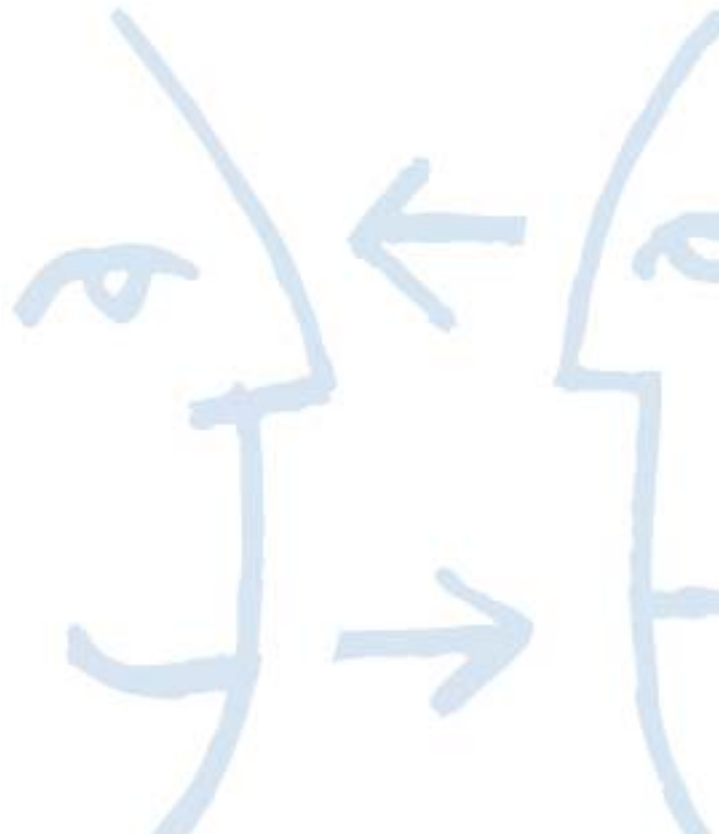
**Utilisateur de Certificat** : Se reporter au § 1.3.7.2.

**Validation de certificat électronique** : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification. Elle inclue également la validation du certificat de l'ensemble des AC du chemin de certification. La validation d'un certificat électronique nécessite au préalable de choisir le certificat auto-signé qui sera pris comme référence.

## 1.6.2 Acronymes

- **AAK** : Autorité Administrative ;
- **AC** : Autorité de Certification ;
- **AE** : Autorité d'Enregistrement ;
- **CC** : **Critères Communs**, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité ;
- **DN**: Distinguished Name ;
- **DPC** : Déclaration des pratiques de certification ;
- **EAL**: Evaluation assurance level, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité ;
- **FIPS**: United State Federal Information Processing Standards, norme fédérale américaine pour l'évaluation de produits de sécurité ;
- **HTTP**: Hypertext Transport Protocol ;
- **ICP** : Infrastructure à Clés Publiques ;
- **IGC** : Infrastructure de Gestion de Clés ;
- **IP**: Internet Protocol ;
- **ISO**: International Organization for Standardization ;
- **LCR** : liste de certificats révoqués ;
- **LDAP**: Lightweight Directory Access Protocol ;
- **OCSP**: Online Certificate Status Protocol ;
- **OID**: Object Identifier ;

- **PC** : Politique de Certification ;
- **PIN**: Personal Identification Number ;
- **PKCS**: Public-Key Cryptography Standard ;
- **RFC**: Request for comment ;
- **RSA**: Rivest, Shamir, Adleman ;
- **SHA**: Secure Hash Algorithm (norme fédérale américaine) ;
- **SP** : Service de Publication ;
- **URL**: Uniform Resource Locator.



## 2 ANNUAIRES ET SERVICES DE PUBLICATION

### 2.1 Service de publication

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

### 2.2 Informations publiées

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

- La PC de l'AC : <https://www.keynectis.com/PC/> ;
- Le certificat de l'AC: téléchargeable sur le site de retrait des certificats utilisateurs ;
- La LCR : [http://crl.certificat2.com/KEYNECTIS/KEYNECTIS\\_SHARED\\_CA.crl](http://crl.certificat2.com/KEYNECTIS/KEYNECTIS_SHARED_CA.crl).

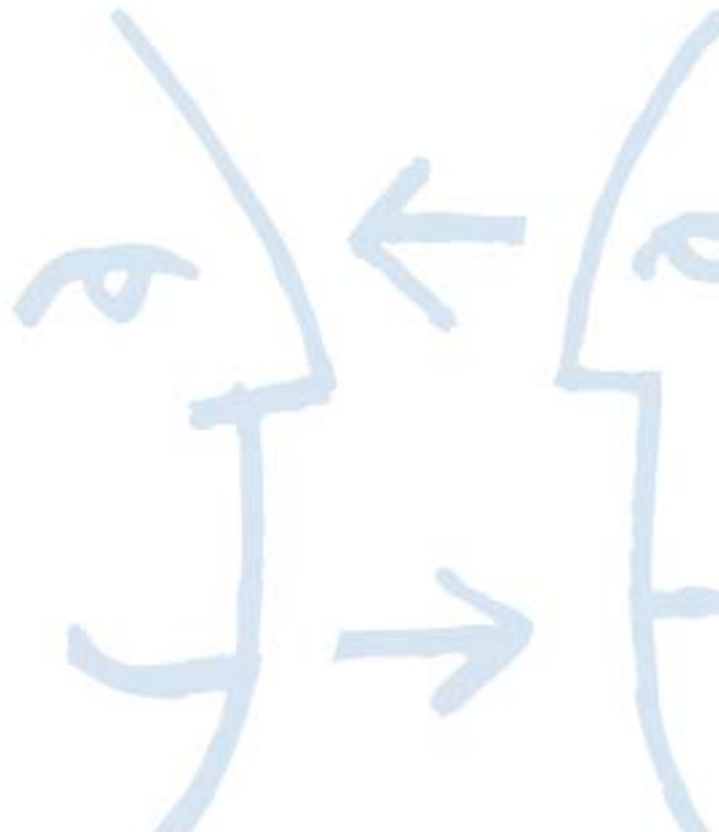
### 2.3 Heure et fréquence de publication

La PC de l'AC et le certificat de l'AC sont disponibles en permanence. Une nouvelle LCR est publiées toutes les 24 heures.

### 2.4 Contrôle d'accès au service de publication

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées.

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



### 3 IDENTIFICATION ET AUTHENTIFICATION

#### 3.1 Nommage

##### 3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X 509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN).

##### 3.1.1.1 Certificat AC

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

Champ de base	Valeur
Issuer DN	C=FR, O=KEYNECTIS, OU=0002 478217318, CN=KEYNECTIS SHARED CA
Subject DN	C=FR, O=KEYNECTIS, OU=0002 478217318, CN=KEYNECTIS SHARED CA

##### 3.1.1.2 Certificat Porteur

L'identité du porteur dans le certificat porteur est la suivante :

Champ de base	Valeur
Issuer DN	C=FR, O=KEYNECTIS, OU=0002 478217318, CN=KEYNECTIS SHARED CA
Subject DN	Définit par le Client dans sa DPC.

##### 3.1.2 Utilisation de noms explicites

L'identité portée dans le certificat comporte le nom du Client identifiée et, éventuellement, toutes les informations complémentaires permettant d'identifier son titulaire sans ambiguïté. Un Client peut employer, en plus de l'identité porté dans le champ « Subject DN », une identité de remplacement en utilisant l'extension « SubjectAlternateName ».

Les certificats associés aux composantes de l'IGC, comportent un nom significatif permettant de retrouver leur attache physique ainsi que la dénomination sociale de l'entité de rattachement de la composante.

Un porteur de certificat doit être en mesure de prouver qu'il a le droit d'utiliser une identité qu'il souhaite avoir dans son certificat.

L'AC s'assure que le contenu des champs « Subject » et « Issuer » ont un lien explicite avec le porteur.

##### 3.1.3 Anonymat ou utilisation de pseudonyme

L'identité utilisée pour les certificats de porteurs n'est ni un pseudonyme ni un nom anonyme (Se reporter au § 3.1.2).

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

Les applications du Client peuvent se servir de l'identité des porteurs telle qu'indiquée dans les certificats (Se reporter au § 3.1.1) afin d'authentifier les porteurs.

##### 3.1.5 Unicité des noms

Les identités disponibles dans les certificats (Se reporter au § 3.1.1) sont uniques au sein du domaine de certification de l'AC. Un champ spécifique (SerialNumber) composé de nombres ou de lettres peut être ajouté afin de garantir le caractère unique du nom distinctif.

Les identités doivent être uniques pour chaque Client. L'AE assure cette unicité au moyen de son processus d'enregistrement. En cas de différend au sujet de l'utilisation d'un nom pour un certificat au sein d'une communauté, c'est l'AE de cette communauté qui a la responsabilité de résoudre le différend en question.

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

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

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

## **3.2 Vérification initiale d'identité**

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

La preuve de la possession de la clé privée par le porteur est obtenue au travers des procédures de génération de la bi-clé privée correspondant à la clé publique à certifier (Se reporter au § 6.1.1) et du mode de transmission de la clé publique (Se reporter au § 6.1.3).

### **3.2.2 Vérification de l'identité des organisations**

#### **3.2.2.1 Client**

Le Client est authentifié dans le cadre des relations commerciales et contractuelles entre KEYNECTIS et le Client.

#### **3.2.2.2 Porteur**

Lorsque le porteur appartient à une entité légale différente de celle du Client, alors le Client procède à l'authentification de l'entité légale dont le porteur dépend conformément aux procédures spécifiques du Client. Ces procédures sont écrites par le Client dans ses procédures d'AE.

L'AE consigne le type d'identification utilisée, ainsi que toutes les informations pertinentes relatives à cet enregistrement.

### **3.2.3 Vérification de l'identité des personnes**

La procédure d'identification, d'authentification et de validation de la demande d'émission d'un certificat est décrite dans les procédures spécifiques du Client utilisées pour les porteurs.

### **3.2.4 Informations non vérifiées**

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

### **3.2.5 Validation de l'autorité d'un porteur**

Le Client en qualité d'AE vérifie également que le demandeur est autorisé à recevoir un certificat pour une ou des application(s) du Client. Le porteur doit donc établir la preuve de son autorisation au sein de l'application, selon des procédures qui lui sont propres.

### **3.2.6 Critères de reconnaissance**

Un porteur qui obtient un certificat émis par l'AC à la garantie d'être authentifiable par les applications du Client qu'il souhaite utiliser.

## **3.3 Vérifications aux fins de renouvellement de clés**

### **3.3.1 Vérifications aux fins de renouvellement de clés en situation normale**

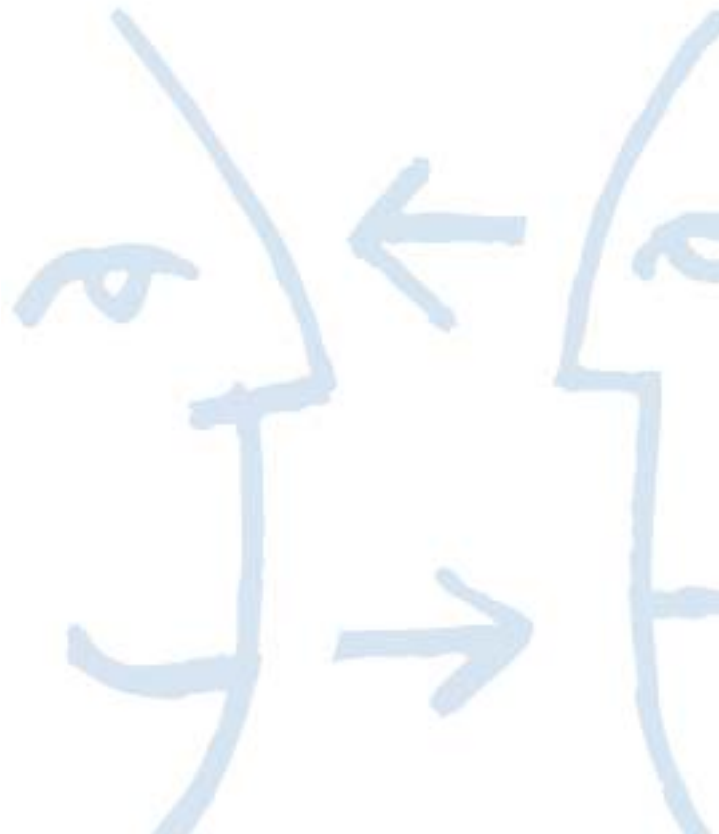
Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat, conformément aux procédures initiales (Se reporter au § 3.2).

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

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

### 3.4 Vérifications aux fins de révocation

Les demandes de révocation sont authentifiées par l'AE. La procédure de vérification est définie dans les procédures du Client.



## 4 EXIGENCES OPERATIONNELLES

### 4.1 Types de certificat

#### 4.1.1 Origine de la demande de certificat

Une demande de certificat de porteur est émise par l'AE d'un Client uniquement et pour tous les porteurs qui font partie de la communauté d'utilisateurs de ce Client.

#### 4.1.2 Procédure d'enregistrement et responsabilités

Les informations suivantes doivent figurer dans la demande d'enregistrement du porteur :

- Les informations qui permettent de construire l'identité du porteur (Se reporter au § 7.1.1.2) ;
- La clé publique à certifier suivant un mécanisme qui apporte la preuve de la possession de la clé privée correspondante à la clé publique à certifier (Se reporter au § 3.2.1).

### 4.2 Traitement d'une demande de certificat

#### 4.2.1 Identification et authentification

La procédure du Client décrit le mode opératoire de remise de la demande de certificat pour un porteur.

#### 4.2.2 Approbation ou rejet d'une demande de certificat

La procédure du Client décrit le contenu attendu d'une demande de certificat et le mode de traitement, de validation ou de rejet d'une demande de certificat.

#### 4.2.3 Durée de traitement d'une demande de certificat

La procédure du Client peut optionnellement donner un délai de traitement d'une demande de certificat.

### 4.3 Emission d'un certificat

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

L'AE authentifie le porteur (Se reporter au § 3.2.3).

L'AE transmet la demande de génération de certificat auprès du service de génération de certificat de l'AC.

L'AC authentifie l'AE qui lui transmet la demande de génération de certificat et vérifie que la demande provient effectivement d'une AE autorisée.

L'AC génère le certificat du porteur.

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

Le porteur récupère son certificat suivant les procédures définies par le Client.

Les communications, entre les différentes entités citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

#### 4.3.2 Notification de l'émission d'un certificat

La notification de l'émission d'un certificat porteur est définie dans la procédure du Client en adéquation avec les moyens techniques et les engagements contractuels pris entre KEYNECTIS et le Client.

### 4.4 Acceptation d'un certificat

#### 4.4.1 Procédure d'acceptation d'un certificat

La procédure d'acceptation d'un certificat par un porteur est définie dans la procédure du Client en adéquation avec les moyens techniques et les engagements contractuels convenus entre KEYNECTIS et le Client.

#### 4.4.2 Publication d'un certificat par l'AC

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

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

Sans objet.

### 4.5 Utilisation des bi-clés et des certificats

#### 4.5.1 Utilisation des bi-clés et des certificats

L'utilisation des bi-clés et des certificats est définie au § 1.4. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (Se reporter au § 6.1.7).

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

Les certificats de porteurs et le certificat d'AC dont il dépend, servent à authentifier les porteurs auprès des applications du Client lors de la mise en œuvre de fonctions de sécurité comme la signature et le contrôle d'accès. L'application du Client authentifie le porteur en vérifiant non seulement le certificat du porteur mais aussi le certificat d'AC et l'état de validité du certificat de l'AC qui a délivré le certificat du porteur. La validation de l'état de validité des certificats peut se faire à l'aide des informations (LCR, certificat d'AC, ...) qui sont recueillies par l'application du Client auprès du porteur, pour son certificat, et du SP pour le certificat de l'AC.

#### **4.6 Demande d'un nouveau certificat**

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

Un certificat peut être renouvelé si la période de validité de sa clé publique n'a pas expiré, si la clé privée associée n'a pas été révoquée ou compromise et si le nom et les attributs du porteur n'ont pas été modifiés. La période de validité du certificat ne doit pas excéder la durée de vie restante de la clé privée, comme spécifié dans au § 5.6. L'AE doit vérifier l'existence et la validité du certificat à renouveler et s'assurer que les informations utilisées pour vérifier l'identité et les attributs du porteur sont toujours valables en suivant les mêmes procédures que celles définies aux § 3.2.2 et 3.2.3

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

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

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

Le renouvellement de la clé d'un certificat implique la création d'un nouveau certificat conformément à la présente PC.

#### **4.8 Modification d'un certificat**

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

Le changement de l'identité contenue dans le certificat de porteur peut être à l'origine de la modification du certificat. La modification d'un certificat est traitée comme la création d'un nouveau certificat conformément à la présente PC.

#### **4.9 Révocation d'un certificat**

##### **4.9.1 Motif de révocation d'un certificat**

Un certificat de porteur est révoqué quand l'association entre ce certificat, la clé publique et le porteur qu'il certifie n'est plus considérée comme valide. Les motifs qui invalident cette association sont :

- Les données d'identification du porteur ont changé ;
- L'information contenue dans le DN du certificat n'est plus valide ;
- Perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé ;
- Révocation de l'AC ;
- Fin de vie de l'AC ;
- Modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

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

##### **4.9.2 Origine d'une demande de révocation**

Le porteur et/ou l'AE dont il dépend peuvent procéder à une demande de révocation dans les cas suivants :

- L'information contenue dans le DN du certificat est invalide ;
- Perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé.

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

- L'information contenue dans le DN du certificat est invalide ;
- Perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé ;
- Révocation de l'AC ;
- Fin de vie de l'AC ;
- Modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

#### **4.9.3 Procédure de demande de révocation**

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

- Son identification personnelle ;
- La raison de la révocation ;

L'AE authentifie la demande de révocation émise (Se reporter au § 3.4).

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

La procédure de révocation d'un certificat porteur est définie dans la procédure du Client en adéquation avec les moyens techniques et les engagements contractuels pris entre KEYNECTIS et le Client.

L'AC authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

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

Le porteur est avisé de la modification de l'état de validité de son certificat suivant les procédures définies par le Client. Une fois révoqué, un certificat ne peut plus changer d'état de validité.

#### **4.9.4 Délai accordé au porteur pour formuler la demande de révocation**

Il n'y a pas de période de grâce dans le cas d'une révocation. Les parties en question doivent demander la révocation d'un certificat dès lors qu'elles en identifient une cause de révocation comme définie au § 4.9.1.

#### **4.9.5 Délai de traitement d'une révocation**

Les demandes de révocation sont traitées dès réception par l'AC. Les LCR sont émises toutes les 24 heures, un certificat révoqués sera inscrit dans la LCR au plus tard 24 heures après que sa révocation ait été demandée. .

En cas d'indisponibilité du système, du service, ou d'autres éléments, qui échappe au contrôle de l'AC, cette dernière fait de son mieux pour que l'indisponibilité de ce service ne dépasse pas la durée maximum prévue qui est de 8 heures. L'AC devra traiter une demande de révocation dès que possible suivant sa réception et de préférence immédiatement.

#### **4.9.6 Exigences de vérification de révocation pour les tierces parties**

Il appartient aux applications du Client de vérifier l'état de validité d'un certificat à l'aide de l'ensemble des LCR émise par l'AC.

#### **4.9.7 Fréquences de publication des LCR**

La LCR est émise toute les 24 Heures.

### **4.10 Service d'état des certificats**

#### **4.10.1 Caractéristiques opérationnelles**

Il n'y a pas de service d'état de validité des certificats autre que la publication de LCR.

### **4.11 Fin de la relation entre Le porteur et l'AC**

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat de porteur doit être révoqué.

#### 4.12 Séquestre et recouvrement de clés

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



## 5 MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN ŒUVRE

### 5.1 Sécurité physique

#### 5.1.1 Situation géographique

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

#### 5.1.2 Accès physique

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

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

#### 5.1.3 Energie et air conditionné

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

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

#### 5.1.4 Exposition aux liquides

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

#### 5.1.5 Prévention et protection incendie

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

#### 5.1.6 Mise hors service des supports

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

#### 5.1.7 Sauvegardes hors site

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

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

### 5.2 Mesures de sécurité procédurales

#### 5.2.1 Rôles de confiance

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

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

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

Les rôles de confiance du Client en qualité d'AE sont classés en deux groupes :

- Opérateur d'AE : personnels autorisés par le Client à procéder à un ou des services de l'AE suivant les règles établies par le Client ;
- Administrateur d'AE : personnels autorisés par le Client pour gérer des Opérateurs d'AE.

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

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

### **5.2.3 Identification et authentification des rôles**

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

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

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

## **5.3 Mesures de sécurité vis-à-vis du personnel**

### **5.3.1 Qualifications, compétence et habilitations requises**

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

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

### **5.3.2 Procédures de vérification des antécédents**

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

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

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

### **5.3.3 Exigences en matière de formation initiale**

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

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

### **5.3.4 Exigences et fréquence en matière de formation continue**

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

### **5.3.5 Gestion des métiers**

Des précisions sont fournies dans la DPC.

### **5.3.6 Sanctions en cas d'actions non autorisées**

Des précisions sont fournies dans la DPC.

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

Des précisions sont fournies dans la DPC.

### 5.3.8 Documentation fournie au personnel

Des précisions sont fournies dans la DPC.

## 5.4 Procédures de constitution des données d'audit

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

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

### 5.4.1 Type d'événements à enregistrer

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

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

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

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

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

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

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

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

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

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

- Destinataire de l'opération ;
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;

- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

#### **5.4.2 Processus de journalisation**

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

#### **5.4.3 Protection des journaux d'événements**

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

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

#### **5.4.4 Procédures de sauvegarde des journaux d'événements**

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

#### **5.4.5 Système de collecte des journaux d'événements**

Des précisions sont fournies dans la DPC.

#### **5.4.6 Evaluation des vulnérabilités**

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

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

### **5.5 Archivage des données**

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

#### **5.5.1 Type de données archivées**

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

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- la politique de certification ;
- la déclaration des pratiques de certification ;
- les certificats tels qu'émis ou publiés ;
- les journaux d'événements des différentes entités de l'IGC.

#### **5.5.2 Période de conservation des archives**

##### **Certificats et LCR émis par l'AC**

Les certificats de porteur et d'AC sont archivés 10 ans après leur expiration.

##### **Journaux d'événements**

Les journaux d'événements traités au chapitre 5.4 sont archivés pendant 10 ans après leur génération.

#### **5.5.3 Protection des archives**

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

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

#### 5.5.4 Exigences d'horodatage des données

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

#### 5.5.5 Système de collecte des archives

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

#### 5.5.6 Procédures de récupération et de vérification des archives

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

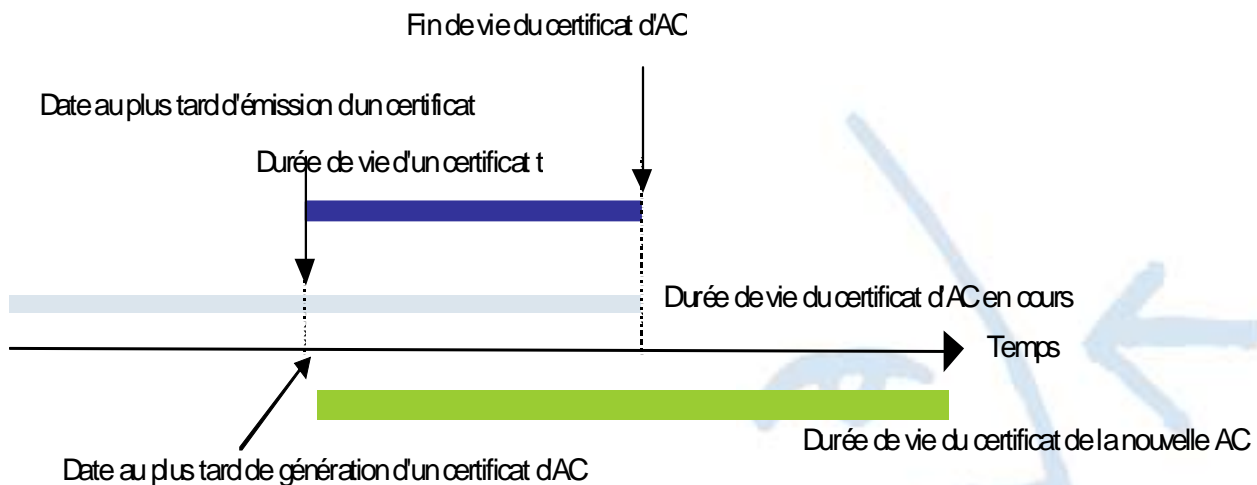
### 5.6 Renouvellement de bi-clé

#### 5.6.1 Certificat d'AC

La durée de vie d'un certificat d'AC est de 20 ans et déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière.

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

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



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

#### 5.6.2 Certificat de Porteur

La durée de validité d'un certificat est de 2 ans maximum.

### 5.7 Compromission et plan de reprise

#### 5.7.1 Procédures en cas d'incident et de compromission

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

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

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

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

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

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

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

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

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

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

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

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

### **5.8 Fin de vie d'AC**

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

- Arrêter d'émettre des certificats de porteurs ;
- Archiver tous les journaux de vérification et autres enregistrements avant la fin de l'activité ;
- Détruire toutes ses clés privées à la fin de l'activité.

## 6 MESURES TECHNIQUES DE SECURITE

### 6.1 Génération et installation des bi-clés

#### 6.1.1 Génération des bi-clés

##### 6.1.1.1 Bi-clé d'AC

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

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

##### 6.1.1.2 Bi-clé de Porteur

La génération de la bi-clé du porteur est réalisée à l'aide du support de la bi-clé cryptographique du porteur conformément à la procédure établie par le Client. La génération permet de garantir la confidentialité et l'intégrité de la clé privée au seul profit du porteur.

#### 6.1.2 Fourniture de la clé privée au porteur

Le porteur génère lui-même sa bi-clé, par conséquent l'AC ne remet pas de clé privée au porteur.

#### 6.1.3 Fourniture de la clé publique à l'AC

La clé publique est transmise à l'AC au format PKCS#10 par le porteur qui initie la demande de certificat auprès de l'AE et lors d'une connexion sécurisée de manière à garantir l'intégrité et la confidentialité de la communication et l'authentification entre l'AC et le porteur.

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

Le certificat de l'AC est remis au porteur lors de la remise du certificat au porteur.

Le certificat de l'AC est aussi remis aux applications du Client qui souhaitent se servir des certificats pour authentifier des porteurs.

#### 6.1.5 Taille de clés

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

L'utilisation de l'algorithme RSA avec fonctions de hachage SHA-1 ou SHA-256 est requis par l'AC. La taille de la bi-clé de l'AC est de 2048 bits pour l'algorithme RSA.

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

#### 6.1.6 Production des paramètres des clés publiques et contrôle de qualité

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles.

Les bi-clés des porteurs sont générées par le porteur à l'aide des outils cryptographique de son choix conformément aux procédures établit par le Client.

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

L'utilisation du champ "key usage" dans le certificat et AC est la suivante :

- AC :
  - o Key CertSign ;
  - o Key CRL Sign ;
- Porteur :
  - o Digital Signature ;
  - o Non Repudiation ;
  - o Key Encipherment ;
  - o Data Encipherment.

## **6.2 Protection des clés privées et normes relatives au module cryptographique**

### **6.2.1 Normes applicables aux ressources cryptographiques et contrôles**

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

### **6.2.2 Contrôle de la clé privée par de multiples personnes**

L'activation de la clé privée d'AC est contrôlée par au moins 3 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée d'AC font l'objet d'une authentification forte. L'AC est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seuls rôles de confiance qui peuvent émettre des certificats.

Le porteur est responsable de la protection et du contrôle de la clé privée à l'aide de sa donnée d'activation.

### **6.2.3 Séquestre de clé privée**

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

### **6.2.4 Sauvegarde de clé privée**

#### **6.2.4.1 AC**

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

#### **6.2.4.2 Porteur**

Le porteur peut procéder à une copie de sauvegarde de sa bi-clé, mais il reste responsable de la protection de la sauvegarde.

### **6.2.5 Archivage de clé privée**

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

### **6.2.6 Importation / exportation d'une clé privée**

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

### **6.2.7 Stockage d'une clé privée dans un module cryptographique**

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

### **6.2.8 Méthode d'activation d'une clé privée**

#### **6.2.8.1 AC**

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

#### **6.2.8.2 Porteur**

La clé privée d'un porteur est activable à l'aide d'une donnée d'activation. L'activation est nécessaire à chaque utilisation de la clé privée à l'aide du support matériel de la bi-clé. Le porteur doit configurer son support de bi-clé de telle sorte qu'il requière la saisie de la donnée d'activation à chaque utilisation de sa clé privée correspondant au certificat que l'AC a émis.

### **6.2.9 Méthode de désactivation d'une clé privée**

### **6.2.9.1 AC**

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

Les ressources cryptographiques de signature de l'AC sont en ligne uniquement afin de signer des certificats porteurs après avoir authentifié la demande de certificat.

### **6.2.9.2 Porteur**

La désactivation de la clé privée du porteur est effectuée à chaque fin d'utilisation de la clé privée à l'aide du support matériel de la bi-clé.

## **6.2.10 Méthode de destruction d'une clé privée**

### **6.2.10.1 AC**

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

### **6.2.10.2 Porteur**

La destruction de la clé privée du porteur, et de ses sauvegardes le cas échéant, est effectuée à l'aide du support matériel de la bi-clé en utilisant les fonctions logiques d'effacement du support de la bi-clé.

### **6.2.11 Certification des ressources cryptographiques**

Se reporter au § 6.2.1.

## **6.3 Autres aspects de la gestion des bi-clés**

### **6.3.1 Archivage des clés publiques**

Les clés publiques sont archivées par archivage des certificats (Se reporter au § 5.5.2 ci-dessus).

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

#### **6.3.2.1 AC**

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

#### **6.3.2.2 Porteur**

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

## **6.4 Données d'activation**

### **6.4.1 Génération et installation des données d'activation**

#### **6.4.1.1 AC**

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (Se reporter au § 6.1.1.1). Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

#### **6.4.1.2 Porteur**

Les données d'activation sont générées par le porteur lui-même. Le porteur a la responsabilité de faire en sorte que les clés privées qu'ils gèrent soient protégées par des données d'activation. Parmi ces caractères, il est recommandé d'avoir au moins des chiffres et des lettres. La chaîne totale de caractère ne doit pas être naturellement intelligible.

## **6.4.2 Protection des données d'activation**

### **6.4.2.1 AC**

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

### **6.4.2.2 Certificat porteur**

Le porteur s'assure que la donnée d'activation de la clé privée est protégée en confidentialité de tel sort qu'il soit le seul à pouvoir activer la clé privée contenue sur son support matériel.

### **6.4.3 Autres aspects touchant aux données d'activation**

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

## **6.5 Mécanismes de sécurité des systèmes informatiques**

### **6.5.1 Exigences techniques de sécurité des ressources informatiques**

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

- Authentification des rôles de confiance ;
- Contrôle d'accès discrétionnaire ;
- Interdiction de la réutilisation d'objets ;
- Exige l'utilisation de la cryptographie lors des communications ;
- Requiert l'identification des utilisateurs ;
- Assure la séparation rigoureuse des tâches ;
- Fournit une autoprotection du système d'exploitation.

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

### **6.5.2 Indice de sécurité informatique**

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

## **6.6 Contrôles techniques du système pendant son cycle de vie**

### **6.6.1 Contrôle des développements des systèmes**

Le contrôle des développements des systèmes s'effectue comme suit :

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

- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

#### **6.6.2 Contrôles de gestion de la sécurité**

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

#### **6.6.3 Contrôle de sécurité du système pendant son cycle de vie**

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

### **6.7 Mécanismes de sécurité du réseau**

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

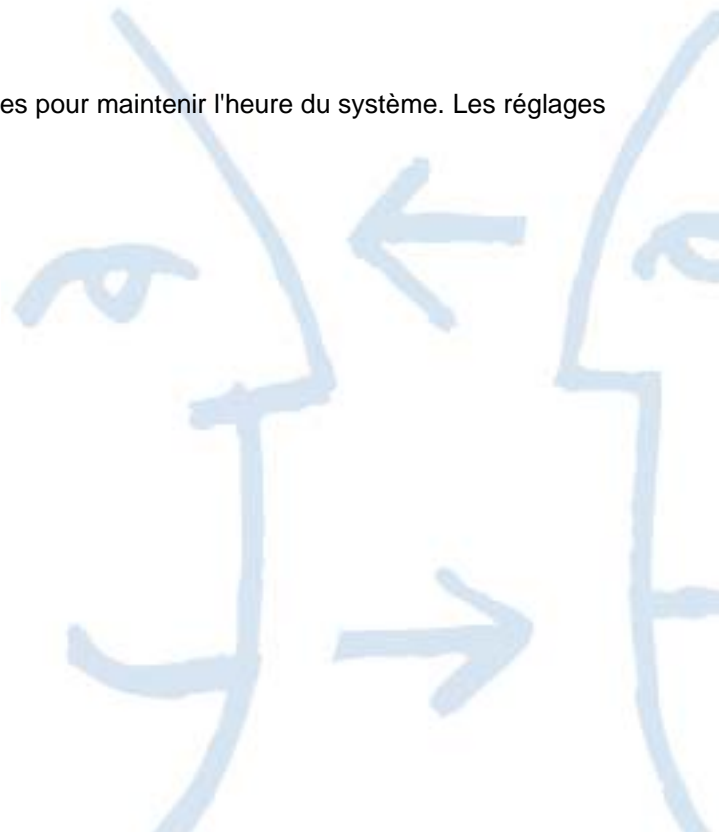
Les autres composantes de l'IGC de l'AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés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

### **6.8 Horodatage/Système de datation**

Il n'y a pas d'horodatage utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP). Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

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

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



## 7 CERTIFICATS, CRL, ET PROFILS OCSP

### 7.1 Profil de Certificats

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

#### 7.1.1 Extensions de Certificats

##### 7.1.1.1 Certificat AC

##### 7.1.1.2 Champs de base du certificat

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

Champ de base	Valeur
Issuer DN	C=FR, O=KEYNECTIS, OU=0002 478217318, CN=KEYNECTIS SHARED CA
Subject DN	C=FR, O=KEYNECTIS, OU=0002 478217318, CN=KEYNECTIS SHARED CA
Longueur des clefs de l'AC :	2048
Durée de validité de l'AC :	20 ans

##### 7.1.1.3 Extension du certificat

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

- Authority Key Identifier ;
- Basic Constraint ;
- Key Usage : Key CertSign, Key CRL Sign;
- Subject Key Identifier ;
- Other Extensions (Netscape Cert Type : SSL CA, S/MIME CA).

##### 7.1.1.4 Certificat Porteur

Les informations principales contenues dans le certificat porteur sont :

Champ de base	Valeur
Issuer DN	C=FR, O=KEYNECTIS, OU=0002 478217318, CN=KEYNECTIS SHARED CA
Subject DN	C = <Pays> ST = <Etat ou Région> (optionnel selon le choix du Client) L = <Localité> (optionnel selon le choix du Client) O = <Organisation> OU = <Applicatif> (optionnel selon le choix du Client) T = <Titre> (optionnel selon le choix du Client) SURNAME = <Nom de famille> (optionnel selon le choix du Client) GIVENNAME = <Prénom> (optionnel selon le choix du Client) CN = <Nom Commun> E = <Email du porteur>
Longueur des clefs du certificat du porteur :	1024 minimum
Durée de validité du certificat du porteur :	1 ou 2 ans

### **7.1.1.5 Extension du certificat**

Les informations principales contenues dans le certificat porteur sont :

- Authority Key Identifier ;
- Basic Constraint ;
- Certificate Policies ;
- CRL Distribution Points ;
- Key Usage : Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment ;
- Subject Alternative Name ;
- Subject Key Identifier ;
- Other Extensions (Netscape Cert Type : sslclient, email).

### **7.1.2 Identifiant d'algorithmes**

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

### **7.1.3 Formes de noms**

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

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

Les certificats émis par l'AC contiennent l'OID de la PC qui est : 1.3.6.1.4.1.22234.2.1.3.2.

### **7.1.5 Extensions propres à l'usage de la Politique**

Sans objet.

### **7.1.6 Syntaxe et Sémantique des qualificateurs de politique**

Sans objet.

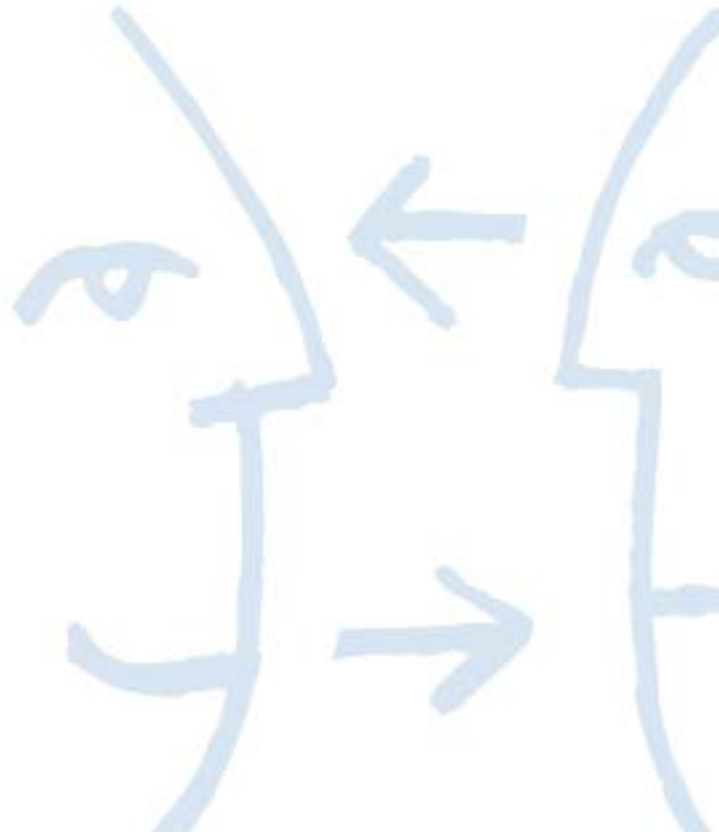
### **7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies"**

Pas d'exigence formulée.

## **7.2 Profil de LCR**

### **7.2.1 LCR et champs d'extensions des LCR**

Défini dans la DPC.



## 8 CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS

### 8.1 Fréquence et motifs des audits

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

### 8.2 Identité / Qualification des auditeurs

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

### 8.3 Lien entre l'auditeur et l'entité contrôlée

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

L'AAK détermine si un auditeur remplit cette condition.

### 8.4 Points couverts par l'évaluation

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

### 8.5 Mesures prises en cas de non-conformité

L'AAK peut décider que l'AC ou l'une de ses composantes n'agit pas en conformité avec les obligations définies dans la présente PC. Quand une telle décision est prise, l'AAK peut suspendre les opérations de la composante non conforme de l'IGC, ou peut donner l'ordre de cesser toute relation avec la composante en question, ou peut décider que des actions correctives sont à prendre.

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

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

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

Quand les actions correctives sont réalisées, l'AC en informe l'AAK et lui fournit un rapport de mise à hauteur, pour évaluation.

### 8.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à l'AAK comme prévu au § 8.1 ci-dessus. Ce rapport cite les versions des PC et DPC utilisées pour cette évaluation. Quand nécessaire, le rapport de contrôle peut être diffusé comme prévu au § 8.5 ci-dessus. Le Rapport de Contrôle de Conformité n'est rendu disponible à des tiers utilisateurs sur Internet.

## 9 AUTRES QUESTIONS COMMERCIALES ET JURIDIQUES

### 9.1 Tarifs

#### 9.1.1 Frais d'émission et de renouvellement de certificats

Des précisions sont données dans la DPC.

#### 9.1.2 Frais d'accès aux certificats

Des précisions sont données dans la DPC.

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

Des précisions sont données dans la DPC.

#### 9.1.4 Frais pour d'autres services

Des précisions sont données dans la DPC.

#### 9.1.5 Politique de remboursement

Des précisions sont données dans la DPC.

### 9.2 Responsabilité financière

#### 9.2.1 Couverture par les assurances

La DPC donne les procédures d'assurances relatives à cette exigence.

#### 9.2.2 Autres ressources

Sans objet.

#### 9.2.3 Couverture et garantie concernant les entités utilisatrices

La DPC définit les garanties relatives à l'utilisation.

### 9.3 Confidentialité des informations

#### 9.3.1 Informations confidentielles

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

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

#### 9.3.2 Information considérées comme non confidentielles

Aucune des informations publiées dans la présente PC n'est considérée comme confidentielle. Néanmoins, celles-ci peuvent être visées par la loi sur la propriété intellectuelle. Seules les données d'activation et les clés privées sont considérées comme des informations confidentielles.

#### 9.3.3 Obligation de protection des informations confidentielles

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

Les LCR ne contiennent que les numéros d'enregistrement des certificats et leurs dates de révocation. Lorsque les causes de révocations sont transmises par l'AE, alors ses causes de révocation sont tenues strictement confidentielles par l'AC et ne sont pas publiées.

Dans le cadre des audits et contrôles auxquels l'AC ou l'AE est soumise en vertu de la PC, des éléments sur les motifs de révocation, non nominatifs et non liés à un certificat, pourront être fournis, sans préjudice des dispositions relevant du secret professionnel auquel l'AE pourrait être soumise.

## **9.4 Confidentialité des informations à caractère personnel**

### **9.4.1 Plan de confidentialité**

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

Le secret des correspondances émises par voie de télécommunication est garanti par la loi française. En cas d'atteinte, toute violation est punie par l'Article 226-15 du code pénal pour celles commises par un particulier et par les Articles 432-9 et 432-17 du code pénal pour celles commises par une personne dépositaire de l'autorité publique.

D'une façon générale, aucun salarié du service de l'IGC, ni aucun collaborateur ou sous-traitant, dans le cadre de leur participation aux services de l'IGC, n'a le droit d'intercepter, d'ouvrir, de détourner, de divulguer, de rechercher ou d'utiliser les documents soumis au service de l'IGC, sauf dans les cas prévus dans la présente politique, ou dans le cadre du régime des interceptions ordonnées par l'autorité judiciaire ou des interceptions de sécurité en vertu de la loi n°91-646 du 10 juillet 1991 (JO du 13 juillet 1991, rectification JO du 10 août 1991).

### **9.4.2 Information considérées comme personnelles**

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

- Données d'identification du porteur ;
- Identité du porteur ;
- Demande (renseigné) de certificat ;
- Demande (renseigné) de révocation ;
- Motif de révocation.

### **9.4.3 Information non considérées comme n'étant pas à caractère personnel**

Sans objet.

### **9.4.4 Obligation de protection des informations à caractère personnel**

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

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique au contenu de tous les documents collectés, détenus ou transmis par l'AC ou par l'AE dans le cadre de la délivrance d'un certificat.

Les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'AC ou l'AE pour l'émission du certificat et la gestion de son cycle de vie. Ce droit peut s'exercer auprès de l'AAK.

Toutes les données collectées et détenues par l'AC sont considérées comme confidentielles, hormis les données figurant dans le certificat.

En vertu des articles 323-1 à 323-7 du Code pénal applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 1 à 3 ans d'emprisonnements assortis d'une amende allant de 15.000 à 225.000 euros pour les personnes morales.

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

Aucune des données à caractère personnel fournies par un porteur ne peut être utilisée par l'AC, pour une autre utilisation autre que celle définie dans le cadre de la présente PC, sans consentement exprès et préalable de la part du porteur. Ce consentement est considéré comme obtenu lors de la soumission de la demande de certificat et du fait de l'acceptation par le porteur du certificat émis par l'AC (en accord avec la présente PC) au titre de l'utilisation par les applications du Client.

### **9.4.6 Divulgarion due à un processus judiciaire ou administratif**

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

#### **9.4.7 Autres motifs de divulgation de données à caractère personnel**

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

### **9.5 Droits relatifs à la propriété intellectuelle**

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

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, ...etc.) est sanctionnée par les articles L 716-1 et suivants du Code de la propriété intellectuelle.

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

Le porteur détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats porteurs émis par l'AC et dont il est propriétaire.

### **9.6 Obligations et garanties**

Les composantes de l'IGC, le Client et la communauté d'utilisateurs sont responsables pour tous dommages et intérêts découlant du non-respect de leurs obligations respectives telles que définies aux termes de la présente PC.

#### **9.6.1 Obligations communes**

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

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

#### **9.6.2 Obligations et garanties de l'AAK**

Les obligations de l'AAK sont les suivantes :

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

#### **9.6.3 Obligations et garanties de l'AC**

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

L'AC est responsable du maintien de la conformité aux procédures prescrites dans la présente PC. L'AC fournit tous les services de certification en accord avec sa DPC. Les obligations communes aux composantes de l'AC sont :

- Protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;

- N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC ;
- Respecter et appliquer les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC doit être transmise à la composante concernée) ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de l'AAK de contrôler et vérifier la conformité avec la PC ;
- Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- Met à la disposition de l'AE l'ensemble des moyens techniques nécessaires à la réalisation de ses obligations conformément au contrat établi entre KEYNECTIS et le Client.

#### **9.6.4 Obligations de l'AE**

Les obligations de l'AE sont les suivantes :

- L'authentification du porteur ;
- La réalisation de toutes les vérifications requises pour les procédures définies par le Client ;
- L'authentification de la demande de certificat ;
- L'authentification de la demande de révocation ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de l'AAK de contrôler et vérifier la conformité avec la PC ;

#### **9.6.5 Obligations et garanties du porteur**

Les obligations du porteur sont :

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

#### **9.6.6 Obligations et garanties du SP**

Les obligations du SP sont :

- De publier les LCR ;
- De garantir les taux de disponibilités des informations publiées.
- De protéger les accès au SP.

#### **9.6.7 Obligations et garanties des autres participants**

##### **9.6.7.1 Obligations et garanties du Client**

Les obligations du Client sont :

- De se conformer à toutes les exigences de la PC et de la DPC associée ainsi qu'aux procédures qu'il définit ;
- D'identifier de manière non ambiguë la communauté d'utilisateurs qu'il souhaite voir porter dans les certificats de porteur ;
- De communiquer les identités des personnes qui ont un rôle de confiance dans le cadre de la mise en œuvre des services de l'AE ;
- De faire respecter une politique de sécurité sur les postes informatiques des rôles de confiance ;
- De garantir que les informations qu'il fournit à l'AC sont exactes et complètes ;
- De ne délivrer des certificats que dans le cadre d'applications qui sont de sa responsabilité ;
- De procéder à la révocation des porteurs lorsque cela s'avère nécessaire.

## **9.7 Dénier de garanties**

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

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

Aucune autre garantie ne peut-être mise en avant par l'AC, les porteurs et les applications du Client dans leurs accords contractuels (s'il en est).

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

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

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

## **9.8 Limites de responsabilité**

En ce qui concerne les certificats émis par l'AC est seulement responsable des exigences et des principes édictés dans la présente PC. L'AC est responsable de tout dommage causé à un porteur ou une application en raison d'une exécution incorrecte des procédures définies dans la présente PC et la DPC associée. L'AC décline toutefois toute responsabilité à l'égard d'une exécution incorrecte des procédures définies par le Client en sa qualité d'AE.

L'AC décline toute responsabilité à l'égard de l'usage des certificats émis par elle ou des bi-clés publiques/privées associées dans des conditions et à des fins autres que celles prévues dans la présente PC.

L'émission du certificat ne vaut pas acceptation de fait par le service d'abonnement de l'application de l'AAK. Il est de la responsabilité du porteur de procéder à la démarche d'abonnement auprès des applications qui souhaite utiliser. De même, il est de la responsabilité du mandataire d'entreprise d'accorder, gérer ou supprimer une délégation et une ou des habilitations sur tout ou partie d'une application données à un porteur d'un certificat.

L'AC n'est tenue qu'à une obligation de moyen pour la mise en œuvre des services de certification qu'elle fournit.

Seule la responsabilité de l'AC peut être mise en cause en cas de non-respect des dispositions prévues par les présentes.

L'AC décline toute responsabilité à l'égard de l'usage qui est fait des certificats qu'elle a émis dans des conditions et à des fins autres que celles prévues dans la présente politique de certification que dans tout autre document contractuel applicable associé.

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, les conflits sociaux, la défaillance du réseau ou des installations ou réseaux de télécommunications externes.

## **9.9 Indemnités**

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'AC vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés lors de l'arbitrage du litige.

## **9.10 Durée et fin anticipée de validité de la PC**

### **9.10.1 Durée**

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

### **9.10.2 Résiliation**

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

### **9.10.3 Effets de la résiliation et survie**

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

## **9.11 Amendements**

### **9.11.1 Procédure pour apporter un amendement**

L'AAK révisé sa PC et sa DPC au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de l'AAK. Les corrections de fautes d'orthographe ou de frappe qui ne modifient pas le sens de la PC sont autorisées sans avoir à être notifiées. L'AAK informe le Client des modifications entraînant des modifications de la DPC.

### **9.11.2 Mécanisme et délais des notifications**

L'AAK donne un préavis de 2 mois au moins aux composantes de l'IGC de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, ...) et non sur la forme de la PC et de la DPC.

### **9.11.3 Motifs selon lesquels un OID doit être changé**

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

## **9.12 Règlement des différends**

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

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

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

L'expert amiable doit tenter de concilier les parties dans un délai de deux (2) mois à compter de sa saisine. Il propose un rapport en vue de concilier chacune des parties. Ce rapport a un caractère confidentiel et ne peut servir que dans le cadre de la procédure d'expertise amiable.

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

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

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

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

Entre autre, l'AC définit sa politique de nommage et propose, et s'autorise dans certains cas, de régler les différends concernant l'identité à inscrire dans un certificat et dans le cas où les parties ne parviendraient pas à un accord amiable, le différend sera réglé par un tribunal français.

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

### **9.13 Droit applicable**

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

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

### **9.14 Conformité au droit applicable**

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

### **9.15 Divers**

#### **9.15.1 Totalité de l'entente**

Le cas échéant, la DPC précisera les exigences spécifiques.

#### **9.15.2 Affectation**

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

#### **9.15.3 Divisibilité**

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

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

#### **9.15.4 Exonération des droits**

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

#### **9.15.5 Force majeure**

L'AC ne saurait être tenue pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs aux porteurs ou aux applications du Client.

### **9.16 Autres dispositions**

Le cas échéant, la DPC en fournira les détails.