

POLITIQUE DE CERTIFICATION – AC RACINE JUSTICE

OID du document :	1.2.250.1.120.2.1.1.1	Nombre total de pages :	42
Statut du document :	<input type="checkbox"/> Projet	<input checked="" type="checkbox"/> Version finale	

Rédaction

Nom	Fonction
Alain GALLET	Responsable du programme Sécurité – ANTS
Philippe BOURDIN	AMOA Sécurité

Validation

Nom	Fonction	Signature
Luc FERRAND	Directeur de projet nouvelles technologies – MJL	
David CROCHEMORE	Fonctionnaire de sécurité des systèmes d'information – MJL	
Cédric SIBEN	Directeur adjoint – ANTS	

Approbation

Nom	Fonction	Signature
André GARIAZZO	Haut fonctionnaire défense et sécurité – MJL	

REVISION DOCUMENTAIRE

Historique du document

Date	Version	Commentaires
22/03/10	0.1	Création du document
06/04/10	0.3	Première mise à jour complète
07/05/10	0.5	Version de travail diffusée au MJL
20/05/10	0.6	Version de travail diffusée au MJL pour finalisation
01/06/10	1.0	Version de référence
23/06/10	1.1	Prise en comptes contributions MJL/SG
15/09/11	1.2	Mise à jour (version pour signature)

SOMMAIRE

1	INTRODUCTION	7
1.1	Généralités	7
1.2	Nom du Document et Identification	7
1.3	Les composantes de l'IGC	8
1.3.1	Ministère de la Justice et des Libertés (ACR – SP)	8
1.3.1.1	Autorité de Certification Racine (ACR)	8
1.3.1.2	Service de Publication (SP)	9
1.3.2	Agence Nationale des Titres Sécurisés (OSC)	9
1.3.3	Porteur	9
1.3.4	Autres participants	9
1.3.4.1	Utilisateur de Certificat (UC)	9
1.4	Utilisation des certificats AC	9
1.4.1	Bi-clés et certificats d'AC	9
1.4.2	Utilisation interdite des certificats	10
1.5	Application de la politique	10
1.5.1	Organisme responsable de la présente politique	10
1.5.2	Point de contact	10
1.5.3	Personne déterminant la conformité de l'implémentation de la présente PC/DPC	10
1.5.4	Procédure d'approbation du présent document	10
1.6	Définitions et Acronymes	11
1.6.1	Acronyme	11
1.6.2	Définitions	11
2	ANNUAIRES ET SERVICES DE PUBLICATION	14
2.1	Service de publication	14
2.2	Informations publiées	14
2.3	Heure et fréquence de publication	14
2.4	Contrôle d'accès au service de publication	14
3	IDENTIFICATION ET AUTHENTIFICATION	15
3.1	Nommage	15
3.1.1	Types de noms	15
3.1.1.1	Certificat d'ACR	15
3.1.1.2	Certificat d'AC « en ligne »	15
3.1.2	Utilisation de noms explicites	15
3.1.3	Anonymat ou utilisation de pseudonyme	15
3.1.4	Règles d'interprétations des différentes formes de noms	15
3.1.5	Unicité des noms	15
3.1.6	Reconnaissance, vérification, et rôle des noms de marques déposées	15
3.2	Vérification initiale d'identité	16
3.2.1	Preuve de possession de la clé privée	16

3.2.2	Vérification de l'identité des organisations.....	16
3.2.3	Vérification de l'identité des personnes	16
3.2.4	Informations non vérifiées.....	16
3.2.5	Validation du représentant légal	16
3.2.6	Critères de reconnaissance	16
3.3	Vérifications aux fins de renouvellement de clés	16
3.3.1	Vérifications aux fins de renouvellement de clés en situation normale	16
3.3.2	Vérifications aux fins de renouvellement de clés après révocation du certificat	16
3.4	Vérifications aux fins de révocation.....	16
4	EXIGENCES OPERATIONNELLES	17
4.1	Types de certificat	17
4.1.1	Origine de la demande de certificat	17
4.1.2	Procédure d'enregistrement et responsabilités	17
4.2	Traitement d'une demande de certificat	17
4.2.1	Identification et authentification.....	17
4.2.2	Approbation ou rejet d'une demande de certificat	17
4.2.3	Durée de traitement d'une demande de certificat	17
4.3	Délivrance d'un certificat.....	17
4.3.1	Actions effectuées par l'AC pendant l'émission d'un certificat d'AC	17
4.3.2	Notification de l'émission d'un certificat	17
4.4	Acceptation d'un certificat	17
4.4.1	Procédure d'acceptation d'un certificat	17
4.4.2	Publication d'un certificat par l'AC.....	17
4.4.3	Notification de l'émission d'un certificat par l'AC à d'autres entités	17
4.5	Utilisation des bi-clés et des certificats	18
4.5.1	Utilisation des bi-clés et des certificats	18
4.5.2	Utilisation des clés publiques et des certificats par les tierces parties	18
4.6	Renouvellement d'un certificat	18
4.7	Changement de clés (ou certification d'une nouvelle clé publique).....	18
4.8	Modification d'un certificat.....	18
4.9	Révocation et suspension d'un certificat	18
4.9.1	Motif de révocation d'un certificat	18
4.9.1.1	Certificat d'ACR	18
4.9.1.2	Certificat d'AC « en ligne »	18
4.9.2	Origine d'une demande de révocation	19
4.9.3	Procédure de demande de révocation.....	19
4.9.4	Délai accordé au porteur pour formuler la demande de révocation	19
4.9.5	Délai de traitement d'une révocation	19
4.9.6	Exigences de vérification de révocation pour les tierces parties	19
4.9.7	Fréquences de publication des LAR	19
4.9.8	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats	19
4.9.9	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats ..	19
4.9.10	Autres moyens disponibles d'information sur les révocations	19
4.9.11	Exigences spécifiques en cas de compromission de la clé privée	19
4.9.12	Causes possibles d'une suspension.....	19
4.9.13	Origine d'une demande de suspension	19
4.9.14	Procédure de traitement d'une demande de suspension	20
4.9.15	Limites de la période de suspension d'un certificat	20
4.10	Service d'état des certificats	20
4.10.1	Caractéristiques opérationnelles.....	20
4.10.2	Disponibilité de la fonction	20
4.11	Fin de la relation entre l'ACR et l'AC	20
4.12	Séquestre et recouvrement de clés.....	20
5	MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN ŒUVRE	21
5.1	Sécurité physique.....	21
5.1.1	Situation géographique et construction des sites	21

5.1.2	Accès physique	21
5.1.3	Alimentation électrique et climatisation	21
5.1.4	Vulnérabilité aux dégâts des eaux	21
5.1.5	Prévention et protection incendie	21
5.1.6	Conservation des supports	21
5.1.7	Retrait de service des supports	21
5.1.8	Sauvegardes hors site	22
5.2	Mesures de sécurité procédurales	22
5.2.1	Rôles de confiance	22
5.2.2	Nombre de personnes requises par tâche.....	22
5.2.3	Identification et authentification pour chaque rôle	22
5.2.4	Rôles exigeant une séparation des attributions.....	23
5.3	Mesures de sécurité vis-à-vis du personnel.....	23
5.3.1	Qualifications, compétences et habilitations requises	23
5.3.2	Procédures de vérification des antécédents.....	23
5.3.3	Exigences en matière de formation initiale	23
5.3.4	Exigences et fréquence en matière de formation continue	23
5.3.5	Fréquence et séquence de rotation entre différentes attributions	23
5.3.6	Sanctions en cas d'actions non autorisées.....	23
5.3.7	Exigences vis-à-vis du personnel des prestataires externes.....	23
5.3.8	Documentation fournie au personnel.....	24
5.4	Procédures de constitution des données d'audit	24
5.4.1	Type d'évènements à enregistrer	24
5.4.2	Fréquence de traitement des journaux d'évènements.....	24
5.4.3	Période de conservation des journaux d'évènements	24
5.4.4	Protection des journaux d'évènements.....	24
5.4.5	Procédure de sauvegarde des journaux d'évènements	25
5.4.6	Système de collecte des journaux d'évènements.....	25
5.4.7	Notification de l'enregistrement d'un évènement au responsable de l'évènement.....	25
5.4.8	Evaluation des vulnérabilités	25
5.5	Archivage des données	25
5.5.1	Types de données à archiver.....	25
5.5.2	Période de conservation des archives	25
5.5.3	Protection des archives.....	25
5.5.4	Procédure de sauvegarde des archives	26
5.5.5	Exigences d'horodatage des données.....	26
5.5.6	Système de collecte des archives	26
5.5.7	Procédures de récupération et de vérification des archives	26
5.6	Changement de clé d'AC	26
5.7	Reprise suite à compromission et sinistre	26
5.7.1	Procédures de remontée et de traitement des incidents et des compromissions	26
5.7.2	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)	27
5.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante.....	27
5.7.4	Capacités de continuité d'activité suite à un sinistre	27
5.8	Fin de vie de l'IGC.....	27
5.8.1	Transfert d'activité.....	27
5.8.2	Cessation d'activité	28
6	MESURES DE SECURITE TECHNIQUES	29
6.1	Génération et installation de bi-clés.....	29
6.1.1	Génération des bi-clés	29
6.1.2	Fourniture de la clé privée à l'AC.....	29
6.1.3	Fourniture de la clé publique à l'AC	29
6.1.4	Fourniture de la clé publique d'ACR aux tierces parties	29
6.1.5	Taille de clés	29
6.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité	29
6.1.7	Objectifs d'usage de la clé	29

6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	29
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques	29
6.2.2	Contrôle de la clé privée par plusieurs personnes	29
6.2.3	Séquestre de clé privée	30
6.2.4	Copie de secours de la clé privée	30
6.2.5	Archivage de la clé privée	30
6.2.6	Transfert de la clé privée vers / depuis le module cryptographique	30
6.2.7	Stockage d'une clé privée dans un module cryptographique	30
6.2.8	Méthode d'activation de la clé privée	30
6.2.9	Méthode de désactivation de la clé privée	30
6.2.10	Méthode de destruction des clés privées	30
6.2.11	Niveau de qualification du module cryptographique	30
6.3	Autres aspects de la gestion des bi-clés	30
6.3.1	Archivage des clés publiques	30
6.3.2	Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés	30
6.4	Données d'activation	31
6.4.1	Génération et installation des données d'activation	31
6.4.2	Protection des données d'activation	31
6.4.3	Autres aspects touchant aux données d'activation	31
6.5	Mécanismes de sécurité des systèmes informatiques	31
6.5.1	Exigences techniques de sécurité des ressources informatiques	31
6.5.2	Indice de sécurité informatique	31
6.6	Contrôles techniques du système pendant son cycle de vie	31
6.6.1	Contrôle des développements des systèmes	31
6.6.2	Contrôles de gestion de la sécurité	32
6.6.3	Contrôle de sécurité du système pendant son cycle de vie	32
6.7	Mécanismes de sécurité du réseau	32
6.8	Horodatage/Système de datation	32
7	CERTIFICATS, CRL, ET PROFILS OCSP	33
7.1	Profil de Certificats	33
7.1.1	Extensions de Certificats	33
7.1.1.1	Certificat ACR	33
7.1.1.2	Certificat AC « en ligne »	33
7.1.2	Identifiant d'algorithmes	34
7.1.3	Formes de noms	34
7.1.4	Identifiant d'objet (OID) de la Politique de Certification	34
7.1.5	Extensions propres à l'usage de la Politique	34
7.1.6	Syntaxe et Sémantique des qualificatifs de politique	34
7.1.7	Interprétation sémantique de l'extension critique "Certificate Policies"	34
7.2	Profil de LAR	34
7.2.1	LAR et champs d'extensions des LAR	34
8	CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS	35
8.1	Fréquences et / ou circonstances des évaluations	35
8.2	Identités / qualifications des évaluateurs	35
8.3	Relations entre évaluateurs et entités évaluées	35
8.4	Sujets couverts par les évaluations	35
8.5	Actions prises suite aux conclusions des évaluations	35
8.6	Communication des résultats	35
9	AUTRES QUESTIONS JURIDIQUES	36
9.1	Tarifs	36
9.2	Responsabilité financière	36
9.3	Confidentialité des informations	36
9.3.1	Informations confidentielles	36
9.3.2	Information considérées comme non confidentielles	36
9.3.3	Obligation de protection des informations confidentielles	36

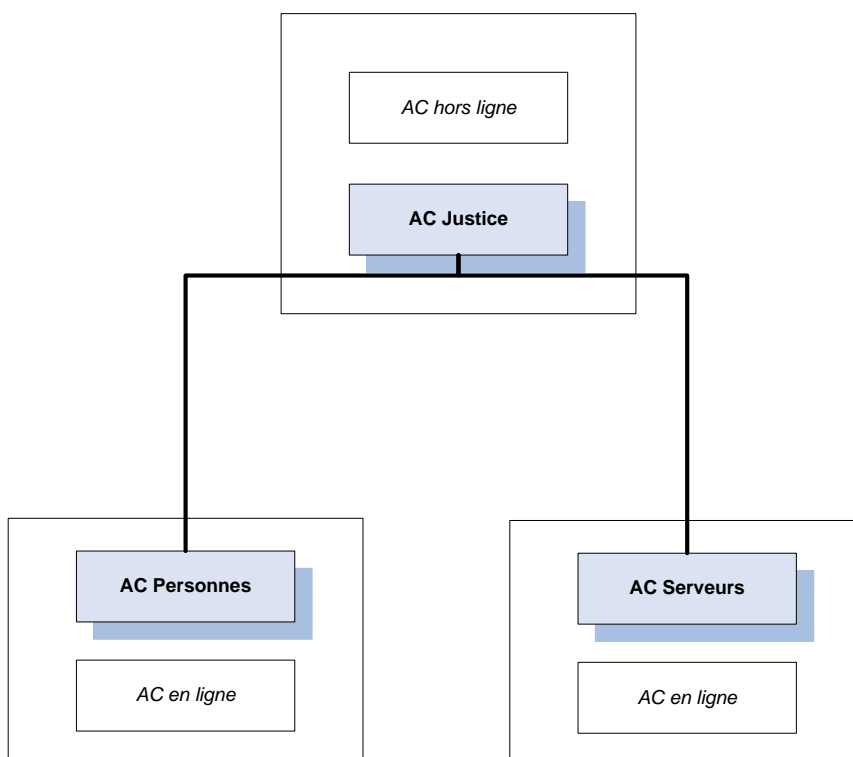
9.4	Confidentialité des informations à caractère personnel	36
9.4.1	Politique de protection des données personnelles	36
9.4.2	Information considérées comme personnelles	36
9.4.3	Information non considérées comme n'étant pas à caractère personnel	36
9.4.4	Responsabilité en termes de protection des données personnelles	36
9.4.5	Notification et consentement d'utilisation des données personnelles	37
9.4.6	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives	37
9.4.7	Autres circonstances de divulgation d'informations personnelles	37
9.5	Droits relatifs à la propriété intellectuelle	37
9.6	Interprétations contractuelles et garanties	37
9.6.1	Ministère de la Justice et des Libertés	37
9.6.2	Obligations et garanties de l'AC	37
9.6.3	Obligations et garanties des autres participants	38
9.7	Limites de garantie	38
9.8	Limites de responsabilité	38
9.9	Indemnités	39
9.10	Durée et fin anticipée de validité de la PC	39
9.10.1	Durée	39
9.10.2	Fin anticipée de validité	39
9.10.3	Effets de la fin de validité et clauses restant applicables	39
9.11	Notifications individuelles et communication avec les participants	39
9.12	Amendements	39
9.12.1	Procédure pour apporter un amendement	39
9.12.2	Mécanisme et période d'information sur les amendements	39
9.12.3	Circonstances selon lesquelles un OID doit être changé	39
9.13	Dispositions concernant la résolution de conflits	39
9.14	Juridictions compétentes	40
9.15	Conformité aux législations et réglementations	40
9.16	Dispositions diverses	40
9.16.1	Accord global	40
9.16.2	Transfert d'activités	40
9.16.3	Conséquences d'une clause non valide	40
9.16.4	Application et renonciation	40
9.16.5	Force majeure	40
9.17	Autres dispositions	40
10	ANNEXE 1 : DOCUMENTS CITES EN REFERENCE	40
10.1	Réglementation	40
10.2	Documents techniques	41
11	ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC	41
11.1	Exigences sur les objectifs de sécurité	41
11.2	Exigences sur la qualification	42

1 INTRODUCTION

1.1 Généralités

Le Ministère de la Justice et des Libertés met en place une Infrastructure de Gestion de Clés (IGC) afin de gérer les certificats d'AC utilisés dans le cadre de ses projets. Cette IGC est appelée IGC Justice.

Les certificats d'utilisateurs sont émis par des Autorité de Certification dites « en ligne » (notées AC « en ligne »). Ces AC sont elles-mêmes signées par une AC de niveau supérieur dite « hors ligne » ou racine. Ainsi donc, les certificats des AC « en ligne » sont signés par l'AC « hors ligne » ou AC racine.



Les AC « hors ligne » servent à authentifier, en signant les AC « en ligne », le domaine de certification de Ministère de la Justice et des Libertés.

La présente politique de certification (PC) a pour objet de décrire la gestion du cycle de vie des certificats des AC « hors ligne » et « en ligne » et des bi-clés associées.


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

L'objectif de cette politique de certification est de définir les engagements minimums que le Ministère de la Justice et des Libertés, en tant que PSCE, doit respecter dans la délivrance et la gestion de certificats d'AC tout au long de son cycle de vie. Certains engagements sont liés à des fréquences et/ou des délais qui ont été regroupés, sous forme de variables de temps, dans le document « Référentiel Général de Sécurité Variables de Temps », version 2.3.

1.2 Nom du Document et Identification

La présente PC appelée : « PC_AC_Justice » est la propriété du Ministère de la Justice et des Libertés. Cette PC est enregistrée par un numéro d'identifiant d'objet (OID) qui est : 1.2.250.1.120.2.1.1.1.

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

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 8

1.3 Les composantes de l'IGC

Pour délivrer les bi-clés et les certificats d'une AC, l'IGC s'appuie sur les services suivants :

- Enregistrement : ce service récupère et vérifie les informations d'identification de l'Autorité Administrative qui demande un certificat d'AC, avant de transmettre la demande de certificat au service de génération de certificat ;
- Génération de bi-clé : ce service génère la bi-clé de l'AC et remet la clé publique à certifier au service de génération de certificat ;
- Génération de certificat : ce service génère les certificats électroniques de l'AC à partir des informations transmises par le service d'enregistrement ;
- Révocation de certificat : ce service traite les demandes de révocation du certificat d'AC et détermine les actions à mener, dont la génération de la Liste d'AC révoquée (LAR ou ARL) ;
- Service de Publication : ce service met à disposition des Utilisateurs de Certificat (UC) et des porteurs de certificat les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, politiques de certification publiées par l'AC, certificats d'AC, certificats, ...), ainsi que les résultats des traitements du service de gestion des révocations (LAR, avis d'information, ...).

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

1.3.1 Ministère de la Justice et des Libertés (ACR – SP)

1.3.1.1 **Autorité de Certification Racine (ACR)**

L'ACR garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Son référentiel de sécurité est composé de la présente PC 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'ACR autorise la création d'AC filles.

L'ACR met en œuvre un service de génération de bi-clés, un service de génération des certificats, un service de révocation de certificats pour la gestion de son certificat et des certificats de porteurs et/ou d'AC conformément à la présente PC et la DPC associée. L'AC a pour responsabilité de garantir le lien (infalsifiable et univoque) entre une identité d'AC et une bi-clé cryptographique. Cette garantie est apportée par le certificat d'AC qu'elle signe avec sa clé privée.


En tant qu'autorité, l'AC doit :

- Définir et valider l'organisation de l'IGC ;
- Définir et contrôler la présente PC et la DPC associée ;
- Contrôler la mise en œuvre de la DPC ;
- Arbitrer les litiges.

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

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

- A l'Opérateur de Service de Certification (OSC), la génération de certificat, la révocation et le renouvellement de certificat ;
- A 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.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 9

1.3.1.2 **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 rend les certificats d'AC et les LAR disponibles auprès des UC. Le SP s'appuie sur les moyens de l'AC afin de réaliser ses services.

Le service de publication (SP) rend disponible les certificats de clés publiques émis par l'AC, aux utilisateurs finaux et aux utilisateurs de certificat conformément à la politique de certification.

Le SP agit conformément à la présente PC qui est établie par l'AC.

1.3.2 **Agence Nationale des Titres Sécurisés (OSC)**

L'Agence Nationale des Titres Sécurisés a le rôle d'Opérateur de Services de Certification.

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

De plus, le Ministère de la Justice et des Libertés a mené une analyse de risques qui a permis de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. L'OSC possède aussi un plan de continuité sur lequel s'appuie l'AC pour la continuité des services d'IGC. Cette analyse de risque 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.

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

1.3.3 **Porteur**

Est considéré comme porteur, toute entité détentrice d'une bi-clé et d'un certificat associé délivrés par l'IGC Ministère de la Justice et des Libertés selon la PC d'une AC (« en ligne »).

Le porteur pourra indifféremment être une personne physique ou morale, un système informatique ou une application. Lorsque le porteur n'est pas une personne physique, il est représenté par la personne qui en est responsable (administrateur, ...). La personne responsable n'est pas obligée de posséder un certificat elle-même, néanmoins si elle en possède un, alors elle peut l'utiliser pour établir une demande de certificat pour l'entité dont elle est responsable.

1.3.4 **Autres participants**

1.3.4.1 **Utilisateur de Certificat (UC)**

Application, personne physique ou morale, organisme administratif ou système informatique matériel qui utilise un certificat de porteur conformément à la politique de sécurité de Ministère de la Justice et des Libertés, afin de valider les fonctions de sécurité mises en œuvre à l'aide des certificats (signature, chiffrement et authentification). L'utilisateur de certificat peut détenir son propre certificat. Un porteur qui reçoit un certificat d'un autre porteur devient de ce fait un utilisateur de certificat. Dans le cadre de cette PC, l'UC doit valider les certificats d'AC et contrôler les LAR.

1.4 **Utilisation des certificats AC**

1.4.1 **Bi-clés et certificats d'AC**

Une bi-clé d'ACR sert à signer des certificats d'AC et des LAR. Un certificat électronique d'ACR identifie les chaînes de certification de Ministère de la Justice et des Libertés utilisées dans le cadre des applications reconnues par Ministère de la Justice et des Libertés.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 10

Les bi-clés d'AC « en ligne » servent à signer des certificats de porteurs et les Listes de Certificats Révoqués (LCR).

Les chaînes de certificats issues de l'IGC de Ministère de la Justice et des Libertés possèdent la structure suivante:

- Certificat ACR (AC « hors ligne ») : certificat électronique auto-signé d'une ACR ;
- Certificat d'AC (AC « en ligne »): certificat électronique délivré à une AC par l'ACR ;
- Certificat porteur : certificat électronique délivré à un porteur par une AC (« en ligne »).

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 deviendrait IGC/A → AC Justice → AC Personnes → Certificat de porteur.

1.4.2 Utilisation interdite des certificats

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

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

1.5 Application de la politique

1.5.1 Organisme responsable de la présente politique

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

Le HFDS ou son délégué ont l'autorité et la responsabilité finale pour déterminer la conformité de la DPC avec la PC.

Le HFDS ou son délégué, peuvent demander au FSSI de procéder à des analyses/contrôles de conformité et/ou des audits.

Au vu de ceux-ci le HFDS ou son délégué accorde ou non l'autorisation pour l'AC d'émettre des certificats.

1.5.4 Procédure d'approbation du présent document

Les personnes habilitées à déterminer la conformité de la DPC avec la présente PC sont nommées par le HFDS ou son délégué sur la base, en particulier, de leur capacité à réaliser des évaluations de sécurité. Ces personnes peuvent être des personnes internes ou externes à l'AA, mais agissant pour son compte.

Les services du HFDS doivent s'assurer de la conformité de la DPC avec la présente PC pour la mise en œuvre opérationnelle des composantes de l'IGC Justice.

1.6 Définitions et Acronymes

1.6.1 Acronyme

AA	Autorité Administrative
AC	Autorité de certification
ACR	Autorité de certification Racine
AE	Autorité d'enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
ANTS	Agence Nationale des Titres Sécurisés
CGU	Conditions Générales d'Utilisation
CRL ou LCR	Certificate Revocation List (Liste des Certificats Révoqués)
DPC	Déclaration des Pratiques de Certification
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	Liste des certificats d'AC Révoqués
LCR ou CRL	Liste des Certificats Révoqués ou (Certificate Revocation List)
MJL	Ministère de la Justice et des Libertés
OID	Object Identifier
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adleman
SHA-256	Secure Hash Algorithm 256
SP	Service de Publication
SSL	Secure socket Layer
PC	Politique de certification
UC	Utilisateur de Certificats
URL	Uniform Resource Locator

1.6.2 Définitions

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

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

Autorité de Certification (AC) : autorité à qui un ou plusieurs utilisateurs se fient pour créer et attribuer des certificats. Facultativement, l'autorité de certification peut créer les clés d'utilisateur [ISO/IEC 9594-8; ITU-T X.509].

Autorité d'Enregistrement (AE) : désigne l'entité qui vérifie les données propres au porteur. L'AE est une composante de l'IGC qui dépend d'au moins d'une Autorité de certification. L'AE a pour fonction de réceptionner et de traiter les demandes d'émission de certificat.

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

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 12

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

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

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

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

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

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

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

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

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

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

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

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


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

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

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

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

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

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>LIBERTÉ • ÉGALITÉ • FRATERNITÉ</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 13

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

Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en 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 : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

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

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'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 qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

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

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

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

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

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de 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 : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 14

2 ANNUAIRES ET SERVICES DE PUBLICATION

2.1 Service de publication

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

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

- La présente PC ;
- Les certificats d'AC ;
- La documentation relative à la demande de certificat et la demande de révocation ;
- Les LAR : http://www.justice.gouv.fr/igc/ants/mj_arl.crl.

2.3 Heure et fréquence de publication

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

Les certificats d'AC sont publiés 24 heures sur 24, 7 jours sur 7.

Les LAR sont publiées 24 heures sur 24, 7 jours sur 7, avec une fréquence de publication annuelle.

2.4 Contrôle d'accès au service de publication

Le SP s'assure que les informations sont libres d'accès en lecture et protégées en intégrité contre les modifications non autorisées.

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

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

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

3.1.1.1 Certificat d'ACR

L'identité de l'ACR dans le certificat de l'ACR 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 Justice

3.1.1.2 Certificat d'AC « en ligne »

L'identité d'AC dans le certificat de l'AC « en ligne » est la suivante :

Champ de base	Valeur
Issuer DN	C = FR O = Justice OU = = 0002 <espace > 110010014 CN = Autorité de certification Justice
Subject DN	<Identifiant de l'AC comme défini dans la PC AC Personnes>

3.1.2 Utilisation de noms explicites

Les certificats d'AC émis conformément à la présente PC comportent des noms explicites et nominatifs.

3.1.3 Anonymat ou utilisation de pseudonyme

L'identité utilisée pour les certificats d'AC n'est ni un pseudonyme ni un nom anonyme.

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 contenus dans les chaînes de certification autorisées (voir § 1.4.1 ci-dessus), pour mettre en œuvre et valider des fonctions de sécurité en vérifiant entre autres les identités (DN) des AC telles que contenues dans les certificats d'AC.

3.1.5 Unicité des noms

Les identités contenues dans les certificats (voir § 3.1.1) sont uniques au sein du domaine de certification des AC. Les AC assurent cette unicité au moyen de leur processus d'enregistrement.

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

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

La présente PC ne formule pas d'exigence spécifique sur le sujet. L'AC est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 16

3.2 Vérification initiale d'identité

3.2.1 Preuve de possession de la clé privée

La preuve de la possession de la clé privée par l'AC est réalisée par les procédures de génération (voir § 6.1.2) de la clé privée correspondant à la clé publique à certifier et le mode de transmission de la clé publique (voir § 6.1.3).

3.2.2 Vérification de l'identité des organisations

L'authentification est réalisée par le Ministère de la Justice et des Libertés qui communique les données d'identification de l'organisme à inclure dans l'identité de l'AC (voir § 3.1.1) à l'OSC au préalable de la cérémonie des clés.

3.2.3 Vérification de l'identité des personnes

Enregistrement d'une AC

L'AE de l'ACR doit enregistrer les informations nécessaires à l'enregistrement. La DPC donnera en outre les détails techniques sur le contenu exact des formulaires, ainsi que les pièces à fournir lors de l'authentification.

Le dossier d'enregistrement doit être déposé auprès de l'AE de l'ACR.

Pour le certificat de l'ACR, l'enregistrement s'effectue conformément à la PC de l'IGC/A.

3.2.4 Informations non vérifiées

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

3.2.5 Validation du représentant légal

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

3.2.6 Critères de reconnaissance

Le Ministère de la Justice et des Libertés gère les demandes d'accords et les accords de reconnaissance avec des AC extérieures de son IGC. Toute demande d'accord de reconnaissance avec d'autres AC doit être soumise à l'approbation de l'ACR. En particulier la reconnaissance de l'AC racine du ministère par l'IGC/A devra se faire après accord de l'autorité responsable de l'ACR.

3.3 Vérifications aux fins de renouvellement de clés

Le renouvellement de la bi-clé d'une AC entraîne automatiquement la génération et la fourniture d'un nouveau certificat d'AC.

3.3.1 Vérifications aux fins de renouvellement de clés en situation normale

Les vérifications relatives au renouvellement d'une bi-clé sont effectuées conformément aux procédures initiales (voir § 3.2 ci-dessus).

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

Les vérifications relatives au renouvellement d'une bi-clé après révocation du certificat de clé publique correspondant sont effectuées conformément aux procédures initiales (voir § 3.2).

3.4 Vérifications aux fins de révocation

Si la demande de révocation est due à une compromission ou suspicion de compromission de clé, perte ou vol, l'authentification de la demande de révocation ne peut être effectuée avec la clé compromise.

Les demandes de révocation sont authentifiées par le Ministère de la Justice et des Libertés. La procédure de vérification est identique à celle utilisée pour l'enregistrement initial (voir § 3.2).

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 17

4 EXIGENCES OPERATIONNELLES

4.1 Types de certificat

4.1.1 Origine de la demande de certificat

Lorsqu'une nouvelle AC « en ligne » doit être créée, une demande de création est effectuée par le Ministère de la Justice et des Libertés.

4.1.2 Procédure d'enregistrement et responsabilités

Les demandes de certificat d'AC sont enregistrées par le Ministère de la Justice et des Libertés.

Une demande de création d'AC « en ligne » contient l'identifiant de l'AC « hors ligne » qui doit lui signer son certificat.

4.2 Traitement d'une demande de certificat

4.2.1 Identification et authentification

Le Ministère de la Justice et des Libertés identifie et authentifie la demande de certificat d'AC.

4.2.2 Approbation ou rejet d'une demande de certificat

Le Ministère de la Justice et des Libertés autorise ou rejette la création d'un certificat d'AC. En cas d'acceptation, le Ministère de la Justice et des Libertés transmet la demande validée à l'OSC afin de procéder à la cérémonie des clés de création du certificat.

4.2.3 Durée de traitement d'une demande de certificat

La durée maximale de traitement d'une demande de certificat est définie dans la DPC.

4.3 Délivrance d'un certificat

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

Les ACR, ACI et AC « en ligne » sont générées pendant une cérémonie des clés (voir § 6.1).

Au préalable de la cérémonie des clés, le Ministère de la Justice et des Libertés vérifie le contenu des documents de nommage des AC, en termes de complétude et d'exactitude des informations présentes. Ce document est utilisé comme base de réalisation de la cérémonie des clés de création des AC.

Les certificats d'ACR et d'AC sont signés par l'ACR pendant la cérémonie des clés (voir § 6.1).

Le Ministère de la Justice et des Libertés vérifie en fin de cérémonie de clés d'AC que le(s) certificat(s) d'AC produit(s) est(sont) conforme(s) au(x) document(s) de nommage.

4.3.2 Notification de l'émission d'un certificat

La notification est effectuée à la fin de la cérémonie des clés de l'AC par remise du certificat d'AC à son demandeur.

4.4 Acceptation d'un certificat

4.4.1 Procédure d'acceptation d'un certificat


L'AC vérifie que le certificat contient les informations décrites dans le document de nommage signé par le Ministère de la Justice et des Libertés. Dès que l'AC confirme l'adéquation entre le certificat et le document de nommage, alors l'AC accepte le certificat d'AC émis.

4.4.2 Publication d'un certificat par l'AC

Les certificats d'AC sont publiés par le SP.

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

Le SP informe les UC de l'émission de certificat d'AC.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 18

4.5 Utilisation des bi-clés et des certificats

4.5.1 Utilisation des bi-clés et des certificats

Les utilisations des bi-clés et des certificats sont définies au § 1.4 ci-dessus. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (voir § 6.1.7 ci-dessous).

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

Les certificats d'AC (composant la chaîne de certification) ne peuvent être utilisés par un UC qu'à des fins de validation d'une chaîne de confiance.

Il est de la seule responsabilité de l'UC de s'assurer de la validité des certificats délivrés par l'ACR ou l'AC à l'aide des listes de certificats d'autorité révoquées publiés par le SP.

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)

La demande d'un nouveau certificat d'AC nécessite le changement de la bi-clé de l'AC.

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

Les bi-clés doivent être périodiquement renouvelées :

- selon les recommandations émises par l'ANSSI en matière de cryptanalyse, afin de minimiser les possibilités d'attaques cryptographiques,
- pour que l'ACR puisse continuer à délivrer des certificats d'AC d'une durée constante,
- en cas de compromission, suspicion de compromission, vol, dysfonctionnement ou perte des moyens de reconstruction de la clé privée de l'AC.

Le changement de bi-clé entraîne le changement de certificat, la procédure à suivre est identique à la procédure initiale de certification décrite aux § 3.2, § 4.1, § 4.3 et § 4.4 ci-dessus.

4.8 Modification d'un certificat

La modification d'un certificat signifie qu'un certificat contenant des informations différentes est créé avec la même clé publique que celle contenue dans le certificat initial.

La modification d'un certificat n'est pas autorisée par la présente PC.

4.9 Révocation et suspension d'un certificat

4.9.1 Motif de révocation d'un certificat

4.9.1.1 Certificat d'ACR

Les causes de révocations sont les suivantes par composante identifiée :

- cessation d'activité de l'ACR ;
- compromission de clé privée de l'ACR ;
- compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'AC (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés) ;
- non-respect de la politique de certification et de la déclaration des pratiques de certification de l'ACR ;
- changement d'informations dans le certificat ;
- obsolescence de la cryptographie au regard des exigences de l'ANSSI.

4.9.1.2 Certificat d'AC « en ligne »

Les causes de révocations sont les suivantes par composante identifiée :

- cessation d'activité de l'ACR ;

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 19

- compromission de clé privée de l'ACR ;
- compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'AC (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés) ;
- non-respect de la politique de certification et de la déclaration des pratiques de certification de l'ACR ;
- non-respect de la politique de certification et de la déclaration des pratiques de certification de l'AC ;
- changement d'informations dans le certificat ;
- obsolescence de la cryptographie au regard des exigences de l'ANSSI.

4.9.2 Origine d'une demande de révocation

Seule l'autorité responsable de l'ACR peut demander la révocation du certificat d'une ACR.

4.9.3 Procédure de demande de révocation

Le Ministère de la Justice et des Libertés transmet une demande de révocation à l'ACR.

L'ACR demande ensuite à l'OSC de révoquer le certificat d'AC en question.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

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

4.9.5 Délai de traitement d'une révocation

Le service de révocation est disponible les jours ouvrés.

En cas d'indisponibilité du système, du service, ou d'autres éléments, qui échappe au contrôle de l'AC, cette dernière fait de son mieux pour que l'indisponibilité de ce service puisse permettre la révocation du certificat d'AC au plus vite. L'AC devra traiter une demande de révocation dès que possible suivant sa réception et de préférence immédiatement.

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

4.9.6 Exigences de vérification de révocation pour les tierces parties

Il appartient aux UC de vérifier l'état de validité d'un certificat d'AC à l'aide de l'ensemble des LAR émises.

4.9.7 Fréquences de publication des LAR

La LAR est émise tous les ans. En cas de révocation d'AC, la LAR est publiée dès qu'elle est générée.

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

Si un autre moyen de diffusion d'information est mis en œuvre, alors les exigences liées à la disponibilité doivent être conformes à celles décrites au § 4.9.6 et au §4.9.7.

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

Voir § 4.9.6 ci-dessus.

4.9.10 Autres moyens disponibles d'information sur les révocations

Si d'autres moyens sont à mettre en œuvre, la DPC les précisera.

4.9.11 Exigences spécifiques en cas de compromission de la clé privée


L'ACR définira les mesures dans la DPC.

4.9.12 Causes possibles d'une suspension

Sans objet.

4.9.13 Origine d'une demande de suspension

Sans objet.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 20

4.9.14 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.15 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Service d'état des certificats

4.10.1 Caractéristiques opérationnelles

Il n'y a pas de service d'état de validité des certificats autre que la publication de LAR. Les LAR sont au format V2 et publiés en HTTP à l'adresse http://www.justice.gouv.fr/igc/ants/mj_ac.crl.

4.10.2 Disponibilité de la fonction


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

4.11 Fin de la relation entre l'ACR et l'AC

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

4.12 Séquestre et recouvrement de clés

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

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 21

5 MESURES DE SECURITE PHYSIQUE, PROCEDURES ET MISE EN ŒUVRE

5.1 Sécurité physique

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. Les caractéristiques ont été définies selon les résultats de l'analyse de risques menée par le Ministère de la Justice et des Libertés.

Les opérations cryptographiques sur l'ACR 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'IG 1300.

5.1.2 Accès physique

Les moyens et informations 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.

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 doit garantir, 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 seront précisés dans la DPC.

5.1.3 Alimentation électrique et climatisation

Afin d'assurer la disponibilité des systèmes informatiques 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 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'informations 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 Retrait de service des supports

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.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 22

5.1.8 Sauvegardes hors site

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.

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'assurera 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

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

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

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 cinq 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.
- « 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 » - personnels, 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 Justice. Il 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).


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 permet de définir 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 ;
- 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.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 23

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. L'annexe "Rôles" de la DPC précise comment et sous quelles conditions ces rôles peuvent être cumulés par un même exploitant.

La séparation de ces rôles reposent sur :

- la notion de séparation des rôles dits « d'administration », des rôles dits « opérationnel » : 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.

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'assurera 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

Tous les personnels opérant pour le compte de l'IGC Justice sont habilités selon le niveau défini par l'Administration. Le nom et la fonction de tous les personnels intervenant pour le compte de l'IGC Justice sont répertoriés par l'OSC. L'OSC s'engage à ce que les compétences professionnelles des personnels soient cohérentes à leurs attributions.

5.3.2 Procédures de vérification des antécédents

Les personnels de l'IGC Justice sont habilités selon le niveau défini par l'OSC.

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.

Les personnels ont eu connaissance et compris les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

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

5.3.5 Fréquence et séquence de rotation entre différentes attributions


Les règles à appliquer en terme de gestion de carrière pour un exploitant donné sont celles pratiquées par l'Administration.

5.3.6 Sanctions en cas d'actions non autorisées

Le responsable de l'AC Justice décide des sanctions à appliquer lorsqu'un agent abuse de ses droits ou effectue une opération non conforme à ses attributions, selon les modalités applicables. 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 les § 5.3.1, § 5.3.2, § 5.3.3 et § 5.3.4.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 24

5.3.8 Documentation fournie au personnel

Chaque personnel doit disposer au minimum 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'assurera de la mise en œuvre effective des mesures de constitution des données d'audit dans la mise en œuvre opérationnelle des certificats 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'ACR (accès physique, ...) qu'elle met en œuvre.

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

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

Pour les types d'évènements pour lesquels ces informations existent, les enregistrements seront opérés :

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

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 doit se faire, sauf exception, le même jour ouvré que l'évènement.

5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'évènements doivent être contrôlés et analysés par un responsable de sécurité de l'OSC afin d'identifier les anomalies liées à des tentatives en échec (voir § 5.4.8).

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 doivent être conservés pendant 10 ans après leur génération. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois. Ils doivent rester sur le site au moins un mois.


5.4.4 Protection des journaux d'évènements

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

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

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

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.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 25

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 peut être interne ou externe aux composantes de l'IGC. Le système 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 doit être 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) doit être 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.

5.5 Archivage des données

5.5.1 Types de données à archiver

L'archivage doit permettre d'assurer la pérennité des journaux constitués au profit de l'IGC. Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont les suivantes :

- Accords contractuels ou conventions ;
- Certificats AC ;
- LAR ;
- Opérations liées à la gestion du cycle de vie des certificats ;
- Données d'identification personnelles (en respectant les exigences de la CNIL) ;
- Journaux d'évènements ;
- Logiciels et fichiers de configuration des différentes composantes ;
- Ensemble des éléments utiles à l'enregistrement.

5.5.2 Période de conservation des archives

La rétention des archives doit être :

- Certificats 30 ans après leur expiration
- LAR : 30 ans après leur expiration ;
- Journaux d'évènements : **5 ans** après leur génération.

5.5.3 Protection des archives

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

- être protégées en intégrité ;
- n'être accessibles qu'aux personnes autorisées ;
- pouvoir être relues et exploitées.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>LIBERTÉ • ÉGALITÉ • FRATERNITÉ</small> <small>REPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 26

5.5.4 Procédure de sauvegarde des archives

Le responsable de l'ACR 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

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

5.5.6 Système de collecte des archives

Le système devra assurer 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

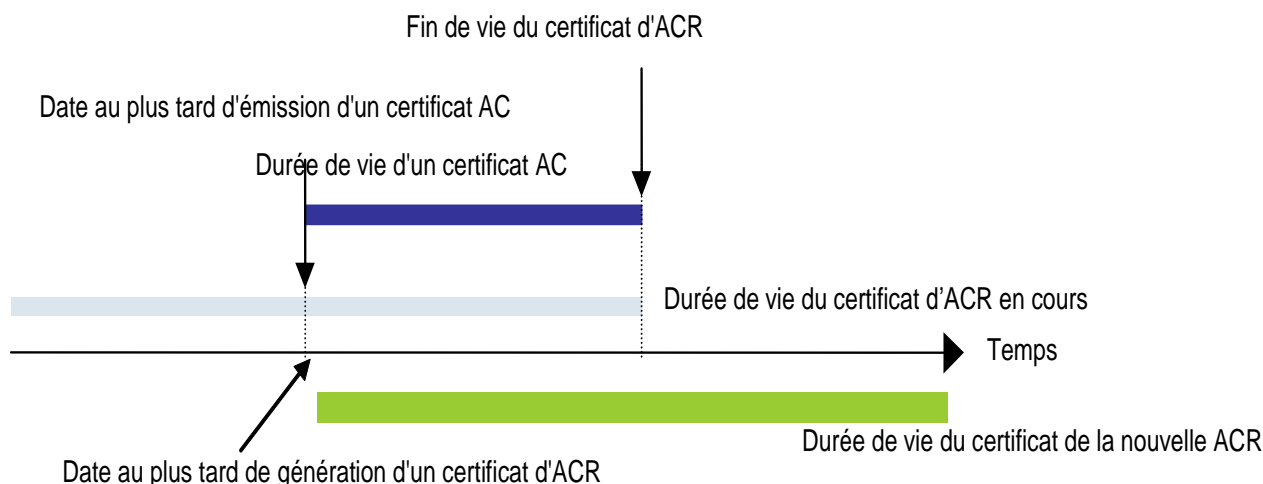
Les archives (papiers et électroniques) doivent pouvoir être récupérées par l'ACR dans un délai maximum de 48 heures ouvrées.

5.6 Changement de clé d'AC

La durée de vie d'un certificat d'ACR est de 12 ans et est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationales ou internationales compétentes en la matière.

Une ACR ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'ACR. Un certificat AC à une durée de vie de 6 ans.

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




Par ailleurs, l'ACR 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

La référence au plan anti-sinistre (du MJL et de l'ANTS), ses modalités de déclenchement et les personnes responsables de ce plan sont identifiées dans la DPC. Notamment chaque entité agissant pour le compte de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, Ce plan doit être

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 27

régulièrement testé. L'IGC dispose d'un plan de reprise d'activité en cas de sinistre qui 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 en cas de compromission de clés.

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

Les incidents ou compromission détectés par l'ACR font l'objet d'une information à l'ACR de l'IGC/A.

En cas de révocation du certificat d'AC, l'ACR pourra proposer 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)

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

Le plan de reprise d'activité doit être testé une fois par an.

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

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

- Le responsable de l'ACR, après enquête sur l'évènement décide 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 ;
- Le responsable de l'ACR décide ou non de générer un nouveau certificat d'AC ;
- Une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis ;
- Les 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 de l'IGC

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 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.

L'ACR s'engage à ce qu'en de fin de vie dont l'IGC dont elle a la charge, à communiquer à l'ACR de l'IGC/A dans un délai de 3 mois avant la cessation d'activité..

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 doit entre autres obligations :

- 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)

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 28

- 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 doit préciser dans sa DPC qui 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'OSC œuvrant pour le compte de l'IGC et procédant au transfert de son activité doit entre autres obligations :

- avertir l'AC de son intention de transférer son activité avec un préavis d'au moins **1** mois ;
- remettre ses archives à 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.

5.8.2 Cessation d'activité

En cas de l'arrêt de son service, l'AC doit :

- Révoquer les certificats d'AC ;
- Informer les porteurs et utilisateurs de certificats, dont l'IGC/A et les États de l'Union Européenne de la révocation de ses propres certificats;
- Prendre toutes les mesures nécessaires pour détruire les clés privées ou les rendre inopérantes.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 29

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

A la demande du Ministère de la Justice et des Libertés pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle qualifiée au niveau renforcé.

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.

6.1.2 Fourniture de la clé privée à l'AC

La clé privée de l'AC reste et est mise en œuvre dans les locaux sécurisés de l'OSC.

6.1.3 Fourniture de la clé publique à l'AC

En cas de transmission de la clé publique de l'ACR vers une autre composante (IGC/A), la clé est protégée en intégrité et son origine est authentifiée (certificat autosigné).

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

Le certificat d'ACR généré est remis au représentant de l'ACR lors de la cérémonie des clés.

6.1.5 Taille de clés

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

L'IGC Justice et les AC filles utilisent l'algorithme RSA avec la fonction de hachage SHA-256. La taille de la bi-clé des AC « en ligne » est de 2048 bits. La taille de la bi-clé d'une AC « hors ligne » est de 4096 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 correspondant à la bi-clé (voir § 6.1.5).

6.1.7 Objectifs d'usage de la clé

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

- Key CertSign ;
- Key CRL Sign.

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

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, aux standards en vigueur ou suivent les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés devront être conformes aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

6.2.2 Contrôle de la clé privée par plusieurs personnes

L'activation de la clé privée d'AC est contrôlée par au moins 3 personnes détenant des données d'activation et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée d'AC font

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 30

l'objet d'une authentification forte. L'AC est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seuls rôles de confiance qui peuvent émettre des certificats.

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

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

6.2.5 Archivage de la clé privée

Les clés privées d'AC ne sont jamais archivées.

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

Les clés d'AC sont générées, activées et stockées dans des ressources cryptographiques matérielles.

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

6.2.7 Stockage d'une clé privée dans un module cryptographique

Les clés privées d'AC stockées dans des ressources cryptographique 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

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

6.2.9 Méthode de désactivation de la clé privée

Après utilisation, les ressources cryptographiques matérielles sont désactivées.

Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

6.2.10 Méthode de destruction des clés privées

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.

6.2.11 Niveau de qualification du module cryptographique

Les ressources cryptographiques matérielles utilisées par l'AC sont certifiées au niveau EAL4+ selon les critères communs (norme ISO 15408).


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 ci-dessus).

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

Une AC ne peut émettre de certificats d'une durée de vie supérieure à celle de son propre certificat. De ce fait, la durée de vie du certificat d'une AC de niveau inférieur ne peut excéder la durée de vie du certificat de l'AC qui l'émet.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 31

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (voir § 6.1). Les données d'activation sont générées automatiquement selon un schéma de partage des secrets de type 3 parmi 5¹. Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.2 Protection des données d'activation

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 AC à un même instant.

6.4.3 Autres aspects touchant aux données d'activation

Les données d'activation ne sont en aucun cas transmises à une entité tierce, en particulier dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance. Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

6.5 Mécanismes de sécurité des systèmes informatiques

6.5.1 Exigences techniques de sécurité des ressources informatiques

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

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

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

6.5.2 Indice de sécurité informatique

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

6.6 Contrôles techniques du système pendant son cycle de vie

6.6.1 Contrôle des développements des systèmes

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

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;
- Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation ;
- Les matériels et logiciels sont dédiés aux activités d'AC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'AC ;

¹ Dans ce schéma le secret est réparti sur cinq porteurs et la restauration du secret impose la présence de 3 porteurs quelconques parmi les 5 porteurs.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>LIBERTÉ • ÉGALITÉ • FRATERNITÉ</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 32

- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'AC. Seules les applications nécessaires à l'exécution des activités IGC sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite ;
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.2 Contrôles de gestion de la sécurité

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

6.6.3 Contrôle de sécurité du système pendant son cycle de vie

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

6.7 Mécanismes de sécurité du réseau

Une analyse de risque est menée par l'AA 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.

Les composants de l'AC « hors ligne » ne sont jamais connectés à un réseau.

6.8 Horodatage/Système de datation

Il n'y a pas d'horodatage utilisé par l'AC « hors ligne » mais une datation des événements qui permet, à partir d'une date fournie par le système d'exploitation de l'AC hors ligne de séquencer les événements. Des procédures automatiques ou manuelles doivent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

7 CERTIFICATS, CRL, ET PROFILS OCSP

7.1 Profil de Certificats

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

7.1.1 Extensions de Certificats

7.1.1.1 Certificat ACR

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

Champ de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil de Key Ceremony
Issuer DN	C = FR
Subject DN	O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification Justice
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Taille des clés	4096 bits
Durée de validité	12 ans

Le certificat d'ACR contient les extensions suivantes :

- Authority Key Identifier (non critique) ;
- Basic Constraints (critique) ;
- Certificate Policies (non critique) ;
- CRL Distribution Points (non critique) ;
- Key usage (critique) ;
- Subject Key Identifier (non critique).


7.1.1.2 Certificat AC « en ligne »

Les informations principales contenues dans le certificat de l'AC « en ligne » sont :

Champ de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil de Key Ceremony
Issuer DN	C = FR O = Justice OU = 0002 <espace > 110010014 CN = Autorité de certification Justice
Subject DN	Défini dans [Document nommage]
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Taille des clés	2048 bits
Durée de validité	6 ans

Par défaut les AC « en ligne » sont signée par l'ACR. Le certificat d'AC « en ligne » contient les extensions suivantes :

- Authority Key Identifier (non critique) ;
- Basic Constraints (critique) ;
- Certificate Policies (non critique) ;
- CRL Distribution Points (non critique) ;
- Key usage (critique) ;

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>LIBERTÉ • ÉGALITÉ • FRATERNITÉ</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 34

- Subject Key Identifier (non critique).

7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est Sha-256WithRSAEncryption: {iso(1) member-body(2) us(840) rsdsi(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 AC qui est portée dans les certificats d'AC.

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

Les certificats d'AC contiennent tous l'OID de la présente PC qui est : 1.2.250.1.120.2.1.1.1.

7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

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

Pas d'exigence formulée.


7.2 Profil de LAR

7.2.1 LAR et champs d'extensions des LAR

Toutes les AC « hors ligne » émettent une LAR.

Les caractéristiques de LAR sont :

Caractéristiques de chaque LAR :	Durée de validité : 14 mois. Périodicité de mise à jour : à chaque cérémonie de clé d'AC Version de la LAR (v1 ou v2) : v2 Extensions : Numéro de la LAR et AKI URL http de publication : URI= http://www.justice.gouv.fr/igc/ants/mj_arl.crl
---	--

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 35

8 CONTROLES DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquences et / ou circonstances des évaluations

Le responsable de l'exploitation des composantes d'IGC (responsable d'application de l'OSC, responsable de l'AE¹) demande l'approbation du responsable de l'ACR du 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.

Le responsable de l'AC Justice doit prévenir les IGC avec lesquelles des accords de reconnaissance entre IGC ont été conclus dans la mesure où ces modifications peuvent affecter ces accords ou le niveau de sécurité offert par l'IGC.

L'ACR doit également procéder 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.

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


A l'issue d'un contrôle de conformité, l'équipe d'audit rend un avis au responsable d'exploitation et au responsable de l'ACR Justice 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'au responsable de l'ACR Justice.

¹ Est concerné par ce point la gestion de l'identifiant unique au sein du Ministère, ainsi que la gestion de l'annuaire comprenant la gestion des droits.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 36

9 AUTRES QUESTIONS JURIDIQUES

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 informations

9.3.1 Informations confidentielles

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

- Clés privées des certificats d'AC ;
- Données d'activation associées à une bi-clé cryptographique ;
- 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 Information considérées comme non 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 Obligation de protection des informations confidentielles

L'IGC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

9.4 Confidentialité des informations à caractère personnel

9.4.1 Politique de protection des données personnelles

Il est entendu que toutes collectes et tout usage de données à caractère personnel qui seraient effectués par l'AC du Ministère de la Justice et des Libertés seront 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

9.4.2 Information considérées comme personnelles

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

- Identité des porteurs de secret ;
- Demande (renseigné) de certificat ;
- Demande (renseigné) de révocation ;
- Motif de révocation.


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

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AE, l'ACR 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 et la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique s'applique au contenu de tous les documents collectés, détenus ou transmis par l'AC dans le cadre de la délivrance d'un certificat.

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 37

Les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'ACR ou l'AE 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 autre que celle définie dans le cadre de la présente PC, sans consentement exprès et préalable de la part du porteur. Ce consentement est considéré comme obtenu lors de la soumission de la demande de certificat et du fait de l'acceptation par le porteur du certificat émis par l'AC (en accord avec la présente PC) au titre de l'utilisation par les 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'AA. 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 à la réglementation en vigueur sur le territoire français et dispose de procédures de restitutions d'informations aux autorités judiciaires et administratives.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Les informations relatives à une personne définies comme confidentielles au § 9.3.1 ne peuvent être divulguées qu'à leur propriétaire ou à un tiers habilité au niveau adéquat.

L'AC obtient l'accord de Ministère de la Justice et des Libertés de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8 **Erreur ! Source du renvoi introuvable.**

9.5 Droits relatifs à la propriété intellectuelle

La présente PC ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

9.6 Interprétations contractuelles et garanties

9.6.1 Ministère de la Justice et des Libertés

Le Ministère de la Justice et des Libertés a pour obligation :


- D'élaborer et de valider la PC ;
- De maintenir la présente PC et la DPC associée en conformité avec les recommandations de l'ANSSI ;
- D'assurer le suivi et le contrôle de l'IGC Ministère de la Justice et des Libertés par le biais d'audit de conformité.

9.6.2 Obligations et garanties de l'AC

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

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

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

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 38

- N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC ;
- Respecter et appliquer les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC doit être transmise à la composante concernée) ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions du Ministère de la Justice et des libertés de contrôler et vérifier la conformité avec la PC ;
- Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- Faire certifier la clé publique, correspondante à sa clé privée, par l'ACR Ministère de la Justice et des libertés ;
- apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs ;
- Se conformer aux procédures et instructions particulières publiées par l'ACR de l'IGC/A pour lui adresser ses demandes de certification, de révocation, ou toute autre demande à l'attention de l'IGC/A ;
- Assurer l'authenticité, l'exactitude et la complétude des informations transmises à l'AE de l'IGC/A par elle-même et par les autorités auxquelles elle délègue ;
- Assurer l'information des autorités et agents auxquelles elle délègue, concernant leurs rôles et responsabilités, et le traitement des informations à caractère personnel ou confidentielles, conformément à la présente PC ;
- Publier les LAR de l'IGC/A dans les délais impartis ;
- Informer dans les plus brefs délais l'ACR de l'IGC/A de tout événement modifiant ou susceptible de modifier les conditions d'application de la présente PC, notamment pour une cause motivant une révocation, pour que l'ACR de l'IGC/A puisse remplir ses obligations en la matière.

9.6.3 Obligations et garanties des autres participants

La DPC précisera les exigences si besoin est.

9.7 Limites de garantie

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

- L'identification et l'authentification de l'ACR avec son certificat ;
- L'identification et l'authentification des AC « en ligne » avec les certificats d'AC générés par l'ACR ;
- 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

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 39

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

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

9.10.2 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.

9.11 Notifications individuelles et communication avec les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'ACR devra au plus tard un mois avant le début de l'opération, 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.

9.12 Amendements

9.12.1 Procédure pour apporter un amendement

L'ACR de l'IGC Justice révisé sa PC et sa DPC à chaque évolution du système et 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 2 mois au moins aux composantes de l'AC (OSC, AE, SP) 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 de l'ACR pouvant être inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des AC, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'ACR doit évoluer dès lors qu'un changement majeur intervient dans les exigences de la présente PC.

9.13 Dispositions concernant la résolution de conflits

Sans objet

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	 <small>Liberté • Égalité • Fraternité</small> <small>RÉPUBLIQUE FRANÇAISE</small>
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 40

9.14 Juridictions compétentes

Sans objet

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 Justice 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]
- l'article 801-1 du CPP [CPP801]
- la loi n° 2004-575 du 21 juin 2004 modifiée, pour la confiance dans l'économie numérique [LCEN] ;
- la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés [LCNIL] ;
- 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 [ORD05-1516] ;
- 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 [DEC01-272] ;
- 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 [ORD05-1516].

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
[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 : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig
[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 : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=vig
[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 : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=vig
[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 : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678&dateTexte=vig
[loi120400]	Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations. Disponible en ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629288&dateTexte=vig

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
[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

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,
- Etre 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,
- Etre 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 créer une signature électronique sécurisée, pour 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,

OID : 1.2.250.1.120.2.1.1.1	Ministère de la Justice et des Libertés	
Date : 15/09/2011	POLITIQUE DE CERTIFICATION – AC Racine Justice	Page 42

- Créer des enregistrements d'audit pour chaque modification concernant la sécurité,
- Si une fonction de sauvegarde et de restauration des clés privée de l'AC est offerte, 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 au niveau renforcé, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre 11.1 ci-dessus.