

## **POLITIQUE DE CERTIFICATION – AC PERSONNES**

---

<b>OID du document :</b>	1.2.250.1.120.2.2.1.2 1.2.250.1.120.2.3.1.2	/	<b>Nombre total de pages :</b>	72
<b>Statut du document :</b>	<input type="checkbox"/> Projet		<input checked="" type="checkbox"/> Version finale	

### Rédaction

<b>Nom</b>	<b>Fonction</b>
Alain GALLET	Responsable du programme Sécurité – ANTS
Philippe BOURDIN	AMOA Sécurité

### Validation

<b>Nom</b>	<b>Fonction</b>	<b>Signature</b>
Luc FERRAND	Directeur de projet nouvelles technologies – MJL	
Luc VALLEE	Fonctionnaire de sécurité des systèmes d'information – MJL	
Cédric SIBEN	Directeur adjoint – ANTS	

### Approbation

<b>Nom</b>	<b>Fonction</b>	<b>Signature</b>
André GARIAZZO	Haut fonctionnaire défense et sécurité – MJL	

## REVISION DOCUMENTAIRE

Historique		
Date	Version	Commentaires
26/03/10	0.1	Création du document
13/04/10	0.2	Mise à jour du document
07/04/10	0.4	Version de travail diffusée au MJL
13/05/10	0.7	Version de travail diffusée au MJL
20/05/10	0.8	Version de travail diffusée au MJL
01/06/10	1.0	Version de référence
23/01/11	1.1	Prise en compte commentaires MJL/SG changement du nom de l'AC ordre judiciaire → AC personnes pour couvrir l'ensemble du ministère
15/10/11	1.6	Version pour relecture finale
25/11/11	2.0	Version pour signature
24/01/11	2.0.1	Prise en compte des fiches d'audit
12/06/11	2.1	Ajout de précisions sur les rôles de confiance
31/07/12	2.1.1	Prise en compte des évolutions 2011 et mise à jour des noms des intervenants

## SOMMAIRE

<b>1</b>	<b>INTRODUCTION</b>	<b>9</b>
1.1	<b>Généralités</b>	<b>9</b>
1.2	<b>Nom du document et identification</b>	<b>10</b>
1.3	<b>Entités intervenant dans l'IGC</b>	<b>10</b>
1.3.1	Ministère de la Justice et des Libertés (AC – AE – SP)	11
1.3.1.1	Autorité de Certification (AC)	11
1.3.1.2	Autorité d'Enregistrement (AE)	12
1.3.1.2.1	Autorité d'Enregistrement Centralisée (AEC)	13
1.3.1.2.2	Autorité d'Enregistrement Déléguée (AED)	13
1.3.1.2.3	Opérateur de Certification (OC)	13
1.3.1.3	Organisation de la DSJ (Direction des Services Judiciaires)	14
1.3.1.4	Service de Publication (SP)	15
1.3.2	Agence Nationale des Titres Sécurisés (CPS - OSC)	16
1.3.2.1	Centre de Personnalisation des Supports (CPS)	16
1.3.2.2	Opérateur de Service de Certification (OSC)	16
1.3.3	Autres participants	16
1.3.3.1	Porteur de certificats	16
1.3.3.2	Utilisateur de Certificats (UC)	17
1.4	<b>Usage des certificats</b>	<b>17</b>
1.4.1.1	Certificat de l'AC	17
1.4.1.2	Certificats de porteur	17
1.4.2	Utilisation interdite des certificats	17
1.5	<b>Gestion de la PC</b>	<b>17</b>
1.5.1	Entité gérant la PC	17
1.5.2	Point de contact	18
1.5.3	Entité déterminant la conformité d'un DPC avec cette PC	18
1.5.4	Procédures d'approbation de la conformité de la DPC	18
1.6	<b>Définitions et Acronymes</b>	<b>19</b>
1.6.1	Acronymes	19
1.6.2	Définitions	20
<b>2</b>	<b>RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES</b>	<b>24</b>
2.1	<b>Entités chargées de la mise à disposition des informations</b>	<b>24</b>

<b>2.2</b>	<b>Informations devant être publiées</b> .....	<b>24</b>
<b>2.3</b>	<b>Délais et fréquences de publication</b> .....	<b>24</b>
<b>2.4</b>	<b>Contrôle d'accès aux informations publiées</b> .....	<b>24</b>
<b>3</b>	<b>IDENTIFICATION ET AUTHENTIFICATION</b> .....	<b>25</b>
<b>3.1</b>	<b>Nommage</b> .....	<b>25</b>
3.1.1	Types de noms.....	25
3.1.1.1	Certificat d'AC.....	25
3.1.1.2	Certificat de porteur.....	25
3.1.2	Nécessité d'utilisation de noms explicites.....	25
3.1.3	Pseudonymisation des porteurs.....	25
3.1.4	Règles d'interprétations des différentes formes de noms.....	26
3.1.5	Unicité des noms.....	26
3.1.6	Identification, authentification et rôle des marques déposées.....	26
<b>3.2</b>	<b>Vérification initiale d'identité</b> .....	<b>26</b>
3.2.1	Méthode pour prouver la possession de la clé privée.....	26
3.2.2	Validation de l'identité d'un organisme.....	27
3.2.3	Validation de l'identité des porteurs.....	27
3.2.4	Informations non vérifiées du porteur.....	27
3.2.5	Validation de l'autorité du demandeur.....	27
3.2.6	Certification croisée d'AC.....	27
<b>3.3</b>	<b>Identification et validation d'une demande de renouvellement des clés</b> .....	<b>27</b>
3.3.1	Identification et validation pour un renouvellement courant.....	27
3.3.2	Identification et validation pour un renouvellement après révocation.....	28
<b>3.4</b>	<b>Identification et validation d'une demande de révocation</b> .....	<b>28</b>
<b>4</b>	<b>EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS</b> .....	<b>29</b>
<b>4.1</b>	<b>Demande de certificat</b> .....	<b>29</b>
4.1.1	Origine d'une demande de certificat.....	29
4.1.2	Processus et responsabilités pour l'établissement d'une demande de certificat.....	29
<b>4.2</b>	<b>Traitement d'une demande de certificat</b> .....	<b>29</b>
4.2.1	Exécution des processus d'identification et de validation de la demande.....	29
4.2.2	Acceptation ou rejet de la demande.....	29
4.2.3	Durée d'établissement du certificat.....	29
<b>4.3</b>	<b>Délivrance d'un certificat</b> .....	<b>30</b>
4.3.1	Actions de l'AC concernant la délivrance du certificat.....	30
4.3.2	Notification par l'AC de la délivrance du certificat au porteur.....	30
<b>4.4</b>	<b>Acceptation du certificat</b> .....	<b>30</b>
4.4.1	Démarche d'acceptation du certificat.....	30
4.4.2	Publication du certificat.....	30
4.4.3	Notification par l'AC aux autres entités de la délivrance du certificat.....	30
<b>4.5</b>	<b>Usages de la bi-clé et du certificat</b> .....	<b>30</b>
4.5.1	Utilisations de la clé privée et du certificat par le porteur.....	30
4.5.2	Utilisation de la clé publique et du certificat par l'utilisateur du certificat.....	31
<b>4.6</b>	<b>Renouvellement d'un certificat</b> .....	<b>31</b>
4.6.1	Causes possibles de renouvellement d'un certificat.....	31
4.6.2	Origine d'une demande de renouvellement.....	31
4.6.3	Procédure de traitement d'une demande de renouvellement.....	32
4.6.4	Notification au porteur de l'établissement du nouveau certificat.....	32
4.6.5	Démarche d'acceptation du nouveau certificat.....	32
4.6.6	Publication du nouveau certificat.....	32
4.6.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	32
<b>4.7</b>	<b>Délivrance d'un nouveau certificat suite à changement de la bi-clé</b> .....	<b>32</b>
4.7.1	Causes possibles de changement d'une bi-clé.....	32
4.7.2	Origine d'une demande d'un nouveau certificat.....	32
4.7.3	Procédure de traitement d'une demande d'un nouveau certificat.....	32
4.7.4	Notification au porteur de l'établissement du nouveau certificat.....	32
4.7.5	Démarche d'acceptation du nouveau certificat.....	33

4.7.6	Publication du nouveau certificat .....	33
4.7.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat .....	33
<b>4.8</b>	<b>Modification du certificat .....</b>	<b>33</b>
4.8.1	Causes possibles de modification d'un certificat .....	33
4.8.2	Origine d'une demande de modification d'un certificat .....	33
4.8.3	Procédure de traitement d'une demande de modification d'un certificat .....	33
4.8.4	Notification au porteur de l'établissement du certificat modifié .....	33
4.8.5	Démarche d'acceptation du certificat modifié .....	33
4.8.6	Publication du certificat modifié .....	33
4.8.7	Notification par l'AC aux autres entités de la délivrance du certificat modifié .....	33
<b>4.9</b>	<b>Révocation et suspension des certificats .....</b>	<b>33</b>
4.9.1	Causes possibles d'une révocation .....	33
4.9.1.1	Certificats de porteurs .....	33
4.9.1.2	Certificats d'une composante de l'IGC .....	34
4.9.2	Origine d'une demande de révocation .....	34
4.9.2.1	Certificats de porteurs .....	34
4.9.2.2	Certificats d'une composante de l'IGC .....	34
4.9.3	Procédure de traitement d'une demande de révocation .....	34
4.9.3.1	Révocation d'un certificat de porteurs .....	34
4.9.3.2	Révocation d'un certificat d'une composante de l'IGC .....	35
4.9.4	Délai accordé au porteur pour formuler la demande de révocation .....	35
4.9.5	Délai de traitement par l'AC d'une demande de révocation .....	35
4.9.5.1	Révocation d'un certificat de porteur .....	35
4.9.5.2	Révocation d'un certificat d'une composante de l'IGC .....	35
4.9.6	Exigences de vérification de révocation par les utilisateurs de certificats .....	36
4.9.7	Fréquence d'établissement des LCR .....	36
4.9.8	Délai maximum de publication d'une LCR .....	36
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats .....	36
4.9.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats .....	36
4.9.11	Autres moyens disponibles d'information sur les révocations .....	36
4.9.12	Exigences spécifiques en cas de compromission de la clé privée .....	36
4.9.13	Causes possibles d'une suspension .....	36
4.9.14	Origine d'une demande de suspension .....	36
4.9.15	Procédure de traitement d'une demande de suspension .....	36
4.9.16	Limites de la période de suspension d'un certificat .....	36
<b>4.10</b>	<b>Fonction d'information sur l'état des certificats .....</b>	<b>37</b>
4.10.1	Caractéristiques opérationnelles .....	37
4.10.2	Disponibilité de la fonction .....	37
4.10.3	Dispositifs optionnels .....	37
<b>4.11</b>	<b>Fin de la relation entre le porteur et l'AC .....</b>	<b>37</b>
<b>4.12</b>	<b>Séquestre de clé et recouvrement .....</b>	<b>37</b>
4.12.1	Politique et pratiques de recouvrement par séquestre des clés .....	37
4.12.2	Politique et pratiques de recouvrement par encapsulation des clés de session .....	37
<b>5</b>	<b>MESURES DE SECURITE NON TECHNIQUES .....</b>	<b>38</b>
<b>5.1</b>	<b>Mesures de sécurité physique .....</b>	<b>38</b>
5.1.1	Situation géographique et construction des sites .....	38
5.1.2	Accès physique .....	38
5.1.3	Alimentation électrique et climatisation .....	39
5.1.4	Vulnérabilité aux dégâts des eaux .....	39
5.1.5	Prévention et protection incendie .....	39
5.1.6	Conservation des supports .....	39
5.1.7	Mise hors service des supports .....	39
5.1.8	Sauvegardes hors site .....	39
<b>5.2</b>	<b>Mesures de sécurité procédurales .....</b>	<b>39</b>
5.2.1	Rôles de confiance .....	39
5.2.2	Nombre de personnes requises par tâche .....	40
5.2.3	Identification et authentification pour chaque rôle .....	40

5.2.4	Rôles exigeant une séparation des attributions.....	41
<b>5.3</b>	<b>Mesures de sécurité vis-à-vis du personnel.....</b>	<b>41</b>
5.3.1	Qualifications, compétences et habilitations requises .....	41
5.3.2	Procédures de vérification des antécédents.....	41
5.3.3	Exigences en matière de formation initiale .....	41
5.3.4	Exigences et fréquence en matière de formation continue .....	42
5.3.5	Fréquence et séquence de rotation entre différentes attributions .....	42
5.3.6	Sanctions en cas d'actions non autorisées.....	43
5.3.7	Exigences vis-à-vis du personnel des prestataires externes.....	43
5.3.8	Documentation fournie au personnel.....	43
<b>5.4</b>	<b>Procédures de constitution des données d'audit .....</b>	<b>43</b>
5.4.1	Type d'évènements à enregistrer .....	43
5.4.2	Fréquence de traitement des journaux d'évènements.....	44
5.4.3	Période de conservation des journaux d'évènements.....	44
5.4.4	Protection des journaux d'évènements.....	44
5.4.5	Procédure de sauvegarde des journaux d'évènements .....	44
5.4.6	Système de collecte des journaux d'évènements.....	44
5.4.7	Notification de l'enregistrement d'un évènement au responsable de l'évènement.....	44
5.4.8	Evaluation des vulnérabilités .....	44
<b>5.5</b>	<b>Archivage des données .....</b>	<b>45</b>
5.5.1	Types de données à archiver.....	45
5.5.2	Période de conservation des archives.....	45
5.5.3	Protection des archives.....	46
5.5.4	Procédure de sauvegarde des archives .....	46
5.5.5	Exigences d'horodatage des données.....	46
5.5.6	Système de collecte des archives .....	46
5.5.7	Procédures de récupération et de vérification des archives.....	46
<b>5.6</b>	<b>Changement de clé d'AC .....</b>	<b>46</b>
<b>5.7</b>	<b>Reprise suite à compromission et sinistre .....</b>	<b>47</b>
5.7.1	Procédures de remontée et de traitement des incidents et des compromissions.....	47
5.7.2	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données).....	47
5.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante.....	47
5.7.4	Capacités de continuité d'activité suite à un sinistre .....	48
<b>5.8</b>	<b>Fin de vie d'AC.....</b>	<b>48</b>
5.8.1	Transfert d'activité.....	48
5.8.2	Cessation d'activité .....	48
<b>6</b>	<b>MESURES DE SECURITE TECHNIQUES .....</b>	<b>50</b>
<b>6.1</b>	<b>Génération et installation des bi-clés.....</b>	<b>50</b>
6.1.1	Génération des bi-clés .....	50
6.1.1.1	Clés d'AC.....	50
6.1.1.2	Transmission de la clé privée à son propriétaire.....	50
6.1.1.2.1	Clés porteurs générées par l'AC.....	50
6.1.1.2.2	Clés porteurs générées par le porteur .....	50
6.1.2	Transmission de la clé privée à son propriétaire .....	51
6.1.3	Transmission de la clé publique à l'AC.....	51
6.1.4	Transmission de la clé publique de l'AC aux utilisateurs de certificats .....	51
6.1.5	Tailles des clés .....	51
6.1.5.1	Certificat AC .....	51
6.1.5.2	Certificat Porteur.....	51
6.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité .....	51
6.1.7	Objectifs d'usage de la clé .....	51
<b>6.2</b>	<b>Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques .....</b>	<b>52</b>
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques.....	52
6.2.1.1	Modules cryptographiques de l'AC.....	52
6.2.1.2	Dispositifs d'authentification et de signature des porteurs .....	52
6.2.2	Contrôle de la clé privée par plusieurs personnes .....	52

6.2.3	Séquestre de clé privée .....	52
6.2.4	Copie de secours de la clé privée.....	52
6.2.5	Archivage de la clé privée.....	52
6.2.6	Transfert de la clé privée vers / depuis le module cryptographique .....	53
6.2.7	Stockage de la clé privée dans un module cryptographique .....	53
6.2.8	Méthode d'activation de la clé privée.....	53
6.2.8.1	Clés privées d'AC .....	53
6.2.8.2	Clés privées des porteurs.....	53
6.2.9	Méthode de désactivation de la clé privée.....	53
6.2.9.1	Clés privées d'AC .....	53
6.2.9.2	Clés privées des porteurs.....	53
6.2.10	Méthode de destruction des clés privées .....	53
6.2.10.1	Clés privées d'AC .....	53
6.2.10.2	Clés privées des porteurs.....	53
6.2.11	Niveau de qualification du module cryptographique et des dispositifs .....	53
6.2.11.1	Niveau de qualification du module cryptographique et des dispositifs d'authentification .....	53
6.2.11.2	Niveau de qualification du module cryptographique et des dispositifs de création de signature..	54
<b>6.3</b>	<b>Autres aspects de la gestion des bi-clés .....</b>	<b>54</b>
6.3.1	Archivage des clés publiques .....	54
6.3.2	Durées de vie des bi-clés et des certificats .....	54
<b>6.4</b>	<b>Données d'activation .....</b>	<b>54</b>
6.4.1	Génération et installation des données d'activation .....	54
6.4.1.1	Génération et installation des données d'activation correspondant à la clé privée de l'AC.....	54
6.4.1.2	Génération et installation des données d'activation correspondant à une clé privée du porteur..	54
6.4.2	Protection des données d'activation .....	54
6.4.2.1	Protection des données d'activation correspondant à la clé privée de l'AC .....	55
6.4.2.2	Protection des données d'activation correspondant aux clés privées des porteurs .....	55
6.4.3	Autres aspects liés aux données d'activation .....	55
<b>6.5</b>	<b>Mesures de sécurité des systèmes informatiques .....</b>	<b>55</b>
6.5.1	Exigences de sécurité technique spécifiques aux systèmes informatiques .....	55
6.5.2	Niveau de qualification des systèmes informatiques .....	55
<b>6.6</b>	<b>Mesures de sécurité liées au développement des systèmes .....</b>	<b>55</b>
6.6.1	Mesures liées à la gestion de la sécurité.....	56
6.6.2	Niveau d'évaluation et sécurité du cycle de vie des systèmes.....	56
<b>6.7</b>	<b>Mesures de sécurité réseau .....</b>	<b>56</b>
<b>6.8</b>	<b>Horodatage/Système de datation .....</b>	<b>56</b>
<b>7</b>	<b>PROFILS DES CERTIFICATS ET DES LCR .....</b>	<b>58</b>
<b>7.1</b>	<b>Profil des Certificats.....</b>	<b>58</b>
7.1.1	Extensions de Certificats .....	58
7.1.1.1	Certificat AC .....	58
7.1.1.2	Certificats de porteur .....	58
7.1.2	Identifiant d'algorithmes .....	59
7.1.3	Formes de noms .....	59
7.1.4	Identifiant d'objet (OID) de la Politique de Certification .....	59
<b>7.2</b>	<b>Profil des LCR.....</b>	<b>59</b>
7.2.1	LCR et champs d'extensions des LCR .....	59
<b>8</b>	<b>AUDIT DE CONFORMITE ET AUTRES EVALUATIONS .....</b>	<b>60</b>
<b>8.1</b>	<b>Fréquences et / ou circonstances des évaluations .....</b>	<b>60</b>
<b>8.2</b>	<b>Identités / qualifications des évaluateurs .....</b>	<b>60</b>
<b>8.3</b>	<b>Relations entre évaluateurs et entités évaluées .....</b>	<b>61</b>
<b>8.4</b>	<b>Sujets couverts par les évaluations .....</b>	<b>61</b>
<b>8.5</b>	<b>Actions prises suite aux conclusions des évaluations.....</b>	<b>61</b>
<b>8.6</b>	<b>Communication des résultats .....</b>	<b>61</b>
<b>9</b>	<b>AUTRES PROBLEMATIQUES METIERS ET LEGALES .....</b>	<b>62</b>
<b>9.1</b>	<b>Tarifs.....</b>	<b>62</b>

<b>9.2</b>	<b>Responsabilité financière</b> .....	<b>62</b>
<b>9.3</b>	<b>Confidentialité des données professionnelles</b> .....	<b>62</b>
9.3.1	Périmètre des informations confidentielles .....	62
9.3.2	Informations hors du périmètre des informations confidentielles .....	62
9.3.3	Responsabilités en termes de protection des informations confidentielles .....	62
<b>9.4</b>	<b>Protection des données personnelles</b> .....	<b>62</b>
9.4.1	Politique de protection des données personnelles .....	62
9.4.2	Informations à caractère personnel .....	62
9.4.3	Informations à caractère non personnel .....	62
9.4.4	Responsabilité en termes de protection des données personnelles .....	63
9.4.5	Notification et consentement d'utilisation des données personnelles .....	63
9.4.6	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives .....	63
9.4.7	Autres circonstances de divulgation d'informations personnelles .....	63
<b>9.5</b>	<b>Droits relatifs à la propriété intellectuelle et industrielle</b> .....	<b>63</b>
<b>9.6</b>	<b>Interprétations contractuelles et garanties</b> .....	<b>64</b>
9.6.1	Autorités de Certification .....	64
9.6.2	Service d'enregistrement .....	64
9.6.3	Porteurs de certificats .....	65
9.6.4	Utilisateurs de certificats .....	65
9.6.5	Autres participants .....	65
<b>9.7</b>	<b>Limite de garantie</b> .....	<b>65</b>
<b>9.8</b>	<b>Limites de responsabilité</b> .....	<b>66</b>
<b>9.9</b>	<b>Indemnités</b> .....	<b>66</b>
<b>9.10</b>	<b>Durée et fin anticipée de validité de la PC</b> .....	<b>66</b>
9.10.1	Durée de validité .....	66
9.10.2	Fin anticipée de validité .....	66
9.10.3	Effets de la fin de validité et clauses restant applicables .....	66
<b>9.11</b>	<b>Notifications individuelles et communications entre les participants</b> .....	<b>67</b>
<b>9.12</b>	<b>Amendements à la PC</b> .....	<b>67</b>
9.12.1	Procédures d'amendements .....	67
9.12.2	Mécanisme et période d'information sur les amendements .....	67
9.12.3	Circonstances selon lesquelles un OID doit être changé .....	67
<b>9.13</b>	<b>Dispositions concernant la résolution de conflits</b> .....	<b>67</b>
<b>9.14</b>	<b>Juridictions compétentes</b> .....	<b>67</b>
<b>9.15</b>	<b>Conformité aux législations et réglementations</b> .....	<b>67</b>
<b>9.16</b>	<b>Dispositions diverses</b> .....	<b>68</b>
9.16.1	Accord global .....	68
9.16.2	Transfert d'activités .....	68
9.16.3	Conséquences d'une clause non valide .....	68
9.16.4	Application et renonciation .....	68
9.16.5	Force majeure .....	68
<b>9.17</b>	<b>Autres dispositions</b> .....	<b>68</b>
<b>10</b>	<b>ANNEXE 1 : DOCUMENTS CITES EN REFERENCE</b> .....	<b>69</b>
10.1	Réglementation .....	69
10.2	Documents techniques .....	69
<b>11</b>	<b>ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC</b> .....	<b>70</b>
11.1	Exigences sur les objectifs de sécurité .....	70
11.2	Exigences sur la qualification .....	70
<b>12</b>	<b>ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE SIGNATURE</b> .....	<b>71</b>
12.1	Exigences sur les objectifs de sécurité .....	71
12.1.1	Authentification .....	71
12.1.2	Signature .....	71
12.2	Exigences sur la qualification .....	72
12.2.1	Authentification .....	72
12.2.2	Signature .....	72

OID : 1.2.250.1.120.2.2.1.2 /  
1.2.250.1.120.2.3.1.2

Date : 15/10/2011

**Ministère de la Justice et des Libertés**

**POLITIQUE DE CERTIFICATION – AC Personnes**



Page 8



## 1 INTRODUCTION

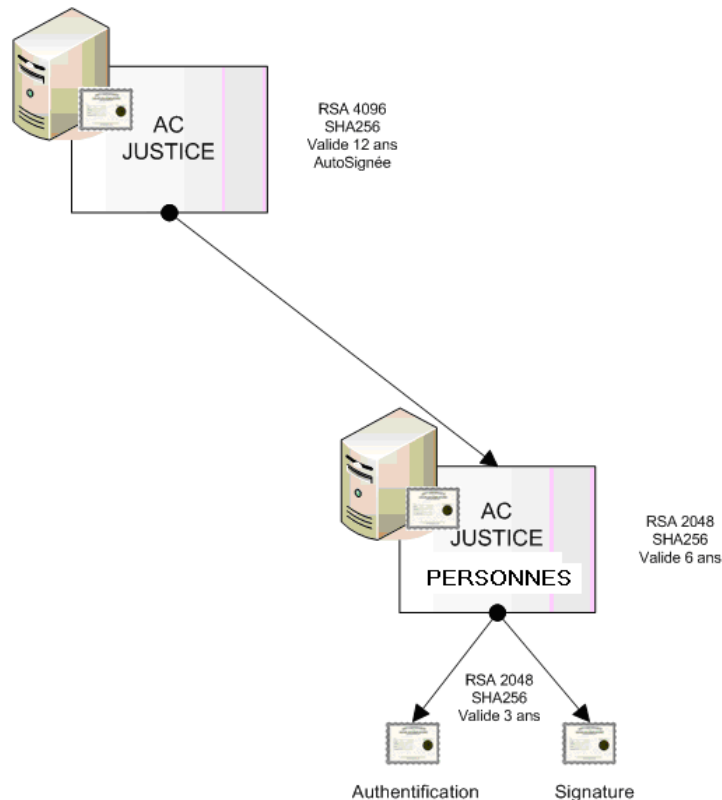
### 1.1 Généralités

Le Ministère de la Justice et des Libertés (MJL) met en place une Infrastructure de Gestion de Clés (IGC) afin de gérer les certificats de clés publiques de son personnel disposant d'un dossier administratif personnel.

Dans le cadre de cette PC, les certificats mis à disposition des porteurs sont au nombre de deux :


- un certificat à usage d'authentification au niveau \*\*\* du RGS, et
- un certificat à usage de signature électronique au niveau \*\*\* du RGS, permettant une signature « présumée fiable » au sens de l'article 1316-4 du code civil.

Ces certificats d'utilisateurs sont émis par une Autorité de Certification (AC) dite « en ligne » appelée « AC Personnes ». L'AC Personnes est placée hiérarchiquement sous une AC supérieure appelée « AC Justice ».



L'AC Justice génère un certificat auto-signé qui peut être utilisé comme racine de confiance pour vérifier la validité d'un chemin de certification. L'AC Justice a vocation à être rattachée à l'IGC gouvernementale appelée IGC/A. Lorsque ce rattachement aura été effectué, il sera possible d'utiliser le certificat auto-signé de l'IGC/A en lieu et place ou en complément de celui de l'IGC Justice.

La présente politique de certification (PC) a pour objet de décrire la gestion du cycle de vie des certificats des porteurs et des bi-clés associées.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 10
---	--	---

La présente Politique de Certification est élaborée conformément :

- Au RFC 3647 « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;
- A la Politique de Certification Type Authentication, version 2.3 du Référentiel Général de Sécurité, OID 1.2.250.1.137.2.2.1.2.2.1
- A la Politique de Certification Type Signature, version 2.3 du Référentiel Général de Sécurité, OID 1.2.250.1.137.2.2.1.2.2.2

L'AC fournit au porteur un dispositif sécurisé de création de signature, qui contient les clés privées et les certificats. Ces dispositifs sécurisés sont qualifiés au niveau renforcé, selon le processus décrit dans le [RGS], et sont conformes aux exigences du chapitre XII.1 de la Politique de Certification Type Signature.

L'utilisation d'un certificat à usage de signature électronique au niveau \*\*\* du RGS, associé à l'usage d'un dispositif sécurisé de signature électronique et d'un logiciel permettant de générer des signatures sécurisées permet d'obtenir une signature électronique « présumée fiable » jusqu'à preuve du contraire, au sens de l'article 1316-4 du code civil.

De manière à faciliter l'identification des différences entre les certificats destinés à l'authentification et ceux destinés à la signature, les exigences spécifiques à un certificat sont encadrées, le titre du cadre précisant le type de certificat auquel l'exigence s'applique. Les exigences qui ne sont pas encadrées s'appliquent de manière identique pour les deux types de certificats.

Nota : La gestion du certificat de l'AC Personnes et de la bi-clé associée est décrite dans la PC AC Racine Justice.

## 1.2 Nom du document et identification

La présente PC appelée : « PC Personnes » est la propriété du Ministère de la Justice et des Libertés.

Ce document couvre deux politiques de certification :


- La politique de certification pour les certificats d'authentification de l'AC Personnes, identifiée par le numéro d'identifiant d'objet (OID) 1.2.250.1.120.2.3.1.2;
- La politique de certification pour les certificats de signature de l'AC Personnes, identifiée par le numéro d'identifiant d'objet (OID) 1.2.250.1.120.2.2.1.2.

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins les seuls identifiants de la version applicable des PC sont les OID.

## 1.3 Entités intervenant dans l'IGC

L'AC s'appuie sur les composantes et sous-composantes suivantes :

- Service d'enregistrement: Ce service, aussi appelé « Autorité d'Enregistrement » (AE), est assuré par le personnel du MJL qui dispose d'un dossier administratif personnel qui utilise, en amont, des annuaires contenant les Dossiers Administratifs Personnels des agents de l'Etat. Les personnes affectées à ce service génèrent des demandes de certificat en se connectant sur un portail dédié. Chaque personne assurant ce service est appelée un « Opérateur de Certification » (OC).
- Service de génération des certificats : Ce service est assuré par un Opérateur de Services de Certification (OSC) qui génère les certificats électroniques des porteurs à partir des informations transmises par le service d'enregistrement qui ont été préalablement vérifiées et validées par ledit service.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2	<b>Ministère de la Justice et des Libertés</b>	 République Française
Date : 15/10/2011	<b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	Page 11

- Service de génération des éléments secrets du porteur : Ce service permet de personnaliser graphiquement et électriquement (génération de bi-clés dans le support de bi-clés) les supports de bi-clé(s) cryptographique(s) en utilisant les données fournies par le service de génération de certificats. Ce service permet également de générer et d'insérer une donnée d'activation dans les supports de clés privées. Cette donnée d'activation consiste en un code d'activation qui permettra au porteur de créer deux codes personnels, appelés « Personal Identification Number » (PIN) afin de protéger/activer chacune des deux clés privées cryptographiques. Ce service génère aussi deux codes de déblocage de support de bi-clé, appelé « Personal Unblocking Key » (PUK). Le code d'activation et les supports de clés privées sont communiqués aux porteurs en utilisant deux chemins différents.
- Service de remise au porteur : Ce service remet au porteur sa carte porteuse de deux certificats : un certificat d'authentification et un certificat de signature. La remise de la carte au porteur est effectuée par le service d'enregistrement dans ses locaux. Les données d'activation sont adressées exclusivement au porteur sur son lieu de travail au moyen d'un courrier postal envoyé en recommandé avec accusé réception.
- Service de publication : Ce service met à disposition des utilisateurs de certificat (UC) au moyen d'un Intranet et de l'Internet les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, politiques de certification publiées par l'AC, certificats d'AC, ...), ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations (LCR, avis d'information, ...);
- Service de gestion des révocations : Ce service traite de la prise en compte des demandes de révocation des certificats des porteurs et détermine les actions à mener. Les résultats des traitements sont diffusés via le service d'information sur l'état des certificats;
- Service d'information sur l'état des certificats : Cette fonction fournit aux utilisateurs de certificats (UC) des informations sur l'état des certificats. Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers sous la forme de Listes de Certificats Révoqués (LCR).
- Service de journalisation : Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC. Il est assuré par l'OSC. Il permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audits consultables. La DPC apporte plus de précisions sur cet aspect.
- Service d'audit : Ce service est assuré par le FSSI.

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 (notée DPC) apporte des détails sur les pratiques de l'IGC dans cette perspective.

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


### **1.3.1 Ministère de la Justice et des Libertés (AC – AE – SP)**

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

Le Ministère de la Justice et des Libertés a le rôle d'Autorité de Certification.

L'AC garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité est composé de la présente PC, des Conditions Générales d'Utilisation (CGU) et de la DPC associée. Elle valide le référentiel de sécurité. Elle autorise et valide la création et l'utilisation des composantes des AC. Elle suit les audits et/ou contrôle de conformités effectués sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

L'AC a pour responsabilité de garantir le lien (infalsifiable et univoque) entre l'identifiant d'un porteur et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par la clé privée de l'AC.

<p>OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2</p> <p>Date : 15/10/2011</p>	<p style="text-align: center;"><b>Ministère de la Justice et des Libertés</b></p> <p style="text-align: center;"><b>POLITIQUE DE CERTIFICATION – AC Personnes</b></p>	 <p style="text-align: center;">Page 12</p>
---	---	--

En tant qu'autorité, l'AC :

- définit et valide l'organisation de l'IGC ;
- définit et contrôle la présente PC, les CGU et la DPC associée ;
- contrôle la mise en œuvre de la DPC ;
- arbitre les litiges.

L'AC peut déléguer tout ou partie de ces fonctions.

Dans le cadre de l'AC Personnes, elle délègue ses services de la façon suivante :

- à la Sous-direction de l'informatique et des télécommunications (SDIT) du MJL la tenue d'un annuaire où figurent tous leurs agents de l'Etat.
- au secrétariat général (SG) et direction des services judiciaires (DSJ) du MJL, l'habilitation des agents de l'Etat du MJL ayant un rôle à jouer dans le cadre de l'enregistrement des utilisateurs au niveau AE, AEC; AED ou OC.
- aux agents de l'Etat du MJL ayant le rôle d'AE, AEC; AED ou OC, pour l'enregistrement des utilisateurs et la remise aux porteurs des supports de clés privées.
- à l'Opérateur de Service de Certification (OSC) : la génération des certificats et leur renouvellement, la génération des éléments secrets du porteur ainsi que des données d'activation temporaires et la gestion des révocations et les systèmes informatiques utilisés par les OC pour l'enregistrement.
- à l'OSC l'acheminement des cartes d'agent et des codes d'activation.
- à la Sous-direction de l'informatique et des télécommunications (SDIT) du MJL : la publication des PC, CGU et des certificats d'AC ainsi que l'information sur l'état des certificats.

### 1.3.1.2 Autorité d'Enregistrement (AE)

Le Ministère de la Justice et des Libertés a le rôle d'Autorité d'Enregistrement.

L'AE est responsable de la délivrance des supports de clés et des certificats aux porteurs lors d'un face à face. L'AE effectue en outre, les opérations de demandes de certificat à la vue des données fournies par différents systèmes d'information. L'AE peut intervenir pour la révocation d'un certificat octroyé à toute personne située dans la hiérarchie de l'AE (AEC, AED ou OC).

L'Autorité d'Enregistrement du MJL est structurée sur la base d'un système hiérarchique à quatre niveaux.

- Le niveau inférieur est celui des Opérateurs de Certification (OC). Ce sont eux qui ont un contact en face à face avec les porteurs lors de la remise du support cryptographique. Les Opérateurs de Certification (OC) sont désignés par des personnes ayant le rôle d'Autorité d'Enregistrement Déléguée (AED).
- Les personnes ayant le rôle d'Autorité d'Enregistrement Déléguée (AED) sont désignées par des personnes ayant le rôle d'Autorité d'Enregistrement Centrale (AEC). Les personnes ayant le rôle d'AED assurent la validation des demandes de certificat initiées par les Opérateurs de Certification (OC). Chacune des personnes ayant le rôle d'AED peut désigner d'autres AED pour l'assister dans son travail. Les RGRH désignent ainsi comme AED le directeur de greffe de la cour d'appel et les directeurs de greffe des juridictions de leur ressort ayant accès au dossier administratif personnel.
- Les personnes ayant le rôle le rôle d'Autorité d'Enregistrement Centrale (AEC).sont désignées par des personnes ayant le rôle d'Autorité d'Enregistrement (AE). L'AEC est chargée de désigner les RGRH comme AED et d'assurer le suivi de ces acteurs.
- Les personnes ayant le rôle d'Autorité d'Enregistrement (AE) sont initialement désignées, sur demande du Secrétariat Général du MJL, par l'administrateur technique de l'annuaire du MJL. L'AE « direction des

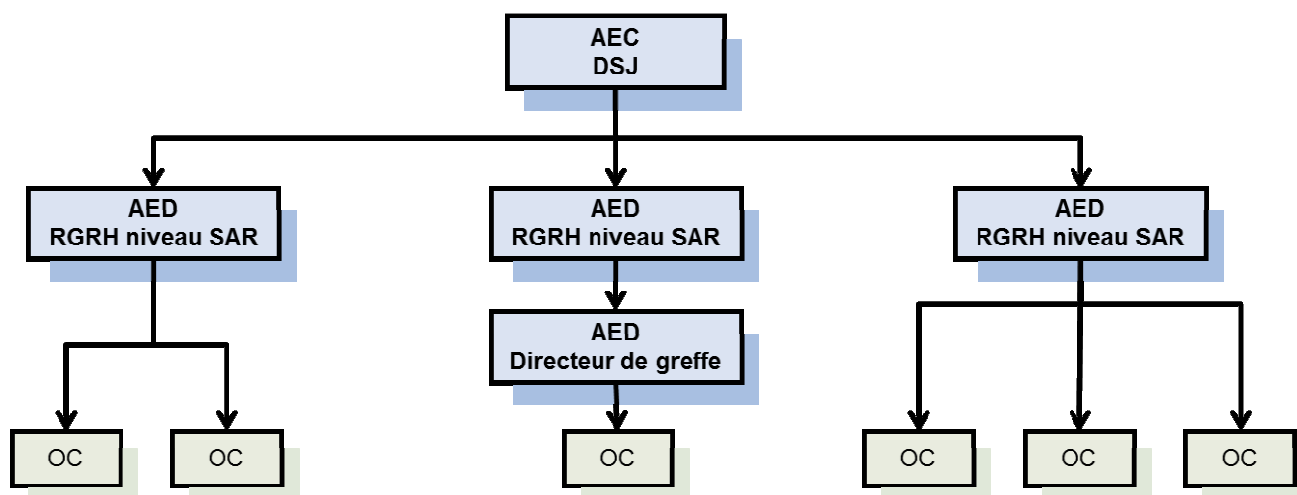
services judiciaires » désigne une AEC au sein de ses services. Toute personne ayant acquis le rôle d'Autorité d'Enregistrement (AE) peut désigner un alter-ego.

Les personnes ayant le rôle d'Autorité d'Enregistrement (AE), d'Autorité d'Enregistrement Centrale (AEC), d'Autorité d'Enregistrement Déléguée (AED) ou d'Opérateur de Certification (OC) sont dotées de certificats de clé publiques et de supports de clés (cartes agent).

La SDIT du MJL tient à jour un annuaire où figurent tous les agents du MJL ayant un rôle à jouer dans le cadre de l'enregistrement des utilisateurs. Chaque agent dispose d'un profil qui définit le périmètre des actions qu'il peut effectuer dans le cadre de l'un des rôles décrits ci-dessus. Ce profil permet de gérer leur site de rattachement et leurs habilitations. Le détail des habilitations figure dans la DPC.

L'enregistrement utilise des informations externes à l'IGC, disponibles sur des systèmes d'information existants. Ces systèmes d'information sont de confiance (informations détenues par les services de l'État, fichier des ressources humaines d'un organisme, etc.).

Pour l'AC Personnes, l'AE est organisée selon le schéma suivant.



#### 1.3.1.2.1 Autorité d'Enregistrement Centralisée (AEC)

Les personnes ayant le rôle d'AEC sont désignées par l'AE. Une fois désignées, elles sont en mesure d'obtenir un certificat et un support de clés. Lors de leur désignation, il leur est attribué un profil d'habilitation qui limite les juridictions situées dans leur domaine de responsabilité.

#### 1.3.1.2.2 Autorité d'Enregistrement Déléguée (AED)

Les personnes ayant le rôle d'AED sont désignées par l'AEC ou mandatés par l'AED. Une fois désignées, elles sont en mesure d'obtenir un certificat et un support de clés. Lors de leur désignation, il leur est attribué un profil d'habilitation qui limite les juridictions et/ou les sites situées dans leur domaine de responsabilité.

Les personnes ayant le rôle d'AED sont les Responsables de Gestion des Ressources Humaines (RGRH) des trente-cinq Services Administratifs Régionaux (SAR) des Cours d'Appel ainsi que les directeurs de greffe ayant accès au dossier administratif personnel.

#### 1.3.1.2.3 Opérateur de Certification (OC)

Les opérateurs de certification (OC) sont les personnes désignées par une AED. Une fois désignées, elles sont en mesure d'obtenir un certificat et un support de clés. Lors de leur désignation, il leur est attribué un profil d'habilitation qui limite les juridictions et/ou les sites situées dans leur domaine de responsabilité.

L'OC effectue les opérations de demandes de certificat à la vue des données fournies par les différents systèmes d'information. Les demandes effectuées par l'OC doivent être validées par une personne ayant le rôle d'AED. Une fois validées les demandes sont transmises à l'AC.

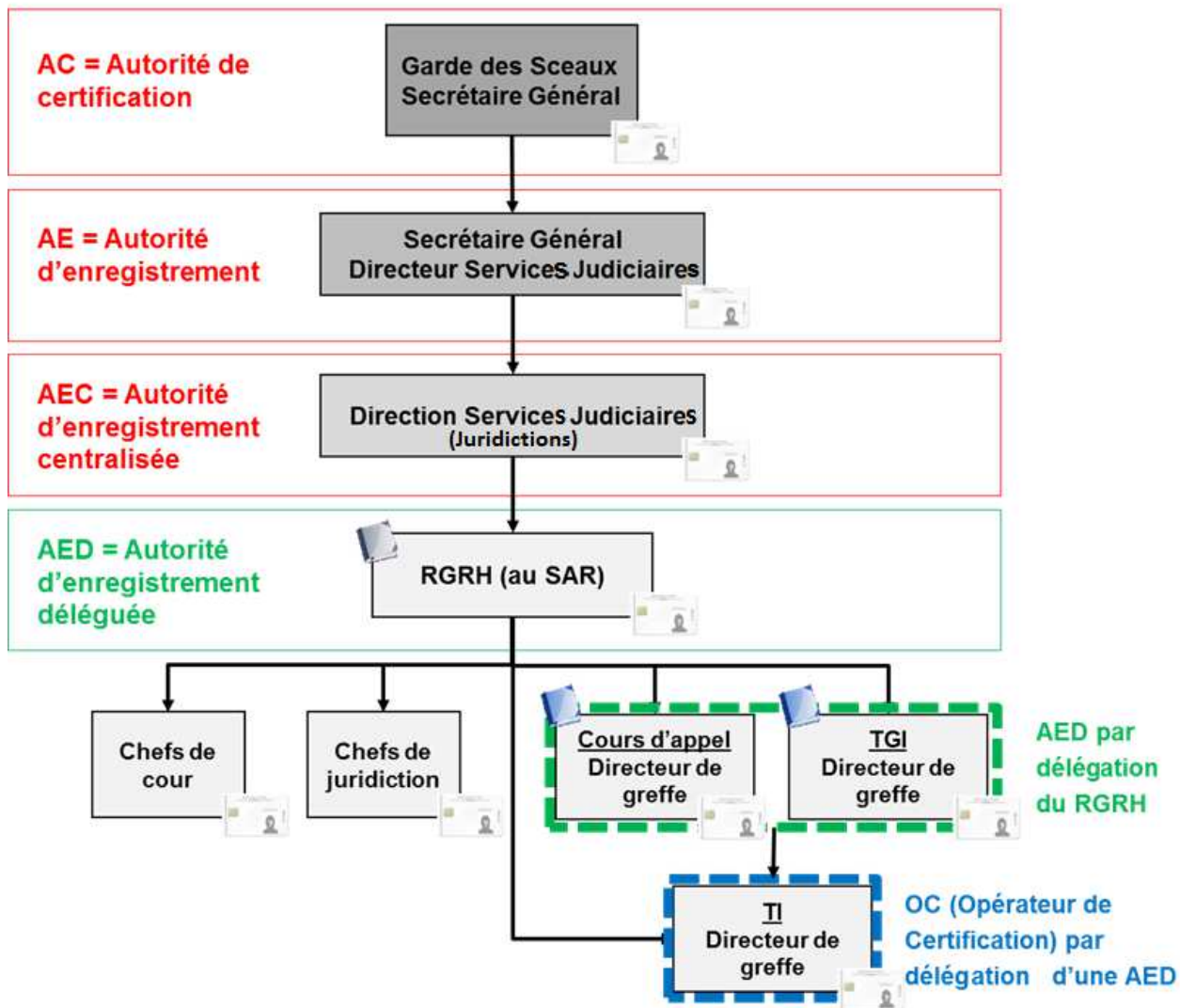
La remise des supports (cartes) est effectuée par l'AED ou l'OC qui s'assure de l'identité du porteur au cours d'un face à face.

L'OC est aussi en mesure d'effectuer des demandes de révocation pour le compte d'un porteur.

Pour les dossiers de demande, l'OC remonte les justificatifs au niveau de l'AED dont il dépend. L'OC ne peut pas valider un dossier de demande.


### 1.3.1.3 Organisation de la DSJ (Direction des Services Judiciaires)

## Scénario d'attribution des rôles de confiance DSJ



Le Directeur des Services Judiciaires, désigné au niveau AE, désigne des AEC au sein de ses services.

L'AEC désigne les personnes ayant le rôle d'AED, ce sont les Responsables de Gestion des Ressources Humaines (RGRH) des trente-cinq Services Administratifs Régionaux (SAR) des Cours d'Appel. Une personne

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 15
---	--	--


ayant le rôle d'AED peut désigner des mandataires, typiquement les Directeurs de Greffe ayant accès au dossier administratif personnel.

Les RGRH (AED) des 35 Cours d'Appel du MJL désignent ensuite les OC. Pour les AEC, ainsi que les AED et les OC nommées par les AED, leur désignation est effectuée selon les modalités décrites dans la DPC.

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

Le Ministère de la Justice et des Libertés a le rôle de Service de Publication.

Le SP est une entité qui met à disposition des utilisateurs de certificat (UC) au moyen d'un Intranet et de l'Internet les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, politiques de certification publiées par l'AC, certificats d'AC, ...). Ce service met aussi à disposition des utilisateurs de certificat (UC) les informations de validité des certificats issues des traitements du service de gestion des révocations (LCR, avis d'information, ...). Le SP s'appuie sur les moyens du MJL et de l'OSC afin de réaliser ses services.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 16
---	--	---

### **1.3.2 Agence Nationale des Titres Sécurisés (CPS - OSC)**

#### **1.3.2.1 Centre de Personnalisation des Supports (CPS)**

L'Agence Nationale des Titres Sécurisés (ANTS) a le rôle de Centre de Personnalisation des Supports.

Un CPS dispose d'une plate-forme pour mettre en œuvre le service de personnalisation et de gestion des supports de bi-clé et la fourniture aux porteurs d'un code d'activation temporaire.

Le centre dispose en outre d'un service de journalisation et d'audit au profit des porteurs conformément à la présente PC et à la DPC applicable.

Le CPS est hébergé et mis en œuvre par l'Opérateur de Services de Certification (OSC).

Le CPS possède un plan de continuité d'activité sur lequel s'appuie l'AC pour la continuité des services d'IGC. Une analyse de risques et ce plan de continuité couvrent le seul périmètre du CPS en tant qu'hébergeur de moyens qui permettent à l'AC de mettre en œuvre ses services d'IGC.

L'organisation et la sécurisation du CPS relèvent de la politique de sécurité de l'OSC.

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

L'Agence Nationale des Titres Sécurisés (ANTS) a le rôle d'Opérateur de Service de Certification.

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

L'OSC possède un plan de continuité d'activité sur lequel s'appuie l'AC pour la continuité des services d'IGC. Une analyse de risques et ce plan de continuité couvrent le seul périmètre de l'OSC en tant qu'hébergeur de moyens qui permettent à l'AC de mettre en œuvre ses services d'IGC.

L'OSC met en place un service de journalisation et d'audit pour les composantes techniques qu'il opère.

Dans la présente PC, le rôle et les obligations de l'OSC ne sont pas toujours distingués de ceux de l'AC. Cette distinction est précisée dans la DPC.

### **1.3.3 Autres participants**

#### **1.3.3.1 Porteur de certificats**

Un porteur de certificats est une personne physique fait nécessairement partie du personnel du Ministère de la Justice et des Libertés et qui possède un dossier administratif personnel.


Un porteur de certificat dispose d'une carte à microcircuit qui comporte deux couples clé privée/certificat, l'un à usage d'authentification et l'autre à usage de signature électronique.

- « certificat d'authentification Personnes » : certificat généré par l'AC Personnes dont les conditions de recevabilité sont décrites dans la Politique de Certification AC Personnes,
- « certificat de signature Personnes » : certificat généré par l'AC Personnes dont les conditions de recevabilité sont décrites dans la Politique de Certification AC Personnes.

Chaque couple est activable/ déverrouillable par l'usage d'un code PIN (Personal Identification Number).

Nota : Dans la suite du document, le terme UF (Utilisateur Final) fait référence à un porteur de certificats.



OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 17
---	--	--

### 1.3.3.2 Utilisateur de Certificats (UC)

L'UC est une application, une personne physique ou morale, un organisme administratif ou un système informatique matériel qui utilise un certificat de porteur conformément à la politique de sécurité du Ministère de la Justice et des Libertés, dans le cadre d'une authentification ou d'une signature électronique.

Dans le cadre de la présente PC, un UC, pour s'assurer de la validité d'un certificat d'un porteur, doit construire et valider un chemin de certification depuis le certificat du porteur jusqu'à une racine de confiance auto-signée qui en la circonstance peut être celle du MJL ou celle de l'IGC/A et doit en outre contrôler les informations de révocation pour chaque élément du chemin de certification (LCR pour le certificat du porteur et LAR pour les certificats d'AC).

## 1.4 Usage des certificats

### 1.4.1 Utilisation appropriée des certificats

#### 1.4.1.1 Certificat de l'AC

La bi-clé de l'AC sert à signer des certificats de porteurs et les Listes de Certificats Révoqués (LCR).

Pour cette AC, les chaînes de certificats issues de l'IGC Personnes possèdent la structure suivante :

- Certificat d'ACR (« AC Justice ») : certificat électronique auto-signé d'une AC racine ;
- Certificat de l'AC « Personnes Agents » : certificat électronique délivré à l'AC Personnes par l'AC Justice ;
- Certificat de porteur : certificat électronique délivré à un porteur par l'AC Personnes.

Note : l'AC racine du Ministère de la Justice et des Libertés (« AC Justice ») a vocation à être signée par l'infrastructure de gestion de la confiance de l'administration « IGC/A ». Dans ce cas la chaîne de certification deviendra IGC/A → AC Justice → AC Personnes → Certificat de porteur.

#### 1.4.1.2 Certificats de porteur

Le porteur dispose de deux certificats :

- le certificat d'authentification sert à authentifier le porteur, typiquement lors d'une authentification du type « client SSL ».
- le certificat de signature sert à vérifier qu'un document a été effectivement signé à l'aide d'une signature électronique sécurisée.

Ces certificats ne sont utilisables que dans le cadre des activités professionnelles, uniquement sur des postes de travail du MJL et uniquement sur les applications professionnelles supportant les cartes à microcircuit qui sont mises à disposition des porteurs par le MJL.

Les certificats ne peuvent être utilisés que conformément aux lois en vigueur et à la réglementation applicable à la profession.


### 1.4.2 Utilisation interdite des certificats

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au paragraphe ci-dessus et par la présente PC ne sont pas autorisées.

Dans le cas où cette interdiction serait outrepassée, l'AC ne peut être en aucun cas être tenue pour responsable d'une utilisation des certificats qu'elle émet.

## 1.5 Gestion de la PC

### 1.5.1 Entité gérant la PC

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 18
---	--	---

Le Ministère de la Justice et des Libertés est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC. A cette fin, il met en œuvre et coordonne une organisation dédiée, qui statue à échéances régulières, sur la nécessité d'apporter des modifications à la PC.

#### **1.5.2 Point de contact**

La personne responsable est le Secrétaire Général du Ministère de la Justice et des Libertés, qui est Haut Fonctionnaire de Défense et de Sécurité (HFDS).

#### **1.5.3 Entité déterminant la conformité d'un DPC avec cette PC**

Le Ministère de la Justice et des Libertés 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 Procédures d'approbation de la conformité de la DPC**


Les personnes ou les sociétés habilitées à déterminer la conformité de la DPC avec la présente PC sont choisies par le Ministère de la Justice et des Libertés sur la base, en particulier, de leur capacité à réaliser des évaluations de sécurité. Ces personnes ou ces sociétés sont rémunérées par le MJL, mais sont des personnes indépendantes du MJL.

Le Ministère de la Justice et des Libertés s'assure de la conformité de la DPC avec la présente PC pour la mise en œuvre opérationnelle des composantes de l'IGC Personnes.

## 1.6 Définitions et Acronymes

### 1.6.1 Acronymes

AA	Autorité Administrative
AC	Autorité de Certification
ACR	Autorité de Certification Racine (Certification Racine de Confiance)
AE	Autorité d'Enregistrement
AEC	Autorité d'Enregistrement Centrale
AED	Autorité d'Enregistrement Délégée
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANTS	Agence Nationale des Titres Sécurisés
ARL ou LAR	Authority Revocation List ou Liste des Autorités Révoquées
ASSCAP	Application de Saisie et de Suivi des Cartes d'Agent Public
CC	Critères Communs
CGU	Conditions Générales d'Utilisation
CPS	Centre de Personnalisation des Supports
CRL ou LCR	Certificate Revocation List (Liste des Certificats Révoqués)
DGME	Direction Générale de la Modernisation de l'État
DPC	Déclaration des Pratiques de Certification
DN	Distinguished Name
DSJ	Direction des Services Judiciaires
FSSI	Fonctionnaire en charge de la Sécurité des Systèmes d'Information
HFDS	Haut Fonctionnaire de Défense et de Sécurité
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
IGC/A	Infrastructure de Gestion de Clés de l'Administration
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAR ou ARL	Liste des Autorités Révoquées ou (Authority Revocation List)
LCR ou CRL	Liste des Certificats Révoqués ou (Certificate Revocation List)
MJL	Ministère de la Justice et des Libertés
NTP	Network Time Protocol
OID	Object Identifier
OC	Opérateur de Certification
OSC	Opérateur de Service de Certification
PUK	Personal Unblocking Key
PSCE	Prestataire de Services de Certification Electronique
PSCO	Prestataire de Services de Confiance
RGRH	Responsable de Gestion des Ressources Humaines
RSA	Rivest Shamir Adleman
SAR	Service Administratif Régional d'une Cour d'Appel
SHA	Secure Hash Algorithm
SP	Service de Publication
SSL	Secure Socket Layer
PC	Politique de certification
UC	Utilisateur de Certificats
UF	Utilisateur final (= porteur)
URL	Uniform Resource Locator

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 20
---	--	--

## 1.6.2 Définitions

**Autorité Administrative** : administration de l'Etat, collectivité territoriale, établissement public à caractère administratif, organisme gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail ou organisme chargé de la gestion d'un service public administratif [Ordonnance].

**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)** : entité responsable de garantir le lien (infalsifiable et univoque) entre l'identifiant d'un porteur et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par la clé privée de l'AC.

**Autorité d'Enregistrement (AE)** : entité responsable de la délivrance des supports de clés et des certificats aux porteurs lors d'un face à face. L'AE effectue en outre, les opérations de demandes de certificat à la vue des données fournies par différents systèmes d'information. L'AE peut intervenir pour la révocation d'un certificat.

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

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

**Certificat électronique** : fichier électronique attestant qu'une clé publique appartient à la personne physique ou morale identifiée dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identifiant de la personne physique ou morale et la bi-clé. Le certificat est valide uniquement s'il est utilisé pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC, le terme "certificat électronique" désigne un certificat délivré à une personne physique et portant sur une bi-clé d'authentification ou de signature, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, ...).

**Certificat d'AC** : certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509].

**Certificat d'AC 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 plusieurs certificats nécessaires pour valider un certificat vis-à-vis d'un certificat d'AC auto-signé.

**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].

**Composante** : plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.

**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 cette clé privée.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 21
---	--	---

**Confidentialité** : la propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus non autorisés.

**Déclaration des Pratiques de Certification (DPC)** : document qui identifie et référence les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

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

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

**Dispositif de création de signature** :

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

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

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

**Infrastructure de gestion de clés (IGC)** : ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques utilisés par des services de confiance.

**Infrastructure à Clé Publique (ICP)** : IGC dédiée à la gestion de clés asymétriques. C'est l'infrastructure requise pour produire, distribuer, gérer des clés publiques et privées, des certificats et des Listes de Certificats Révoqués.

**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** : ensemble de composants logiciels et matériels utilisés pour mettre en œuvre 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 œuvre la clé privée AC.

**Période de validité d'un certificat** : 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).

<p>OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2</p> <p>Date : 15/10/2011</p>	<p><b>Ministère de la Justice et des Libertés</b></p> <p><b>POLITIQUE DE CERTIFICATION – AC Personnes</b></p>	 <p>Page 22</p>
---	---	--

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

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

**Politique de Certification (PC)** : ensemble de règles, identifié par un nom (OID), définissant (a) les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes (b) les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

**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** : personne physique du Ministère de la Justice et des Libertés qui dispose d'un dossier administratif personnel ainsi que d'une carte à microcircuit comportant deux couples clé privée/certificat, l'un à usage d'authentification et l'autre à usage de signature électronique.

**Porteur de secret** : personne 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.

**Prestataire de services de confiance (PSCO)** : personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique [Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives].

**Prestataire de services de certification électronique (PSCE)** : un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE est un type de PSCO particulier.

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


**Qualification d'un prestataire de services de certification électronique** : le [DécretRGS] décrit la procédure de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

**Qualification d'un produit de sécurité** : acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS]. La procédure de qualification des produits de sécurité est décrite dans le [DécretRGS].


**RSA** : algorithme de cryptographie à clé publique inventé par Rivest, Shamir, et Adleman.

**Unité d'Horodatage** : Ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.

**Utilisateur de Certificats (UC)** : application, personne physique ou morale, organisme administratif ou système informatique matériel qui utilise un certificat de porteur conformément à la politique de sécurité du MJL dans le cadre d'une authentification ou d'une signature électronique.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 Page 23
---	--	--

**Validation d'un 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 certification (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 contenues 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.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2	<b>Ministère de la Justice et des Libertés</b>	 République Française
Date : 15/10/2011	<b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	Page 24

## 2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

### 2.1 Entités chargées de la mise à disposition des informations

Le service de publication est le service en charge de la publication du présent document et des autres documents ou informations dont la publication est nécessaire afin d'assurer la bonne utilisation des certificats délivrés au titre de la présente PC.

Le SP est chargé de mettre à disposition les informations, citées ci-après, au niveau de l'Intranet du Ministère de la Justice et des Libertés. La DPC précise les différentes interfaces du SP en fonction des informations à publier.

### 2.2 Informations devant être publiées

L'AC s'assure que les termes et conditions applicables à l'usage des certificats qu'elle délivre sont mis à la disposition des porteurs et des UC.

Les informations sont accessibles depuis le site suivant : <http://www.justice.gouv.fr/igc/ants>

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

- La présente PC ;
- Les certificats de l'AC ;
- Les conditions générales d'utilisation (CGU) des certificats ;
- Les LCR, qui sont publiées aux points de distribution des LCRs (CRL Distribution Point)<sup>1</sup>.

Nota : A partir du moment où l'IGC justice sera rattachée à l'IGC/A, le SP indiquera les liens permettant de vérifier un chemin de certification jusqu'au niveau de l'IGC/A.

### 2.3 Délais et fréquences de publication

La PC de l'AC et les documentations relatives aux demandes de certificat et de révocation sont accessibles 24 heures sur 24, 7 jours sur 7.

Le certificat de l'AC Racine à laquelle est rattachée l'AC Personnes et le certificat de l'AC personnes sont publiés préalablement à toute diffusion de certificats porteurs ou de LCR avec une disponibilité de 24h/24 7j/7.

### 2.4 Contrôle d'accès aux informations publiées

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

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

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

---

<sup>1</sup> Chaque certificat comporte l'adresse du point de distribution de la LCR le concernant.



### 3 IDENTIFICATION ET AUTHENTIFICATION

#### 3.1 Nommage

##### 3.1.1 Types de noms

Les identifiants utilisés dans un certificat sont conformes à la norme X.501. Dans chaque certificat X 509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un nom distinctif, en anglais « Distinguished Name » (DN).

##### 3.1.1.1 Certificat d'AC

L'identifiant inclus dans le certificat de l'AC est conforme aux exigences de la PC AC Racine Ministère de la Justice et des Libertés.

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

Champ de base	Valeur
Issuer DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification Justice
Subject DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification personnes

##### 3.1.1.2 Certificat de porteur

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

Champ de base	Valeur
Issuer DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification personnes
Subject DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = premier prénom de l'état civil <espace> nom de l'état civil <espace> identifiant unique.


L'identifiant unique du CN permet de faire le lien entre le certificat attribué au porteur et les données du porteur contenues dans l'annuaire qui a été utilisé à l'origine pour créer le porteur.

##### 3.1.2 Nécessité d'utilisation de noms explicites

Les identités incluses dans les certificats émis conformément à la présente PC sont toujours explicites et nominatives. Le nom de famille ou le nom d'usage et prénoms du porteur sont ceux qui correspondent à l'identité du porteur (personne) à l'état civil conformément au contenu de son dossier administratif personnel.

##### 3.1.3 Pseudonymisation des porteurs

L'identité utilisée dans les certificats de porteurs n'est ni un pseudonyme ni un nom anonyme (Voir § 3.1.2).

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 26
---	--	---

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

Les UC (applications, réseaux, machines, organisme extérieurs, ...) et les porteurs peuvent se servir des certificats d'AC et de porteurs pour mettre en œuvre et valider des fonctions de sécurité, en vérifiant entre autre les identifiants (DN) des porteurs et des AC contenues respectivement dans les certificats de porteur et d'AC.

### 3.1.5 Unicité des noms

Les DN des certificats porteurs sont uniques au sein du domaine de certification de l'AC qui émet le certificat.

L'identifiant unique qui fait partie intégrante du DN assure à lui seul l'unicité des DN, i.e. indépendamment du contenu du prénom et du nom. Cet identifiant unique peut être utilisé pour rechercher dans l'annuaire d'origine des propriétés ou des attributs liés au porteur.

Durant toute la durée de vie de l'AC, un DN attribué à un porteur ne peut être attribuée à un autre porteur.

### 3.1.6 Identification, authentification et rôle des marques déposées

Sans objet.

## 3.2 Vérification initiale d'identité

Pour être un futur porteur, il est nécessaire d'avoir été préalablement enregistré dans l'un des annuaires utilisé comme référentiel.

Les OC sont en mesure de connaître les demandes de certificats pour les sites dont ils sont responsables.

La validation initiale de l'identité consiste pour l'OC ou l'AED à :

1. vérifier que le futur porteur appartient bien au site ou bien à un site rattaché,
2. vérifier que le futur porteur fait partie d'une catégorie éligible à l'obtention d'un certificat,
3. valider la demande une fois ces vérifications effectuées,
4. transmettre la demande à l'AED dont il dépend.

La phase suivante est du ressort de l'AED. Sa tâche consiste à :


1. vérifier que le futur porteur appartient bien au site ou bien à un site rattaché,
2. vérifier que le futur porteur fait partie d'une catégorie éligible à l'obtention d'un certificat,
3. valider la demande une fois ces vérifications effectuées.

Dans le cadre de l'AC Personnes, tous les futurs porteurs sont déclarés dans l'annuaire du Ministère de la Justice et des Libertés. L'identification de la personne physique a donc été préalablement effectuée.

### 3.2.1 Méthode pour prouver la possession de la clé privée

Les clés privées initiales sont générées par l'AC. Seule la personne possédant à la fois le support des clés (une carte à microcircuit) et les codes d'activation initiaux est en mesure d'utiliser les clés privées.

Lors d'un premier renouvellement des clés privées, les bi-clés sont générées par le support de clés. Il est alors vérifié que les clés privées ont bien été générées dans le support initialement en possession du porteur. De ce fait, seul le porteur original est en mesure d'utiliser les nouvelles clés privées.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 27
---	--	--

### **3.2.2 Validation de l'identité d'un organisme**

Sans objet.

### **3.2.3 Validation de l'identité des porteurs**

Le dossier d'enregistrement déposé auprès de l'AE comprend :

- le nom de famille ou d'usage et prénoms, date de naissance, issus du dossier personnel administratif de l'agent,
- l'identifiant unique MJL,
- une adresse de messagerie permettant de contacter le porteur. Cette information est obtenue par interrogation de l'annuaire.
- une adresse pour l'expédition de la carte. Cette information est obtenue par interrogation de l'annuaire.
- une adresse pour l'expédition des codes d'activation temporaires. Cette information est obtenue par interrogation de l'annuaire.

L'authentification d'un porteur est réalisée lors d'un face à face physique entre le futur porteur et l'OC. Cette disposition permet d'être conforme au niveau (\*\*\*). Le face-à-face physique est réalisé lors de la remise au porteur du support de clés (i.e. la carte à microcircuit) qui contient à la fois les clés privées et les certificats.

L'OC s'assure de l'identité de la personne en :

- lui demandant de présenter une pièce d'identité comportant une photographie ; par exemple, la carte professionnelle, une carte d'identité ou un passeport.
- s'assurant que la personne est bien en possession de son code d'activation temporaire.

**Nota** : pour pouvoir emporter la carte, le futur porteur doit présenter à la carte le code d'activation et définir deux codes PIN, l'un pour la fonction authentification, l'autre pour la fonction signature. Si la procédure n'est pas effectuée avec succès, l'OC en est averti et la carte est alors restituée à l'OC par le futur porteur.

### **3.2.4 Informations non vérifiées du porteur**

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

### **3.2.5 Validation de l'autorité du demandeur**

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'OC et l'AED).

### **3.2.6 Certification croisée d'AC**


L'AC Personnes est uniquement rattachée à l'AC Justice. Tout autre rattachement n'est pas autorisé.

## **3.3 Identification et validation d'une demande de renouvellement des clés**

### **3.3.1 Identification et validation pour un renouvellement courant**

Lors du premier renouvellement, le porteur est invité par un courriel à se connecter à un portail qui lui permet de renouveler à la fois ses deux clés privées et ses certificats. Dans ce cas, la bi-clé est générée par la carte.

Avant l'envoi du courriel, l'AC s'assure que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide. Cette disposition permet d'être conforme au niveau (\*\*\*).

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 28
---	--	--

Le renouvellement suivant suit le même processus que celui de la première demande de certificats : le porteur reçoit un courrier postal contenant un code d'activation temporaire et qui l'invite à retirer sa carte auprès de l'OC de rattachement. Dans ce cas, la bi-clé est générée par l'AC.

Si lors du premier renouvellement l'un des certificats à renouveler a été révoqué, alors les conditions du § 3.2.2 s'appliquent.

### **3.3.2 Identification et validation pour un renouvellement après révocation**

Les vérifications aux fins de renouvellement de clés après révocation du certificat sont identiques à celles prévues par la procédure initiale (Voir § 3.2).

## **3.4 Identification et validation d'une demande de révocation**

Un certificat porteur peut être révoqué par :


- le porteur au nom duquel le certificat a été émis,
- le personnel appartenant au service qui lui a remis la carte (en l'occurrence l'OC), ou à défaut sa hiérarchie fonctionnelle (AED, AEC ou AE).

Si la demande de révocation est faite par le porteur via un service en ligne (serveur web), le demandeur est formellement authentifié sur la base d'un mot de passe connu uniquement par le porteur<sup>1</sup> et d'une série de trois questions. Cette disposition permet d'être conforme au niveau (\*\*).

Si le porteur n'est pas en mesure de présenter les quatre bonnes réponses, il doit alors s'adresser au personnel appartenant au service qui lui a remis la carte (en l'occurrence l'OC), ou à défaut sa hiérarchie fonctionnelle (AED, AEC ou AE). Ces personnes, après s'être authentifiées à l'aide d'une carte à microcircuit, sont en mesure de révoquer toute personne appartenant au site ou bien à un site rattaché.

---

<sup>1</sup> Ce mot de passe a été choisi par le porteur lors de l'activation de son support.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 29
---	--	--

## 4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

### 4.1 Demande de certificat

#### 4.1.1 Origine d'une demande de certificat

L'OC est à l'origine d'une demande de certificat. En fonction de l'avancement des projets de dématérialisation au niveau du SAR, l'OC effectue des demandes de certificats pour le compte des futurs porteurs qui ont besoin d'une carte.

Vis-à-vis de l'AC, l'AED est à l'origine des demandes de certificats des porteurs pour le Ministère de la Justice et des Libertés.

#### 4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Le dossier de demande de certificat d'un futur porteur est composé des pièces suivantes (voir § 3.2.3) :

- le nom de famille ou le nom d'usage et les prénoms,
- la date de naissance,
- l'identifiant unique MJL,
- une adresse de messagerie,
- une adresse postale pour l'expédition de la carte
- une adresse postale pour l'expédition des codes d'activation temporaires,
- une identification de l'opération : génération de certificat ou renouvellement de certificat.

L'AED établit le dossier de demande ou de renouvellement.

Si des informations supplémentaires sont requises pour la constitution du dossier de demande de certificat, alors elles sont décrites dans la DPC.

La demande de certificat est, après validation, signée par un opérateur de l'AED. Elle est alors immédiatement transmise à l'AC pour y être traitée.

### 4.2 Traitement d'une demande de certificat

#### 4.2.1 Exécution des processus d'identification et de validation de la demande

L'OC établit la demande de certificat qui est ensuite transmise à l'AED qui contrôle et valide le dossier d'enregistrement fourni (voir § 3.2.3).


#### 4.2.2 Acceptation ou rejet de la demande

Si l'AED accepte la demande de certificat initiée par l'OC, alors la demande de certificat peut être traitée. L'AED émet alors la demande de génération de la bi-clé et du certificat vers le service adéquate de l'AC. L'AC conserve une trace de la demande de certificat.

L'utilisateur final n'étant pas à l'origine de la demande, il n'est pas informé en cas de rejet.

#### 4.2.3 Durée d'établissement du certificat

Lorsque la demande de certificat de porteur est validée par l'AED, son traitement est immédiat. La durée du traitement d'une demande de certificat est précisée dans la DPC.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 30
---	--	--

### 4.3 Délivrance d'un certificat

#### 4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération de la carte, du certificat du porteur et des codes d'activation temporaires. Les conditions de génération des bi-clés et des certificats et les mesures de sécurité sont précisées aux § 5 et 6.

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

Le futur porteur est informé par un courrier postal envoyé en courrier suivi que sa carte est à sa disposition. Ce courrier postal contient un code d'activation temporaire qu'il aura à utiliser pour pouvoir activer sa carte.

### 4.4 Acceptation du certificat

#### 4.4.1 Démarche d'acceptation du certificat

Pour la remise de sa carte, le futur porteur est tenu de s'authentifier. L'authentification du porteur se fait lors d'un face-à-face au moment de la remise du support (cf. § 3.2). Après vérification de son identité au moyen d'un titre comportant une photographie (carte professionnelle, carte d'identité, passeport, ...), l'AED remet le support au porteur.

Le porteur peut contrôler l'identifiant qui figure dans ses certificats et définir deux codes PIN, l'un pour la fonction d'authentification l'autre pour la fonction de signature. Pour cela, il utilise son code d'activation temporaire et choisit ensuite ses codes PIN, puis signe les Conditions Générales d'Utilisation (CGU) au moyen de sa clé privée de signature. Après quoi, le porteur est autorisé à repartir avec son support de clés. L'AED contresigne l'attestation d'acceptation. L'AC garde une trace de l'acceptation du certificat par le porteur. Ces dispositions permettent d'être conforme au niveau (\*\*\*).

#### 4.4.2 Publication du certificat

Après l'acceptation des certificats par le porteur, ceux-ci sont publiés dans l'annuaire du MJL.

Nota : les certificats des porteurs ne sont pas publiés par le SP.

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

L'ensemble des composantes de l'IGC, à l'exception du SP, est informé de la délivrance du certificat.


### 4.5 Usages de la bi-clé et du certificat

#### 4.5.1 Utilisations de la clé privée et du certificat par le porteur

Les usages autorisés des bi-clés et des certificats sont définis au § 1.4.1.2 ci-dessus.

Le porteur dispose de deux clé privées :

- la clé privée d'authentification sert à signer numériquement des données permettant d'authentifier le porteur, typiquement lors d'une authentification du type « client SSL ».
- la clé privée de signature sert à signer numériquement des données permettant de vérifier qu'un document a été effectivement signé à l'aide d'une signature électronique sécurisée.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 31
---	--	--

L'usage d'une bi-clé et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (voir § 6.1.7).

#### Certificats d'authentification

Les bi-clés et les certificats générés dans le cadre de la PC pour les certificats d'authentification sont uniquement destinés à l'authentification des porteurs.

#### Certificats de signature

Les bi-clés et les certificats générés dans le cadre de la PC pour les certificats de signature sont uniquement destinés à la vérification de signatures électroniques sécurisées.

Cet usage est également explicité dans les conditions générales d'utilisation qui sont fournies au porteur lors de la remise du support. Le porteur est tenu de les respecter.

#### **4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat**

Un utilisateur de certificats doit utiliser des logiciels qui sont à même de vérifier que le certificat d'un porteur est effectivement utilisé selon l'usage prescrit dans le certificat (authentification ou signature). Pour cela, il doit soit utiliser les logiciels mis à sa disposition par le MJL, soit sous sa propre responsabilité utiliser des logiciels donnant les mêmes garanties. Dans le cas contraire, sa responsabilité pourrait être engagée.

Un utilisateur de certificat doit utiliser un logiciel qui vérifie que le certificat est valide. La vérification que doit effectuer le logiciel est différente selon qu'il s'agit de la vérification en temps-réel d'un échange d'authentification ou la vérification en temps différé d'une signature électronique.

Pour la vérification en temps-réel d'un échange d'authentification, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC Justice (ou ultérieurement le certificat auto-signé de l'IGC/A), et s'assurer qu'au moment de l'échange aucun des certificats du chemin n'est en dehors de sa période de validité ou révoqué.

Pour la vérification en temps différé d'une signature électronique, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC Justice (ou ultérieurement le certificat auto-signé de l'IGC/A), et s'assurer qu'au moment où la signature numérique a été horodatée par une unité d'horodatage de confiance qu'aucun des certificats du chemin n'était en dehors de sa période de validité ou révoqué. Il doit en outre s'assurer que le certificat de l'unité d'horodatage est valide.

### **4.6 Renouvellement d'un certificat**

Nota - Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique).


Dans la cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. La délivrance d'un nouveau certificat suite à changement de la bi-clé est traitée à la section 4.7.

#### **4.6.1 Causes possibles de renouvellement d'un certificat**

Sans objet.

#### **4.6.2 Origine d'une demande de renouvellement**

Sans objet.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 32
---	--	--

#### **4.6.3 Procédure de traitement d'une demande de renouvellement**

Sans objet.

#### **4.6.4 Notification au porteur de l'établissement du nouveau certificat**

Sans objet.

#### **4.6.5 Démarche d'acceptation du nouveau certificat**

Sans objet.

#### **4.6.6 Publication du nouveau certificat**

Sans objet.

#### **4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat**

Sans objet.

### **4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé**

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur liée à la génération d'une nouvelle bi-clé.

#### **4.7.1 Causes possibles de changement d'une bi-clé**

Les bi-clés des porteurs, et les certificats correspondants, sont renouvelés tous les 3 ans. Une bi-clé et un certificat peuvent aussi être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. § 4.9, notamment le § 4.9.1 pour les différentes causes possibles de révocation) ou pour anticiper un renouvellement massif de certificats.

#### **4.7.2 Origine d'une demande d'un nouveau certificat**

En temps normal, le certificat est renouvelé tous les trois ans :

- une fois sur deux, la carte est conservée et le renouvellement des bi-clés et des certificats s'effectue en ligne.
- une fois sur deux, une nouvelle carte est générée.

L'IGC gère automatiquement la durée de 3 ans.

#### **4.7.3 Procédure de traitement d'une demande d'un nouveau certificat**

Trois mois avant la fin de validité d'un certificat, l'IGC ajoute automatiquement à la liste des demandes initiales de certificats à valider, les demandes de renouvellement de certificats à valider. Ces demandes sont ventilées auprès des personnes ayant le rôle d'AED.


Ces personnes vérifient que les personnes pour lesquelles le renouvellement est demandé font toujours partie de leurs effectifs et, si cela est le cas, valident la demande de renouvellement.

#### **4.7.4 Notification au porteur de l'établissement du nouveau certificat**

Lorsque la carte est conservée, le porteur est invité par la réception d'un courriel à effectuer le renouvellement des bi-clés et des certificats en se connectant à un portail dont l'adresse est spécifiée dans ce courriel.

Lorsque la carte est changée et une fois que la nouvelle carte a été fabriquée, le porteur est invité par la réception d'un courrier postal envoyé en RAR à retirer sa nouvelle carte. La procédure est alors analogue à un retrait de carte initial.



OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  <b>Page 33</b>
---	--	---

Lorsque les certificats d'une carte ont été révoqués, la procédure est alors analogue à une demande de carte initiale.

Lors d'un renouvellement anticipé, le porteur peut recevoir, selon le cas, un courriel ou un courrier postal avant la date anniversaire.

#### **4.7.5 Démarche d'acceptation du nouveau certificat**

Lorsqu'il s'agit de la délivrance d'une nouvelle carte, se reporter à la section § 4.4.1.

Lorsqu'il s'agit d'un renouvellement des bi-clés et des certificats sans changement de carte, le porteur se connecte à un portail en utilisant sa carte. Il doit alors suivre les instructions données par le portail.

#### **4.7.6 Publication du nouveau certificat**

Après l'acceptation des certificats par le porteur, ceux-ci sont publiés dans l'annuaire du MJL.

#### **4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat**

L'ensemble des composantes de l'IGC, à l'exception du SP, est informé de la délivrance du certificat.

### **4.8 Modification du certificat**

La modification du certificat n'est pas autorisée au titre de la présente PC.

#### **4.8.1 Causes possibles de modification d'un certificat**

Sans objet.

#### **4.8.2 Origine d'une demande de modification d'un certificat**

Sans objet.

#### **4.8.3 Procédure de traitement d'une demande de modification d'un certificat**

Sans objet.

#### **4.8.4 Notification au porteur de l'établissement du certificat modifié**

Sans objet.

#### **4.8.5 Démarche d'acceptation du certificat modifié**

Sans objet.

#### **4.8.6 Publication du certificat modifié**

Sans objet.

#### **4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat modifié**

Sans objet


### **4.9 Révocation et suspension des certificats**

#### **4.9.1 Causes possibles d'une révocation**

##### **4.9.1.1 Certificats de porteurs**

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 peuvent être :

- le décès du porteur ou la cessation d'activité du porteur ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- l'information contenue dans le DN du certificat n'est plus valide (changement de nom, par exemple suite à un mariage) ;

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 34
---	--	--

- le porteur n'a pas respecté les modalités applicables à l'utilisation du certificat ;
- le support de clés du porteur a été perdu ou volé ;
- l'une des données d'activation a été compromise ou est suspectée d'avoir été compromise ;
- le support de clés du porteur est bloqué et ne peut être débloqué
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le porteur n'a pas respecté ses obligations découlant de cette PC;
- la modification de la taille des clés imposée par des institutions nationales compétentes ;
- la perte de l'autorisation de possession d'un certificat.

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

#### **4.9.1.2 Certificats d'une composante de l'IGC**

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats ou de LCR) :

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

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

##### **4.9.2.1 Certificats de porteurs**

Les personnes / entités qui peuvent demander la révocation d'un certificat porteur sont les suivantes :

- le porteur au nom duquel le certificat a été émis, ou
- une personne ayant le rôle d'AED, dans l'AED de rattachement du porteur.

##### **4.9.2.2 Certificats d'une composante de l'IGC**

La révocation d'un certificat d'une composante de l'IGC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

#### **4.9.3 Procédure de traitement d'une demande de révocation**

##### **4.9.3.1 Révocation d'un certificat de porteurs**


L'AE authentifie la demande de révocation (Voir § 4.9.2).

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

Les informations suivantes figurent dans la demande de révocation de certificat :

- l'identifiant (DN) du porteur du certificat ;
- le nom du demandeur de la révocation et ses contacts (téléphone, email) ;
- la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via la LCR signée par l'AC sans contenir la cause de révocation.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 35
---	--	---

Le demandeur de la révocation et l'AED sont informés du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il est informé de la révocation effective de son certificat par l'envoi d'un courriel.

#### **4.9.3.2 Révocation d'un certificat d'une composante de l'IGC**

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

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs et des utilisateurs de certificats concernés. Pour cela, l'AC utilise les moyens d'information à destination des agents du ministère qui sont à sa disposition (intranet, directive).

Le FFSI doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

La DGME et l'ANSSI se réservent le droit de diffuser par tout moyen l'information.

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

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

#### **4.9.5 Délai de traitement par l'AC d'une demande de révocation**

##### **4.9.5.1 Révocation d'un certificat de porteur**


Par nature, une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations est disponible 24h/24 7j/7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1 heure et une durée maximale totale d'indisponibilité par mois de 4 heures.

Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur ou égal à 24 heures. Il s'agit du délai entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

##### **4.9.5.2 Révocation d'un certificat d'une composante de l'IGC**

La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat. La révocation d'un certificat de signature de l'AC (signature de certificats et de LCR) est effectuée après accord ou sur demande du Ministère de la Justice et des Libertés.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 36
---	--	---

#### **4.9.6 Exigences de vérification de révocation par les utilisateurs de certificats**

L'utilisateur d'un certificat de porteur est tenu de vérifier, l'état des certificats de l'ensemble du chemin de certification correspondant, en utilisant une LCR pour chaque certificat faisant partie du chemin.

#### **4.9.7 Fréquence d'établissement des LCR**

Une nouvelle LCR est émise toutes les 24 heures.  
 Il n'est pas mis en place de mécanisme de delta LCR.

#### **4.9.8 Délai maximum de publication d'une LCR**

Une LCR est publiée dans un délai maximum de 30 minutes après sa génération.

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

Il n'est pas mis en place de service OCSP.

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

Sans objet, car il n'est pas mis en place de service OCSP.

#### **4.9.11 Autres moyens disponibles d'information sur les révocations**

En cas de changement de ce certificat auto-signé avant la date initialement prévue, le SP informe les porteurs et les utilisateurs de certificats qu'un nouveau certificat auto-signé est disponible et de la date de révocation programmée du certificat auto-signé courant.

#### **4.9.12 Exigences spécifiques en cas de compromission de la clé privée**

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

Le porteur, en cas de compromission de sa clé privée ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

#### **4.9.13 Causes possibles d'une suspension**

Dans le cadre de la présente PC, la suspension de certificats n'est pas autorisée.

#### **4.9.14 Origine d'une demande de suspension**


Sans objet.

#### **4.9.15 Procédure de traitement d'une demande de suspension**

Sans objet.

#### **4.9.16 Limites de la période de suspension d'un certificat**

Sans objet.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 37
---	--	---

## 4.10 Fonction d'information sur l'état des certificats

### 4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LAR / LCR au format v2. De ce fait, les LAR / LCR comportent la date au plus tard de leur prochaine publication.

Les LAR sont publiées aux points de distribution des LARs (ARL Distribution Point). Chaque certificat d'AC comporte l'adresse du point de distribution de la LAR le concernant.

Les LCR sont publiées aux points de distribution des LCRs (CRL Distribution Point). Chaque certificat d'un porteur comporte l'adresse du point de distribution de la LCR le concernant.

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

### 4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2 heures et une durée maximale totale d'indisponibilité par mois de 8 heures.

### 4.10.3 Dispositifs optionnels

Sans objet.

## 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 de clé et recouvrement


Le séquestre des clés privées des porteurs est interdit par la présente PC.

### 4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

### 4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 38
---	--	--

## 5 MESURES DE SECURITE NON TECHNIQUES

### 5.1 Mesures de sécurité physique

La section § 1.3 définit les différentes entités intervenant dans l'IGC.

- Service d'enregistrement,
- Service de génération des certificats,
- Service de génération des éléments secrets du porteur,
- Service de remise au porteur,
- Service de publication,
- Service de gestion des révocations,
- Service d'information sur l'état des certificats, et
- Service de journalisation.

Ces services ne sont pas réalisés sur le même site.

Le site d'exploitation de l'IGC regroupe les services suivants : service de génération des certificats, service de génération des éléments secrets du porteur, service de gestion des révocations et service de journalisation. Ce site est placé sous la responsabilité de l'ANTS.

Le site de mise à disposition des informations aux utilisateurs supporte le service suivant : service de publication et service d'information sur l'état des certificats. Ce site est placé sous la responsabilité du MJL.

Le service d'enregistrement et le service de remise au porteur sont des services décentralisés réalisés au niveau des 35 SAR, dans les locaux du MJL. Il s'agit des AED et des OC.

#### 5.1.1 Situation géographique et construction des sites

Le site d'exploitation de l'IGC est installé dans les locaux de l'OSC, situés sur le territoire national. La construction des sites respecte les règlements et normes en vigueur, ainsi que les recommandations de l'ANSSI. Les caractéristiques ont été définies selon les résultats de l'analyse de risques précisée dans la DPC. Les opérations cryptographiques sur l'AC sont réalisées au sein des locaux de l'OSC qui sont à plus de 20 mètres à l'intérieur d'une zone réservée au sens de l'IGI 1300.


Le site de mise à disposition des informations est installé dans les locaux du MJL.

Les sites où sont implantées les AED et les OC sont répartis sur tout le territoire national, dans les locaux du MJL.

#### 5.1.2 Accès physique

Les moyens et informations du site d'exploitation de l'IGC utilisés dans le cadre de la mise en œuvre opérationnelle de l'IGC sont installés dans une enceinte des locaux d'exploitation de l'OSC dont les accès sont contrôlés et réservés aux personnels habilités.

L'OSC met en œuvre un système de contrôle des accès qui permet de garantir la traçabilité des accès aux zones en question. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Si des personnes non habilitées doivent pénétrer dans les installations, elles font l'objet d'une prise en charge par une personne habilitée qui en assure la surveillance. Ces personnes doivent en permanence être accompagnées par des personnels habilités.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 39
---	--	---

L'OSC a défini un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans la présente PC. Ce périmètre de sécurité garantit, en cas de mise en œuvre dans des locaux en commun, que les fonctions et informations hébergées sur les machines ne sont accessibles qu'aux seules personnes ayant des rôles de confiance reconnus et autorisés. Ces points sont précisés dans la DPC. Ces dispositions permettent d'être conforme au niveau (\*\*\*).

### **5.1.3 Alimentation électrique et climatisation**

Afin d'assurer la disponibilité des systèmes informatiques du site d'exploitation de l'IGC, des systèmes de génération et de protection des installations électriques sont mis en œuvre par l'OSC. Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements du site d'exploitation de l'IGC telles que fixées par leurs fournisseurs.

### **5.1.4 Vulnérabilité aux dégâts des eaux**

Les mesures de protection contre les dégâts des eaux mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, notamment en matière de disponibilité de ses fonctions de gestion des révocations de publication et d'information sur l'état de validité des certificats.

### **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, notamment en matière de disponibilité de ses fonctions de gestion des révocations, de publication et d'information sur l'état de validité des certificats.

### **5.1.6 Conservation des supports**

Les mesures et moyens de conservation des supports d'information mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC. En particulier la disponibilité, la confidentialité et l'intégrité des données conservées dans les journaux, les archives et les logiciels utilisés par l'AC est assurée.

### **5.1.7 Mise hors service des supports**

Le site d'exploitation de l'IGC utilise des mécanismes de destruction des supports papiers (tels que des broyeurs) et des supports magnétiques d'information. Les matériels réformés ayant servi à supporter l'IGC font l'objet de mesures préalables de neutralisation. En fin de vie, les supports sont détruits.

### **5.1.8 Sauvegardes hors site**


Le site d'exploitation de l'IGC réalise des sauvegardes placées hors site en s'appuyant majoritairement sur les procédures d'exploitation interne existantes de l'OSC, ajustées en fonction des particularités de cette IGC. Celles-ci sont de nature à permettre une reprise rapide des fonctions de gestion des révocations, de publication et d'information sur l'état des certificats, suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces fonctions.

Le site de mise à disposition des informations du MJL, met en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

## **5.2 Mesures de sécurité procédurales**

L'ensemble de ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, l'OSC s'assure de la mise en œuvre effective des mesures de sécurité procédurales pour l'utilisation opérationnelle des certificats d'AC au sein de ses locaux.

### **5.2.1 Rôles de confiance**

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 40
---	--	---

Les personnes auxquelles sont attribués des rôles de confiance de l'IGC sont toutes des personnes habilitées de l'OSC ou du MJL.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité des opérations au sein de l'IGC. Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance sont classés en sept groupes :

- « Responsable de sécurité » - il est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc...
- « Responsable d'application » - il est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
  - o Pour ces responsabilités il s'appuie sur le « responsable d'application SP » et le « responsable d'application OSC » pour leurs domaines de compétences propres
- « Ingénieur système » - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- « Opérateur » - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante
- « Contrôleur » - Personnel, dont la responsabilité est de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de l'IGC Personnes. Ce personnel est désigné par le HFDS du Ministère de la Justice et des Libertés, ou par le responsable d'application de l'OSC (avec dans ce dernier cas une portée des opérations de vérification limitées aux prestations opérées par l'OSC).
- « Autorité d'Enregistrement » - Personnel du Ministère de la Justice dont la responsabilité est la mise en œuvre d'un service d'enregistrement (demande de certificats, gestion des révocations...). L'AE doit être reconnue par l'AC pour laquelle elle authentifie, édite et valide les demandes de certificat et de révocation. L'AE effectue également les opérations de remise en face à face. Une AE peut déléguer ce rôle de confiance à une AE déléguée.
- « Opérateur de certification » - Personnel du Ministère de la Justice dont la responsabilité est d'assister une autorité d'enregistrement dans la mise en œuvre de son rôle. L'opérateur de certification peut authentifier et saisir tout type de demande mais n'est pas en mesure de les valider.

Les attributions détaillées de chaque rôle de l'IGC sont données dans l'annexe « Rôles » de la DPC.

### **5.2.2 Nombre de personnes requises par tâche**


Selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peuvent être différents. L'annexe "Rôles" de la DPC définit le nombre d'exploitants nécessaires à chaque opération.

### **5.2.3 Identification et authentification pour chaque rôle**

L'OSC procède à la vérification de l'identité et des autorisations de tout membre de son personnel amené à travailler au sein 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 l'IGC ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement aux systèmes ;



OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2	<b>Ministère de la Justice et des Libertés</b>	 LIBERTÉ • ÉGALITÉ • FRATERNITÉ RÉPUBLIQUE FRANÇAISE
Date : 15/10/2011	<b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	Page 41

- le cas échéant et en fonction du rôle tenu, qu'un compte soit ouvert à son nom sur les systèmes ;
- que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

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

#### **5.2.4 Rôles exigeant une séparation des attributions**

Les attributions de chaque rôle de l'IGC sont données dans l'annexe « Rôles » de la DPC qui précise comment et sous quelles conditions ces rôles peuvent être cumulés par un même exploitant.

La séparation de ces rôles repose sur :

- la notion de séparation des rôles dits « d'administration », des rôles dits « opérationnels » : une personne qui peut assigner des fonctions et/ou un rôle sur une composante d'IGC pour la mise en œuvre d'un service ne met pas en œuvre le service correspondant ;
- la notion de double contrôle sur un service de l'IGC : une double validation est nécessaire sur les opérations dites « sensibles » (cérémonie des clés, demande et génération d'un certificat, ...).

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur,
- contrôleur et tout autre rôle,
- ingénieur système et opérateur.

Ces dispositions permettent d'être conforme au niveau (\*\*\*) .

La mise en œuvre de cette séparation repose sur des mécanismes organisationnels et/ou techniques.

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

L'ensemble des mesures décrites dans ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, l'OSC s'assure de la mise en œuvre effective des mesures de sécurité du personnel lors de la mise en œuvre opérationnelle des certificats d'AC au sein de ses locaux.

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

Tout le personnel opérant pour le compte de l'IGC Personnes est formé pour comprendre les rôles qui leur sont attribués. Le nom et la fonction de tout le personnel intervenant pour le compte de l'IGC Personnes sont répertoriés. Le MJL et l'OSC font en sorte que les compétences professionnelles des personnes placées sous leur responsabilité soient cohérentes à leurs attributions.

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


Chaque entité opérant une composante de l'IGC s'assure de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Ils sont tenus de remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire. 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 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, au sein de l'entité dans laquelle il opère.

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

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2 Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 Page 42
---	--	--


#### **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 et dans l'organisation, en fonction de la nature de ces évolutions.

#### **5.3.5 Fréquence et séquence de rotation entre différentes attributions**

Aucune rotation n'est imposée dans le cadre de la présente PC.

---

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 43
---	--	---

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

Le responsable de l'AC Personnes décide des sanctions à appliquer lorsqu'un agent sous la responsabilité MJL abuse de ses droits ou effectue une opération non conforme à ses attributions, selon les modalités applicables. Lorsque le manquement est commis par un agent de l'OSC, le responsable de l'AC demande au responsable de l'OSC de prendre les sanctions appropriées et de lui en rendre compte. Les modalités d'application et de délégation sont précisées dans la DPC.

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

Les éventuels personnels contractants doivent respecter les mêmes conditions que celles énoncées dans le § 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

### **5.3.8 Documentation fournie au personnel**

Chaque personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille, en particulier en termes de sécurité.

## **5.4 Procédures de constitution des données d'audit**

L'ensemble de ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, l'OSC s'assure de la mise en œuvre effective des mesures de constitution des données d'audit dans la mise en œuvre opérationnelle des certificats, des supports de clé et des données d'activation au sein de ses locaux.

### **5.4.1 Type d'évènements à enregistrer**

L'IGC enregistre les évènements liés aux services et à la protection de l'AC (accès physique, ...) qu'elle met en œuvre.

Chaque enregistrement d'un évènement dans un journal contient au minimum les informations suivantes :


- le type d'évènement ;
- le nom de l'exécutant ou la référence du système déclenchant l'évènement ;
- la date et heure de l'évènement ;
- le résultat de l'évènement (échec ou réussite).

Pour les types d'évènements pour lesquels ces informations existent, les enregistrements comporteront également les champs suivants :

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

Les opérations de journalisation sont effectuées en tâche de fond tout au long de la vie de l'IGC. L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée.

En cas de saisie manuelle, l'écriture est effectuée, sauf exception, le même jour ouvré que l'évènement.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 44
---	--	---

#### **5.4.2 Fréquence de traitement des journaux d'évènements**

Les journaux d'évènements sont contrôlés et analysés sur une base hebdomadaire par un responsable de sécurité de l'OSC afin d'identifier les anomalies liées à des tentatives en échec. Cette analyse donne lieu à un résumé qui fait apparaître les anomalies et les falsifications constatées.

#### **5.4.3 Période de conservation des journaux d'évènements**

Les journaux d'évènements sont conservés pendant 5 ans après leur génération. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois. Ils restent sur le site au moins un mois.

#### **5.4.4 Protection des journaux d'évènements**

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système interne de datation de l'IGC associe à toutes les archives une date locale.

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

#### **5.4.5 Procédure de sauvegarde des journaux d'évènements**

Chaque entité intervenant pour le compte de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité de ses journaux d'évènements, conformément aux exigences de la présente PC.

#### **5.4.6 Système de collecte des journaux d'évènements**

Le système de collecte des journaux assure la collecte des archives en respectant le niveau de sécurité relatif à l'intégrité, la disponibilité et la confidentialité des données.

#### **5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement**

Le journal d'évènements permet d'imputer chaque opération sensible à toute personne, organisme ou système ayant un rôle identifié dans la présente PC.


#### **5.4.8 Evaluation des vulnérabilités**

Chaque entité intervenant pour le compte de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de son fonctionnement.

Les journaux sont analysés dans leur totalité chaque jour ouvré par un responsable de sécurité de l'OSC.

Un rapprochement entre les journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, par exemple) est effectué sur une base hebdomadaire par un responsable de sécurité de l'OSC afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

Les procédures sont détaillées dans la DPC.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 45
---	--	--

## 5.5 Archivage des données

### 5.5.1 Types de données à archiver

L'archivage permet d'assurer la pérennité des données numériques constituées lors des opérations effectuées au profit de l'IGC. Il permet également la conservation de pièces papier, ainsi que leur disponibilité en cas de nécessité.

Les informations archivées sont les suivantes :

- les PC ;
- les DPC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les engagements signés électroniquement des porteurs;
- les demandes d'enregistrement signées par le personnel ayant le rôle d'EAD ;
- les journaux d'événements des différentes entités de l'IGC.

### 5.5.2 Période de conservation des archives

#### **Dossiers de demande de certificat**

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat est en mesure d'être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par une personne ayant le rôle d'AED, permet de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

#### **Noms Distinctifs**

Tout DN (Distinguished Name) est conservé aussi longtemps que le DN de l'AC Personnes perdure. Les informations personnelles associées au DN sont conservées pendant la même durée afin de garantir qu'un même DN n'est jamais utilisé par une autre personne que le premier titulaire du DN.

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

La période de conservation des certificats et des LCR est de 30 ans après leur expiration<sup>1</sup>.

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins 5 années après leur expiration.

#### **Journaux d'évènements**

Les journaux d'évènements sont archivés pendant au moins 5 ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des journaux est assurée tout au long de leur cycle de vie.

---

<sup>1</sup> La PC Type demande cinq ans, mais cette période a été portée à trente ans.

### 5.5.3 Protection des archives

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

- sont protégées en intégrité ;
- ne sont accessibles qu'aux personnes autorisées ;
- peuvent être relues et exploitées.

### 5.5.4 Procédure de sauvegarde des archives

Le responsable de l'AC et l'OSC ont la responsabilité de mettre en place et maintenir les mesures requises afin d'assurer l'intégrité et la disponibilité de leurs archives, conformément aux exigences de la présente PC.

### 5.5.5 Exigences d'horodatage des données

Tous les composants de l'AC sont régulièrement synchronisés avec un serveur Network Time Protocol (NTP).

### 5.5.6 Système de collecte des archives

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

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

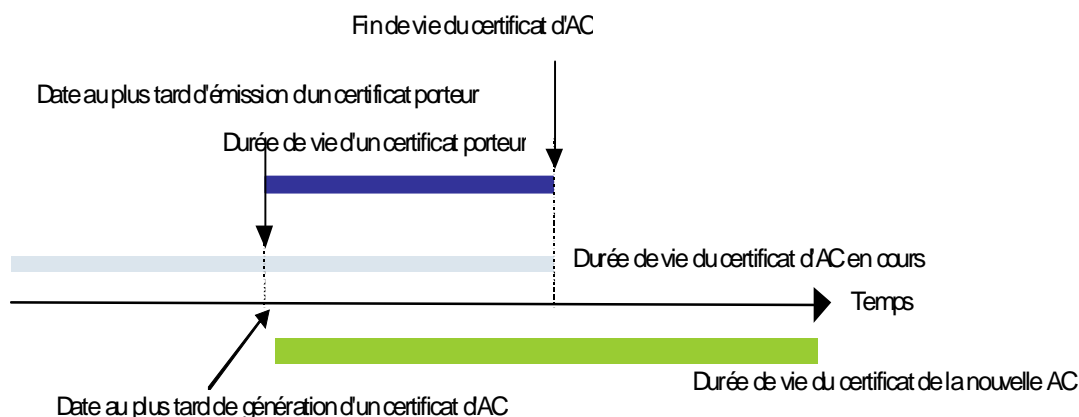
Les archives (papiers et électroniques) sont accessibles dans un délai maximum de 2 jours ouvrés.


## 5.6 Changement de clé d'AC

La durée de vie d'un certificat d'AC est de 6 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 nationales compétentes en la matière.

Une AC ne peut pas générer de certificats porteurs 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 porteurs émis. La durée de vie des certificats des porteurs est de 3 ans.

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 porteurs 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. L'ancienne clé de l'AC sert alors à signer les LCR pour les certificats émis sous cette ancienne clé d'AC.



OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 47
---	--	--

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.

## 5.7 Reprise suite à compromission et sinistre

### 5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Notamment chaque entité agissant pour le compte de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, Ce plan est régulièrement testé. L'IGC dispose d'un plan de reprise d'activité en cas de sinistre. La référence au plan anti-sinistre, ses modalités de déclenchement et les personnes responsables de ce plan sont identifiées dans la DPC. Le plan de reprise d'activité en cas de sinistre prend en compte les paramètres suivants :

- priorisation des actions à mener et délais maximums de recouvrement pour la continuité des services ;
- politique de sécurité et de protection des secrets ;
- procédures de secours ;
- tests pratiques, formation et entraînement des personnels ;
- procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) ;
- procédure de reprise en cas de compromission de clés ;

Ces procédures sont établies en cohérence avec la politique de sécurité des systèmes d'information de l'OSC.

En cas de révocation du certificat d'AC, l'AC Racine peut demander un contrôle préalable à la remise en service de l'AC.

### 5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et à la révocation des certificats.

Ce plan de continuité est testé au minimum une fois par an.

Si le matériel de l'AC est endommagé ou hors service alors que les clés privées 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 de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante (voir § 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat de l'AC doit être immédiatement révoqué.

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

- le responsable de l'AC, après enquête sur l'évènement décide de demander à l'AC de niveau supérieur (l'AC Justice) de révoquer le certificat de l'AC ;
- tous les porteurs 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 ;
- les personnes ayant le rôle d'AE, AEC, AED ou OC sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué ;
- une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis ;

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2	<b>Ministère de la Justice et des Libertés</b>	 LIBERTÉ • ÉGALITÉ • FRATERNITÉ RÉPUBLIQUE FRANÇAISE
Date : 15/10/2011	<b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	Page 48

- le responsable de l'AC demande à l'AC de niveau supérieur (l'AC Justice) de générer un nouveau certificat d'AC ;
- les personnes ayant le rôle d'AE, AEC, AED ou OC sont informées de la capacité retrouvée de l'AC de générer des certificats
- les porteurs sont informés de la capacité retrouvée de l'AC de générer des certificats.

#### **5.7.4 Capacités de continuité d'activité suite à 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**

Le transfert d'activité est défini comme la fin d'activité d'une entité agissant pour le compte de l'IGC qui n'induit pas d'incidence sur la validité des certificats antérieurement émis. La reprise de cette activité vers une autre entité est organisée par l'AC.

La cessation d'activité est définie comme la fin d'activité de l'autorité responsable d'une entité agissant pour le compte de l'IGC, qui induit une incidence sur la validité des certificats antérieurement émis, autres que les certificats de l'AC.

#### **5.8.1 Transfert d'activité**

Dans le cas d'un transfert d'activité d'une entité œuvrant pour le compte de l'IGC, l'AC s'engage à :

- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC ;
- informer ses partenaires du transfert d'activité et de sa réalisation.

L'AC précise dans la DPC qu'elle doit prévenir comment se déroule le transfert des obligations (archives et logs à une autre entité), et comment seront traités les certificats encore valides qui seraient amenés à être révoqués.


L'entité œuvrant pour le compte de l'IGC et procédant au transfert de son activité s'engage à :

- avertir l'AC de son intention de transférer son activité avec un préavis d'au moins un mois ;
- remettre ses archives à l'autorité responsable de l'AC ;
- mettre à disposition de l'entité à laquelle son activité est transférée les informations et moyens nécessaires au maintien ou la reprise de l'activité ;
- communiquer au FSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à la cessation d'activité ou au transfert d'activité de la composante ;
- communiquer à l'ANSSI et à la DGME en tant que de besoin, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus ;
- tenir informées l'ANSSI et à la DGME en tant que de besoin de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

#### **5.8.2 Cessation d'activité**

La cessation d'activité peut être totale ou partielle, typiquement, la cessation d'émission de nouveaux certificats sous cette PC.



OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2 Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 <b>Page 49</b>
---	--	---

En cas de cessation partielle d'activité et dans le cadre d'une cessation de l'émission de nouveaux certificats sous cette PC, l'AC :


- 1) en informe à l'avance, via le SP, les porteurs et les utilisateurs de certificats ;
- 2) continue à assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC, le temps que les porteurs soient équipés de nouveaux certificats, et au plus tard jusqu'à la fin de validité du dernier certificat émis.

Dans l'hypothèse d'une cessation partielle d'activité et dans le cadre d'une cessation de gestion totale des certificats émis sous cette PC, l'AC :

- 1) en informe à l'avance, via le SP, les porteurs et les utilisateurs de certificats ;
- 2) cesse d'émettre des CRLs, ce qui a pour conséquence d'empêcher la validation des chemins de certification ;

Dans l'hypothèse d'une cessation totale d'activité de l'AC, c'est-à-dire pour tous les certificats émis sous cette clé d'AC (toutes PC confondues), l'AC :

- 1) s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
  - 2) prend toutes les mesures nécessaires pour détruire la clé privée lui ayant permis d'émettre des certificats (y compris les copies de sauvegarde) ou la rendre inopérante ;
  - 3) demande la révocation de son certificat par l'AC de niveau supérieur (AC Justice) ;
  - 4) informe via le SP les porteurs et les utilisateurs de certificats.
-

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 50
---	--	---

## 6 MESURES DE SECURITE TECHNIQUES

### 6.1 Génération et installation des bi-clés

#### 6.1.1 Génération des bi-clés

##### 6.1.1.1 Clés d'AC

Les bi-clés de signature d'AC sont générées 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). 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 approuvé par le Ministère de la Justice et des Libertés. Les rôles des personnels impliqués dans les cérémonies de clés sont précisés dans la DPC.

Les manipulations de données secrètes en clair (clés privées d'AC, clés privées des porteurs, parts de secrets d'IGC) sont effectuées dans un environnement protégé contre les rayonnements parasites compromettant : matériels protégés, locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques (zonage).

Ces dispositions permettent d'être conforme au niveau (\*\*\*).

##### 6.1.1.2 Transmission de la clé privée à son propriétaire

###### 6.1.1.2.1 Clés porteurs générées par l'AC

Ce paragraphe ne s'applique que lorsque la bi-clé d'un porteur est générée par l'AC.

La génération des clés des porteurs est effectuée dans un environnement sécurisé (voir § 6.4.1). L'OSC génère, pour une bi-clé, les données d'activations associées (voir § 6.4.1).

Les bi-clés des porteurs sont générées dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré, puis la clé privée est transférée de manière sécurisée dans le support de clés destiné au porteur, sans que l'AC n'en garde aucune copie, tandis que la clé publique est incorporée à la demande de certificat afin d'obtenir un certificat.


Les clés privées sont protégées à la fois en intégrité et en confidentialité et protégées contre un usage abusif à l'aide de données d'activation temporaires au sein de leur support de clés de telle sorte qu'elles ne soient utilisables que par le détenteur des données d'activation.

###### 6.1.1.2.2 Clés porteurs générées par le porteur

Ce paragraphe ne s'applique que lorsque la bi-clé d'un porteur est générée par le support de clés.

Dans le cas où le porteur génère sa bi-clé, cette génération est effectuée dans un dispositif répondant aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré. L'AC s'en assure en mettant en œuvre un canal sécurisé (secure channel) entre l'AC et la carte pour récupérer la valeur de la clé publique.

Les clés privées sont protégées à la fois en intégrité et en confidentialité et protégées contre un usage abusif à l'aide de données d'activation courantes au sein de leur support de clés de telle sorte qu'elles ne soient utilisables que par le détenteur des données d'activation.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 51
---	--	---

### **6.1.2 Transmission de la clé privée à son propriétaire**

Lorsque l'AC génère la bi-clé du porteur (cf. chapitre 6.1.1.2), la délivrance du support de clés au porteur s'effectue via l'AE (AEC, AED ou OC) de manière à garantir la confidentialité et l'intégrité des clés privées et à ne les délivrer qu'au seul porteur. Chaque clé privée est protégée dans son support de clés à l'aide d'un code d'activation temporaire. L'envoi du support de clés est effectué de manière séparée dans l'espace et le temps de l'envoi des codes d'activation temporaires. L'AE ne garde aucune donnée permettant de récupérer tout ou partie des clés privées qu'elle a transmise au porteur

La vérification de l'identité du porteur par l'AE (AEC, AED ou OC) est effectuée via un face-à-face physique lors de la remise de la bi-clé générée par l'AC en présence du porteur. Ces dispositions permettent d'être conforme au niveau (\*\*).

### **6.1.3 Transmission de la clé publique à l'AC**

Lorsque l'AC génère la bi-clé d'un porteur (cf. chapitre 6.1.1.2), la clé publique est protégée en intégrité et son origine authentifiée lorsqu'elle est extraite du module cryptographique.

Lorsque la bi-clé d'un porteur est générée par le support de clés, la clé publique est protégée en intégrité et son origine authentifiée lorsqu'elle est extraite du support de clés : un canal sécurisé (secure channel) est mis en œuvre entre l'AC et la carte.

### **6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats**

Le certificat de l'IGC Personnes est publié à l'URL : <http://www.justice.gouv.fr/igc/ants/>

### **6.1.5 Tailles des clés**

Les clés d'AC et de porteurs respectent les exigences de caractéristiques (longueurs, algorithmes, etc.) du document [RGS\_A\_14].

#### **6.1.5.1 Certificat AC**

L'algorithme RSA avec la fonction de hachage SHA-2 est utilisé. La taille des bi-clés de l'AC Personnes est de 2048 bits.

#### **6.1.5.2 Certificat Porteur**

L'algorithme RSA avec la fonction de hachage SHA-2 est utilisé pour les certificats de porteur. La taille des bi-clés est de 2048 bits.


### **6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité**

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles qualifiées au niveau renforcé par l'ANSSI et respectent donc les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

### **6.1.7 Objectifs d'usage de la clé**

Certificat d'AC

L'utilisation de la clé privée de l'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR. (Voir §1.4.1.1).

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 52
---	--	---

#### Certificat d'authentification

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification (voir § 1.4.1.2 et § 4.5). L'utilisation du champ "keyUsage" dans le certificat porteur est : « digitalSignature ».

#### Certificat de signature

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature (cf. § 1.4.1.2 et § 4.5). L'utilisation du champ "keyUsage" dans le certificat porteur est « nonRepudiation » tel qu'appelé dans le RFC 5280 de l'IETF ou « content Commitment » tel qu'appelé dans la recommandation ITU-T X.509.

## 6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

### 6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

#### 6.2.1.1 Modules cryptographiques de l'AC

Les ressources cryptographiques de l'AC sont qualifiées au niveau renforcé par l'ANSSI.

La ressource cryptographique matérielle de l'AC utilise des générateurs d'aléas qui sont conformes à l'état de l'art, et aux standards en vigueur. Les algorithmes utilisés pour générer l'aléa de départ sont conformes aux standards en vigueur.

#### 6.2.1.2 Dispositifs d'authentification et de signature des porteurs

L'AC fournit aux utilisateurs le dispositif d'authentification et de signature (carte d'agent). Ce dispositif est qualifié au niveau renforcé par l'ANSSI et respecte les exigences du § 12.

Le renouvellement des bi-clés se fait par la mise en place d'un « secure messaging » entre la carte et l'AC permettant de s'assurer que le porteur utilise bien le dispositif fourni originellement.

### 6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où 3 exploitants parmi 5 doivent s'authentifier). Cette disposition permet d'être conforme au niveau (\*\*).

### 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 Copie de secours de la clé privée

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de disponibilité. Les copies de secours 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.

### 6.2.5 Archivage de la clé privée

Les clés privées de l'AC Personnes et des porteurs ne sont pas archivées.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 53
---	--	---

### **6.2.6 Transfert de la clé privée vers / depuis le module cryptographique**

Les clés d'AC sont générées et stockées dans des modules de sécurité matériels (HSM). Lors d'un transfert, la clé privée est chiffrée. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'un HSM et l'action des personnes identifiées dans les rôles de confiance.

### **6.2.7 Stockage de la clé privée dans un module cryptographique**

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

### **6.2.8 Méthode d'activation de la clé privée**

#### **6.2.8.1 Clés privées d'AC**

L'activation des clés privées d'AC dans les modules cryptographiques est contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire intervenir au moins trois personnes dans des rôles de confiance. Cette disposition permet d'être conforme au niveau (\*\*).

#### **6.2.8.2 Clés privées des porteurs**

La méthode d'activation d'une clé privée du porteur est contrôlée via un code confidentiel (PIN) (voir § 6.4) et répond aux exigences définies dans le § 12. Les codes d'activation temporaires attribués par l'AC doivent être changés par le porteur lors du face à face avant de pouvoir repartir avec sa carte.

### **6.2.9 Méthode de désactivation de la clé privée**

#### **6.2.9.1 Clés privées d'AC**

La désactivation des clés privées de l'AC dans le module cryptographique est automatique dès qu'il y a arrêt ou déconnexion du module. Les ressources cryptographiques sont stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

#### **6.2.9.2 Clés privées des porteurs**

Les conditions de désactivation de la clé privée d'un porteur répondent aux exigences du § 12. Toute mise hors tension de la carte désactive les clés privées. La désactivation peut aussi s'obtenir au moyen de commandes logicielles spécifiques.

### **6.2.10 Méthode de destruction des clés privées**

#### **6.2.10.1 Clés privées d'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, et l'effacement de cette clé sur la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

#### **6.2.10.2 Clés privées des porteurs**


En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

### **6.2.11 Niveau de qualification du module cryptographique et des dispositifs**

Les ressources cryptographiques des AC de l'IGC Justice et des dispositifs des porteurs sont qualifiées au niveau renforcé par l'ANSSI conformément aux exigences du § 11.

#### **6.2.11.1 Niveau de qualification du module cryptographique et des dispositifs d'authentification**

Les dispositifs d'authentification des porteurs sont évalués conformément aux exigences du § 12.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 54
---	--	--

Les dispositifs des porteurs sont choisis par les produits qualifiés des constructeurs Gemalto, Morpho et Oberthur.

### **6.2.11.2 Niveau de qualification du module cryptographique et des dispositifs de création de signature**

Les dispositifs de création de signature des porteurs sont évalués conformément aux exigences du § 12.

Les dispositifs des porteurs sont choisis par les produits qualifiés des constructeurs Gemalto, Morpho et Oberthur.

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

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

Les clés publiques sont archivées par archivage des certificats (Voir § 5.5.2).

### **6.3.2 Durées de vie des bi-clés et des certificats**

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.

L'AC Personnes ne peut pas émettre des certificats porteur dont la durée de vie est supérieure à celle de son certificat, cf. § 5.6. Les bi-clés et les certificats des porteurs couverts par la présente PC ont une durée de vie de 3 ans. Les certificats d'AC ont une durée de vie de 6 ans.

## **6.4 Données d'activation**

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

#### **6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC**

Les données d'activation des clés privées de l'AC Personnes sont générées durant les cérémonies de clés (Voir § 5.2.1). Les données d'activation sont générées automatiquement selon un schéma de type m parmi n. Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après leur génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

#### **6.4.1.2 Génération et installation des données d'activation correspondant à une clé privée du porteur**

L'OCS transmet par courrier à chaque porteur, protégé en intégrité et en confidentialité, un code d'activation temporaire de la carte. Ce code est à usage unique. L'envoi du code d'activation de la carte est séparé dans le temps et dans l'espace de la remise de la carte.


Chaque donnée d'activation d'une clé privée, appelée « code PIN », est choisie par le porteur lors de l'activation de sa carte.

- une donnée d'activation de la fonction authentification (code PIN) : donnée d'activation utilisée par le porteur pour s'authentifier. C'est ce code qui est utilisé pour protéger et utiliser la clé privée d'authentification contenue dans le support de clés.
- une donnée d'activation de la fonction de signature (code PIN) : donnée d'activation utilisée par le porteur pour signer électroniquement un ou plusieurs documents. C'est ce code qui est utilisé pour protéger et utiliser la clé privée de signature contenue dans le support de clés.

L'OSC transmet au porteur, protégée en intégrité et en confidentialité, les données d'activation temporaires. L'envoi des données d'activation est séparé dans le temps et dans l'espace de la remise du support matériel protégé à l'aide des données d'activation correspondantes.

L'OSC conserve le code d'activation temporaire jusqu'au moment où le porteur a pris possession de son support, après quoi les données d'activation temporaires sont détruites.

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

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 55
---	--	--

#### 6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'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 secret sont responsables de la gestion et de la protection des parts de secrets dont ils sont porteurs. Un porteur de secret ne peut détenir plus d'une donnée d'activation d'une même clé d'AC à un même instant.

#### 6.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Le code d'activation temporaire est communiqué au porteur au moyen d'un courrier postal envoyé à son attention en courrier suivi. Les codes PIN créés par le porteur doivent être mémorisés par le porteur.

#### 6.4.3 Autres aspects liés aux données d'activation

Sans objet.

### 6.5 Mesures de sécurité des systèmes informatiques

#### 6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC. Il répond aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlés par rôle et nom d'utilisateur) ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- protection du réseau contre toute intrusion d'une personne non autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (voir § 1.4.1.1) fait l'objet de mesures particulières, découlant de l'analyse de risque.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.


#### 6.5.2 Niveau de qualification des systèmes informatiques

Les composants d'ICP 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" et sont qualifiés par l'ANSSI.

### 6.6 Mesures de sécurité liées au développement des systèmes

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

- les matériels et les logiciels sont achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2	<b>Ministère de la Justice et des Libertés</b>	 LIBERTÉ • ÉGALITÉ • FRATERNITÉ RÉPUBLIQUE FRANÇAISE
Date : 15/10/2011	<b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	Page 56

- les matériels et logiciels sont mis au point dans un environnement contrôlé, et le processus de mise au point est défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;
- tous les matériels et logiciels sont 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 de l'AC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités de l'AC ;
- les applications nécessaires à l'exécution des activités de l'AC sont acquises auprès de sources autorisées.
- 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 sont installés par des personnels de confiance et formés selon les procédures en vigueur.

### **6.6.1 Mesures liées à la 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'AC. Lors de son premier chargement, il est vérifié que le logiciel de l'AC 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.

Toute évolution significative d'un système d'une composante de l'AC Personnes est signalée au responsable de l'AC pour validation.

### **6.6.2 Niveau d'évaluation et sécurité du cycle de vie des systèmes**

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 Mesures de sécurité réseau**

Une analyse de risque est menée par le responsable de l'AC afin d'établir les objectifs et les règles de sécurité pour la protection des réseaux qui permettent de mettre en œuvre les services de l'AC. Les solutions de sécurité pour ces réseaux sont déclinées en fonction de ses objectifs et règles de sécurité afin de garantir que l'accès aux réseaux n'est possible qu'aux seules entités autorisées. La DPC précise les mesures mises en œuvre pour la protection des réseaux.

Une partie des composantes de l'AC (AE) est accessible en ligne par des postes informatiques sous contrôle ou sous le contrôle du MJL. Une partie des composantes de l'AC (SP) est connectée à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service conforme aux exigences de disponibilité.


Les autres composantes 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 détecteurs d'intrusion, de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont fermés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système est hébergé refuse tout service, hormis ceux qui sont nécessaires au système lui-même, 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 au sens du RFC 3161 de l'IETF utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés au moyen d'un serveur NTP (Network Time Protocol). Le temps fourni par ce serveur de temps est utilisé en particulier pour établir:


- la date du début de validité d'un certificat porteur ;
- la date du début de l'instant de révocation d'un certificat porteur ;



OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2 Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 Page 57
---	--	--

- les dates utilisées dans les journaux.

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.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2	<b>Ministère de la Justice et des Libertés</b>	 LIBERTÉ • ÉGALITÉ • FRATERNITÉ REPUBLIQUE FRANÇAISE
Date : 15/10/2011	<b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	Page 58

## 7 PROFILS DES CERTIFICATS ET DES LCR

### 7.1 Profils des Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3. Les champs des certificats porteurs et AC sont définis par le RFC 5280.

#### 7.1.1 Extensions de Certificats

##### 7.1.1.1 Certificat AC

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

Champ de base	Valeur
Version	2 (=version 3)
Serial number	
Issuer DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification Justice
Subject DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification personnes
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Taille des clés	2048 bits
Durée de validité	6 ans


Le certificat d'AC contient les extensions suivantes :

- Authority Key Identifier (extension non critique) ;
- Basic Constraints (extension critique) ; le booléen cA doit être présent
- Certificate Policies (extension non critique) ; contient l'identifiant de la politique de certification utilisée par l'AC Justice pour émettre ce certificat d'AC.
- CRL Distribution Points (extension non critique) ;
- Key usage (extension critique) ; indique le point de distribution de la LAR pour ce certificat.
- Subject Key Identifier (extension non critique).

##### 7.1.1.2 Certificats de porteur

Les informations principales contenues dans un certificat du porteur sont :

Champ de base	Valeur
Version	2 (=version 3)
Serial number	
Issuer DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification personnes
Subject DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Prénom<espace>Nom<espace>Identifiant unique
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Taille des clés	2048 bits
Durée de validité	3 ans

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 59
---	--	---

Le certificat porteur contient les extensions suivantes :

- Authority Key Identifier (extension non critique) ;
- Basic Constraints (extension critique) ; le booléen cA ne doit pas être présent.
- Certificate Policies (extension non critique) ; contient l'identifiant de la politique de certification. Selon le type de certificat, le champ contient un OID différent. Il contient l'OID 1.2.250.1.120.2.3.1.2 s'il s'agit d'un certificat d'authentification ou bien l'OID 1.2.250.1.120.2.2.1.2 s'il s'agit d'un certificat de signature.
- CRL Distribution Points (extension non critique) ; indique le point de distribution de la LCR pour ce certificat.
- Key usage (extension critique) ; selon le type de certificat, le bit 0 prend la valeur 1 s'il s'agit d'un certificat d'authentification ou bien le bit 1 prend la valeur 1 s'il s'agit d'un certificat de signature, tandis que tous les autres bits prennent la valeur 0.
- Subject Key Identifier (extension non critique).
- Pour la fonction de signature, le certificat contient une extension QcStatements qui contient identifiants d'objet (OID) l'un indiquant qu'il s'agit d'un certificat qualifié et l'autre indiquant que la clé privée réside sur un dispositif sécurisé de création de signature (SSCD)

### 7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est sha256WithRSAEncryption {iso(1) member-body((2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}.

### 7.1.3 Formes de noms

Les formes de noms respectent les exigences du § 3.1.1 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

Certificat d'authentification

Les certificats porteurs émis par l'AC Personnes contiennent l'OID de la PC qui est : 1.2.250.1.120.2.3.1.2.

Certificat de signature


Les certificats porteurs émis par l'AC Personnes contiennent l'OID de la PC qui est : 1.2.250.1.120.2.2.1.2.

## 7.2 Profil des LCR

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

Les caractéristiques des LCRs sont :

<b>Caractéristiques d'une LCR :</b>	Durée de validité : 7 jours Périodicité de mise à jour : 24 heures Version de la CRL (v1 ou v2) : v2 Extensions : Numéro de la CRL et AKI URL http de publication : adresse variable indiquée dans chaque certificat de porteur.
-------------------------------------	--

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 60
---	--	---

## 8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Ainsi que le précise l'article 8 de l'[Ordonnance], lorsqu'une autorité administrative (AA) met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le [RGS], elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes.

Dans le cadre de la présente PC, le niveau de sécurité choisi par le MJL est le niveau \*\*\*.

Ainsi que le précise l'article 8 de l'[Ordonnance], les actes des autorités administratives qui font l'objet d'une signature électronique doivent être signés au moyen d'un procédé, conforme aux règles du [RGS] mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte.

Dans le cadre de la présente PC, des certificats à usage de signature sont délivrés pour signer et vérifier des actes. Le niveau de sécurité choisi par le MJL pour ces certificats est le niveau \*\*\*.

Le [RGS] liste les règles que les prestataires de service de certification électronique (PSCE) délivrant des certificats électroniques de type signature électronique ou authentification doivent respecter. Les documents de référence du RGS, pour ce qui concerne les certificats objets de cette PC, sont au nombre de quatre :

- RGS\_A\_7 : RGS\_PC-Type\_Authentification\_V2\_3.pdf
- RGS\_A\_8 : RGS\_PC-Type\_Signature\_V2\_3.pdf
- RGS\_A\_13 : RGS\_Variables\_de\_temps\_V2\_3.pdf
- RGS\_A\_14 : RGS\_Profils\_Certificat\_LCR\_OCSP\_V2-3.pdf

Le RGS 1.0 a été approuvé par l'arrêté du Premier Ministre du 6 mai 2010 [Arrêté060510].

L'article 23 du décret du décret n° 2010-112 du 2 février 2010 [DécretRGS] précise que les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs agents au plus tard dans les trois ans à compter de la publication de l'arrêté du 6 mai 2010.

Le présent chapitre ne traite pas des audits effectués par les organismes qui procèdent à la qualification des prestataires de services de confiance dans le but d'obtenir la validation des certificats électroniques des agents du MJL. La compétence de ces organismes est appréciée par l'ANSSI à partir d'un audit des moyens, des ressources et de l'expérience de l'organisme, cf. [DécretRGS].

Le présent chapitre traite uniquement des audits et des évaluations de la responsabilité de l'AC afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

### 8.1 Fréquences et / ou circonstances des évaluations

Le responsable de l'exploitation des composantes de l'AC demande l'approbation de l'AA pour toute modification jugée comme étant une perte de la conformité avec la présente PC et la DPC qu'il met en œuvre.


L'AA se doit de prévenir les IGC avec lesquelles des accords sont conclus dans la mesure où ces modifications peuvent affecter ces accords ou le niveau de sécurité offert par l'IGC.

Le responsable de l'exploitation des composantes d'IGC demande l'approbation du responsable de l'AC Personnes pour le Ministère de la Justice et des Libertés pour toute modification jugée comme étant une perte de la conformité avec la présente PC et la DPC qu'il met en œuvre.

L'AC Personnes procède à un contrôle de conformité de l'ensemble de son IGC tous les ans.

### 8.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante est effectué par une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 61
---	--	--

### 8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante contrôlée, quelle que soit cette composante, elle est dûment autorisée à pratiquer les contrôles visés.

### 8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la présente PC et dans la DPC associée, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

Les éléments relatifs au contrôle de conformité sont décrits dans le référentiel d'audit de l'IGC/A.


### 8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend un avis au responsable d'exploitation et à l'AC Personnes parmi les suivants : "réussite", "échec", "à confirmer". Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations au responsable d'exploitation qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par le responsable d'exploitation et doit respecter ses politiques de sécurité internes.
- En cas de résultat "A confirmer", le responsable d'exploitation remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, le responsable d'exploitation confirme à la composante contrôlée la conformité aux exigences de la présente PC et la DPC.

### 8.6 Communication des résultats

Les résultats des contrôles de conformité sont communiqués à la composante contrôlée ainsi qu'à l'AC Personnes.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 62
---	--	--

## 9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

### 9.1 Tarifs

Sans objet.

### 9.2 Responsabilité financière

Le responsable de l'ACR pour le Ministère de la Justice et des Libertés s'engage à respecter la présente PC. Toute condition supplémentaire non portée dans ce document ne pourra être valablement considérée comme une obligation de l'ACR du Ministère de la Justice et des Libertés.

### 9.3 Confidentialité des données professionnelles

#### 9.3.1 Périmètre des informations confidentielles

Les informations suivantes (liste non exhaustive) sont considérées comme confidentielles :

- les clés privées des certificats d'AC ;
- les données d'activation associées à une bi-clé cryptographique ;
- les journaux d'événements des composantes d'IGC ;
- les rapports d'audits ;
- les informations techniques relatives à la sécurité des fonctionnements des modules cryptographiques ;
- les informations techniques relatives à la sécurité des fonctionnements de certaines composantes d'IGC ;
- la DPC et les procédures associées ;
- les causes de révocation.

#### 9.3.2 Informations hors du périmètre des informations confidentielles

Les informations concernant l'IGC publiées par le SP sont considérées comme non confidentielles, elles sont communiquées selon le principe du besoin d'en connaître.

#### 9.3.3 Responsabilités en termes de protection des informations confidentielles

L'IGC respecte la législation et la réglementation en vigueur sur le territoire français.

### 9.4 Protection des données personnelles

#### 9.4.1 Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel qui est effectuée par l'AC du Ministère de la Justice et des Libertés sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi informatique et libertés [CNIL].


#### 9.4.2 Informations à caractère personnel

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

- données d'identification du porteur (hors celles figurant dans le certificat) ;
- demande (renseignée) de certificat ;
- demande (renseignée) de révocation ;
- motif de la révocation.

#### 9.4.3 Informations à caractère non personnel

Sans objet.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2	<b>Ministère de la Justice et des Libertés</b>	 République Française
Date : 15/10/2011	<b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	Page 63

#### **9.4.4 Responsabilité en termes de protection des données personnelles**

L'AEC, l'AED, le CPS 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 [CNIL] et la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [LCEN] s'applique au contenu de tous les documents collectés, détenus ou transmis par l'AC 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, l'AEC ou l'AED pour l'émission du certificat et la gestion de son cycle de vie. Ce droit peut s'exercer auprès du Ministère de la Justice et des Libertés.

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 Notification et consentement d'utilisation des données personnelles**

Aucune des données à caractère personnel fournies par un porteur ne peut être utilisée par l'AC, pour une autre utilisation 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 UC.

Les composantes d'IGC et les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'IGC. Ce droit peut s'exercer auprès de l'AC Personnes. Les opérations demandées par l'AC ne doivent pas porter atteinte à l'intégrité de l'ensemble des données propres aux opérations mise en œuvre pour la gestion de son certificat.

#### **9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives**

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


#### **9.4.7 Autres circonstances de divulgation d'informations personnelles**

Les informations relatives à une personne définies comme confidentielles au § 9.4.2 ne peuvent être divulguées qu'à leur propriétaire ou à un tiers habilité au niveau adéquat.

L'AC s'oblige à obtenir l'accord du Ministère de la Justice et des Libertés pour 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 et industrielle**

La législation et de la réglementation en vigueur sur le territoire français est applicable.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 64
---	--	---

## 9.6 Interprétations contractuelles et garanties

L'AC a pour obligation de :

- respecter et appliquer la PC et la DPC,
- se soumettre aux contrôles de conformité effectués, d'une part par l'équipe d'audit mandatée par l'AC et, d'autre part par l'organisme de qualification,
- respecter les clauses qui la lient aux porteurs et aux utilisateurs de certificats,
- documenter les procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elle s'engage dans des conditions garantissant qualité et sécurité.

### 9.6.1 Autorités de Certification

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.

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:

- de protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;
- de 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 ;
- de respecter et appliquer les dispositions de la partie de la DPC qui les concerne ;
- de documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- de 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 ;
- de faire certifier la clé publique, correspondante à sa clé privée, par l'AC Justice ;
- d'apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs ;
- de communiquer toutes les informations utiles, d'une part à l'équipe d'audit mandatée par l'AC et, d'autre part à l'organisme de qualification.


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

### 9.6.2 Service d'enregistrement

Les obligations découlent des obligations pertinentes de l'AC du chapitre § 9.6.1 en se restreignant aux services qu'elle met en œuvre dans le cadre de la présente PC. Les obligations communes aux composantes de l'AE sont:

- de respecter et appliquer les dispositions de la partie de la DPC qui les concerne ;
- de documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- de 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 ;
- d'assurer l'information des agents auxquelles elle délègue, concernant leurs rôles et responsabilités, et le traitement des informations à caractère personnel ou confidentielles, conformément à la présente PC ;



OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 65
---	--	--

- d'apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs ;
- de communiquer toutes les informations utiles, d'une part à l'équipe d'audit mandatée par l'AC et, d'autre part à l'organisme de qualification.

### 9.6.3 Porteurs de certificats

Le porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat
- informer l'AC de toute modification concernant les informations contenues dans son certificat
- s'engager à ne pas prêter sa carte et à la conserver constamment sous sa garde ;
- s'engager à prendre toutes les précautions pour les données d'activation qu'il détient ne soient pas divulguées ;
- s'engager à rendre sa carte à sa hiérarchie en cas de cessation d'activité ou à remettre sa carte à la demande de sa hiérarchie ;
- s'engager à ne s'authentifier au moyen de sa carte que sur les systèmes d'information en relation avec son activité professionnelle au sein du Ministère de la Justice et des Libertés ;
- s'engager à ne signer les décisions judiciaires que sur des applications diffusées par le Ministère de la Justice et des Libertés, sur le réseau privé virtuel justice et sur le poste de travail fourni par le MJL et dans l'enceinte des locaux du Ministère ;
- en cas de perte ou vol de leur carte ou bien de divulgation d'un PIN, et dès la découverte du vol ou de la perte, s'engager à en faire la déclaration auprès du service qui lui a remis sa carte ou sur le site prévu à cet effet (<https://www.asscap.justice.ants.gouv.fr>) ;
- s'assurer que les données dans son dossier administratif personnel sont à jour ;
- avertir son AEC de toute modification concernant les informations contenues dans son certificat.

La relation entre le porteur et l'AC est formalisée dans les Conditions Générales d'Utilisation.

### 9.6.4 Utilisateurs de certificats

Les utilisateurs de certificats doivent :


- vérifier et respecter l'usage (authentification ou signature électronique) pour lequel un certificat a été émis ;
- pour chaque certificat du chemin de certification, depuis le certificat du porteur jusqu'à un certificat de l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- utiliser le certificat auto-signé de l'AC Racine qui est disponible sur le site du ministère à l'adresse <http://www.justice.gouv.fr/igc/ants>.
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC publiée sur le site du ministère à l'adresse Intranet <http://www.justice.gouv.fr/igc/ants>.

### 9.6.5 Autres participants

La DPC précisera les exigences si besoin est.

## 9.7 Limite de garantie

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

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 66
---	--	---

- 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 UC dans leurs accords contractuels (s'il en est).

## 9.8 Limites de responsabilité

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.

Seule la responsabilité de l'ETAT 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 d'AC qu'elle a émis dans des conditions et à des fins autres que celles prévues dans la présente politique de certification ainsi 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

Sans Objet

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

### 9.10.1 Durée de validité

La présente PC devient effective une fois approuvée par le Ministère de la Justice et des Libertés. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

### 9.10.2 Fin anticipée de validité


La publication d'une nouvelle version de la présente PC peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer la PC qu'elle met en œuvre.

En fonction de la nature et de l'importance des évolutions apportées à la PC, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié aux modifications des exigences de sécurité contenu dans la présente PC.

### 9.10.3 Effets de la fin de validité et clauses restant applicables

Les clauses restant applicables au-delà de la fin d'utilisation de la PC, sont celles concernant l'archivage des données. Toutes les autres obligations deviennent caduques et sont remplacées par celles décrites dans la ou les PC encore en vigueur.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 67
---	--	---

## 9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC s'engage :

- au plus tard un mois avant le début de l'opération, à faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'ACR et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, à en informer l'organisme de qualification.

## 9.12 Amendements à la PC

### 9.12.1 Procédures d'amendements

L'AC s'engage à contrôler que tout projet de modification de sa PC reste conforme aux exigences de la présente PC Type et des éventuels documents complémentaires du [RGS]. L'AC pourra réviser sa PC et/ou sa DPC chaque fois qu'une évolution remarquable de l'état de l'art le justifie.

### 9.12.2 Mécanisme et période d'information sur les amendements

Le Ministère de la Justice et des Libertés donne un préavis de deux mois au moins aux composantes de l'AC de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification.

### 9.12.3 Circonstances selon lesquelles un OID doit être changé

L'OID de la PC est inscrit dans les certificats émis. Toute évolution d'une PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduira par un changement de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

## 9.13 Dispositions concernant la résolution de conflits

Les conflits entre des personnes appartenant au MJL sont traités au niveau du secrétariat général du ministère de la Justice et des Libertés. A défaut, ils sont du ressort du Tribunal Administratif.

## 9.14 Juridictions compétentes


Le Tribunal Administratif compétent est soit celui du plaignant soit celui du défendeur.

## 9.15 Conformité aux législations et réglementations

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

L'environnement législatif pour la mise en œuvre de l'AC Personnes est notamment constitué des textes de lois et règlements suivants :

- la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques [Directive] ;
- les articles 1316 et suivants du Code Civil relatif à la signature électronique [CC1316] ;
- le décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique [SIG] ;
- l'article 801-1 du CPP [CPP801] ;
- la loi n°2004-575 du 21 juin 2004 modifiée, pour la confiance dans l'économie numérique, et en particulier l'article 33 [LCEN] ;
- la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés [CNIL] ;

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 68
---	--	---

- l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [Ordonnance] ;
- le décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique [DEC2001-272] ;
- l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation [Arrêté260704] ;
- le décret n°2010-112 du 2 février 2010 pris pour application des articles 9 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [DécretRGS] ;
- l'arrêté du 10 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques [Arrêté060510].

## 9.16 Dispositions diverses

### 9.16.1 Accord global

Les éventuels accords passés avec les partenaires doivent être validés par le Ministère de la Justice et des Libertés.

### 9.16.2 Transfert d'activités

Voir § 5.8.

### 9.16.3 Conséquences d'une clause non valide

Les conséquences, le cas échéant, seront traitées en fonction de la législation en vigueur.

### 9.16.4 Application et renonciation

La présente PC ne formule pas d'exigence spécifique sur le sujet.

### 9.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

## 9.17 Autres dispositions

Le cas échéant, la DPC en fournira les détails.


## 10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

### 10.1 Réglementation

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[Directive]	Directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques
[Ordonnance]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (Journal Officiel du 9 décembre 2005). Disponible en ligne : <a href="http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&amp;dateTexte=vig">http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&amp;dateTexte=vig</a>
[CPP801]	Article 801-1 du code de procédure pénale
[CC1316]	Articles 1316 et suivants du Code Civil relatif à la signature électronique [CC1316]
[DécretRGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'[Ordonnance]. Disponible en ligne : <a href="http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&amp;dateTexte=vig">http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&amp;dateTexte=vig</a>
[Décret2001-272]	Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. Disponible en ligne : <a href="http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&amp;dateTexte=vig">http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&amp;dateTexte=vig</a>
[Arrêté260704]	Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation. Disponible en ligne : <a href="http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678&amp;dateTexte=vig">http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678&amp;dateTexte=vig</a>
[Arrêté060510]	Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. Disponible en ligne : <a href="http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022220429&amp;fastPos=1&amp;fastReqId=1704766824&amp;categorieLien=id&amp;oldAction=rechTexte">http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022220429&amp;fastPos=1&amp;fastReqId=1704766824&amp;categorieLien=id&amp;oldAction=rechTexte</a>
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[SIG]	Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

### 10.2 Documents techniques

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS_A2]	RGS – Fonction de sécurité « Authentification » – Version 2.3
[RGS_A3]	RGS – Fonction de sécurité « Signature électronique » – Version 2.3
[RGS_A7]	RGS – Politique de Certification Type Authentification – Version 2.3
[RGS_A8]	RGS – Politique de Certification Type Signature – Version 2.3
[RGS_A_13]	RGS – Politiques de Certification Types - Variables de Temps - Version 2.3

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  <b>Page 70</b>
---	--	---

[RGS_A_14]	RGS – Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3
[RGS_B_1]	RGS – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 1.20
[X.509]	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. 6 th Edition. Version de novembre 2008. Disponible à l'adresse : <a href="http://www.x500standard.com/index.php?n=lq.LatestAvail">http://www.x500standard.com/index.php?n=lq.LatestAvail</a> .
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003. Disponible à l'adresse : <a href="http://www.ietf.org/rfc/rfc3647.txt">http://www.ietf.org/rfc/rfc3647.txt</a>

## 11 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC


### 11.1 Exigences sur les objectifs de sécurité

Le module cryptographique (HSM), utilisé par l'AC pour générer et mettre en œuvre ses clés d'authentification (pour la génération des certificats électroniques, des LCR) et ses clés de signature (pour la génération des certificats électroniques, des LCR) répond aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie,
- être capable d'identifier et d'authentifier ses utilisateurs,
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné,
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur,
- permettre de signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées,
- créer des enregistrements d'audit pour chaque modification concernant la sécurité,
- dans le cadre des fonctions de sauvegarde et de restauration des clés privées de l'AC, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

### 11.2 Exigences sur la qualification

Le module cryptographique utilisé par l'AC fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 11.1 ci-dessus.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2  Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 République Française  Page 71
---	--	---

## 12 ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE SIGNATURE

### 12.1 Exigences sur les objectifs de sécurité

#### 12.1.1 Authentification

Le dispositif d'authentification, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée répond aux exigences de sécurité suivantes :


- lorsque la bi-clé de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée (dans la mesure où la fonction de hachage utilisée à l'extérieur du dispositif soit exempte de collisions et que le protocole d'authentification soit exempt de faiblesses et de possibilités de rejeu) ;
- assurer la fonction d'authentification pour le porteur légitime uniquement en utilisant un code d'activation personnel et spécifique pour mettre en œuvre la fonction.

#### 12.1.2 Signature

Le dispositif de création de signature, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, répond aux exigences de sécurité suivantes :

- lorsque la bi-clé de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée (dans la mesure où la fonction de hachage utilisée à l'extérieur du dispositif soit exempte de collisions et que le format de signature électronique soit exempt de faiblesses et de possibilités d'anti-datation) ;
- assurer la fonction de signature électronique pour le porteur légitime uniquement en utilisant un code d'activation personnel et spécifique pour mettre en œuvre la fonction.

Les dispositifs d'authentification des porteurs sont des cartes à puce respectant le socle commun IAS (Identification, Authentification, Signature) et permettent de répondre à l'ensemble de ces exigences de sécurité.

OID : 1.2.250.1.120.2.2.1.2 / 1.2.250.1.120.2.3.1.2 Date : 15/10/2011	<b>Ministère de la Justice et des Libertés</b>  <b>POLITIQUE DE CERTIFICATION – AC Personnes</b>	 Page 72
---	--	--

## 12.2 Exigences sur la qualification

### 12.2.1 Authentification

Le dispositif d'authentification utilisé par le porteur fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1.1 ci-dessus.

### 12.2.2 Signature

Le dispositif de création de signature utilisé par le porteur fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1.2 ci-dessus.

---