

NATURE DU DOCUMENT			
Document Sécurité			
			
REFERENCE	DATE	VERSION	
DT-FL-0905/001	14 Janvier 2009	1.2	
POLITIQUE DE CERTIFICATION AUTORITE DE CERTIFICATION RACINE			
EMETTEUR	DESTINATAIRES	COPIES	
CERTINOMIS	PUBLIC		
CertiNomis			
Certinomis SA au capital de 40 000 euros. Siège social : 10 avenue Charles de Gaulle 94220 Charenton Le Pont – France. RCS Créteil B 433 998 903			
Historique des versions			
DATE	VERSION	EVOLUTION	AUTEUR
06/11/2008	1.0	Version publique	Franck Leroy
14/01/2009	1.1	Intégration RGS_A v2.2	Franck Leroy
14/01/2010	1.2	Intégration RGS_A v2.3	Franck Leroy

TABLE DES MATIERES

1	INTRODUCTION	9
1.1	PRESENTATION GENERALE	9
1.2	IDENTIFICATION DU DOCUMENT	10
1.3	ENTITES INTERVENANT DANS L'IGC	10
1.3.1	AUTORITES DE CERTIFICATION RACINE	10
1.3.2	AUTORITE D'ENREGISTREMENT	11
1.3.3	AUTORITE DE CERTIFICATION DELEGUEE	12
1.3.4	UTILISATEURS DE CERTIFICATS	12
1.3.5	AUTRES PARTICIPANTS	12
1.4	USAGE DES CERTIFICATS	13
1.4.1	DOMAINES D'UTILISATION APPLICABLES	13
1.4.2	DOMAINES D'UTILISATION INTERDITS	13
1.5	GESTION DE LA PC	14
1.5.1	ENTITE GERANT LA PC	14
1.5.2	POINT DE CONTACT	14
1.5.3	ENTITE DETERMINANT LA CONFORMITE D'UNE DPC AVEC CETTE PC	14
1.5.4	PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPC	14
1.6	DEFINITIONS ET ACRONYMES	14
1.6.1	ACRONYMES	14
1.6.2	DEFINITIONS	15
2	RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	17
2.1	ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS	17
2.2	INFORMATIONS DEVANT ETRE PUBLIEES	17
2.3	DELAIS ET FREQUENCES DE PUBLICATION	18
2.4	CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES	18
3	IDENTIFICATION ET AUTHENTIFICATION	19
3.1	NOMMAGE	19
3.1.1	TYPES DE NOMS	19
3.1.2	NECESSITE D'UTILISATION DE NOMS EXPLICITES	19
3.1.3	ANONYMISATION OU PSEUDONYMISATION DES IDENTITES	19
3.1.4	REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOM	19
3.1.5	UNICITE DES NOMS	20
3.1.6	IDENTIFICATION, AUTHENTIFICATION ET ROLE DES MARQUES DEPOSEES	20
3.2	VALIDATION INITIALE DE L'IDENTITE	20
3.2.1	METHODE POUR PROUVER LA POSSESSION DE LA CLE PRIVEE	20
3.2.2	VALIDATION DE L'IDENTITE D'UN ORGANISME	20
3.2.3	VALIDATION DE L'IDENTITE D'UN INDIVIDU	20
3.2.4	INFORMATIONS NON VERIFIEES	20
3.2.5	VALIDATION DE L'AUTORITE DU DEMANDEUR	21
3.2.6	CRITERES D'INTEROPERABILITE	21
3.3	IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES	21
3.3.1	IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT	21
3.3.2	IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION	21
3.4	IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION	21
4	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	22

4.1	DEMANDE DE CERTIFICAT	22
4.1.1	ORIGINE D'UNE DEMANDE DE CERTIFICAT	22
4.1.2	PROCESSUS ET RESPONSABILITES POUR L'ETABLISSEMENT D'UNE DEMANDE DE CERTIFICAT	22
4.2	TRAITEMENT D'UNE DEMANDE DE CERTIFICAT	22
4.2.1	EXECUTION DES PROCESSUS D'IDENTIFICATION ET DE VALIDATION DE LA DEMANDE.....	22
4.2.2	ACCEPTATION OU REJET DE LA DEMANDE.....	22
4.2.3	DUREE D'ETABLISSEMENT DU CERTIFICAT	22
4.3	DELIVRANCE DU CERTIFICAT.....	23
4.3.1	ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT	23
4.3.2	NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT AU BENEFICIAIRE	23
4.4	ACCEPTATION DU CERTIFICAT	23
4.4.1	DEMARCHE D'ACCEPTATION DU CERTIFICAT	23
4.4.2	PUBLICATION DU CERTIFICAT	23
4.4.3	NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT	23
4.5	USAGES DE LA BI-CLE ET DU CERTIFICAT	23
4.5.1	UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE BENEFICIAIRE	23
4.5.2	UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR L'UTILISATEUR DU CERTIFICAT	24
4.6	RENOUVELLEMENT D'UN CERTIFICAT	24
4.6.1	CAUSES POSSIBLES DE RENOUVELLEMENT D'UN CERTIFICAT	24
4.6.2	ORIGINE D'UNE DEMANDE DE RENOUVELLEMENT	24
4.6.3	PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE RENOUVELLEMENT	24
4.6.4	NOTIFICATION AU BENEFICIAIRE DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT	24
4.6.5	DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT.....	24
4.6.6	PUBLICATION DU NOUVEAU CERTIFICAT.....	24
4.6.7	NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT	25
4.7	DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE	25
4.7.1	CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE	25
4.7.2	ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT	25
4.7.3	PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT	25
4.7.4	NOTIFICATION AU BENEFICIAIRE DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT	25
4.7.5	DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT.....	25
4.7.6	PUBLICATION DU NOUVEAU CERTIFICAT.....	25
4.7.7	NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT	25
4.8	MODIFICATION DU CERTIFICAT	26
4.8.1	CAUSES POSSIBLES DE MODIFICATION D'UN CERTIFICAT	26
4.8.2	ORIGINE D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT	26
4.8.3	PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT.....	26
4.8.4	NOTIFICATION AU BENEFICIAIRE DE L'ETABLISSEMENT DU CERTIFICAT MODIFIE.....	26
4.8.5	DEMARCHE D'ACCEPTATION DU CERTIFICAT MODIFIE.....	26
4.8.6	PUBLICATION DU CERTIFICAT MODIFIE.....	26
4.8.7	NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT MODIFIE	26
4.9	REVOCACTION ET SUSPENSION DES CERTIFICATS	26
4.9.1	CAUSES POSSIBLES D'UNE REVOCACTION	26
4.9.2	ORIGINE D'UNE DEMANDE DE REVOCACTION.....	27
4.9.3	PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCACTION	28
4.9.4	DELAI ACCORDE AU BENEFICIAIRE POUR FORMULER LA DEMANDE DE REVOCACTION	28
4.9.5	DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCACTION	29
4.9.6	EXIGENCES DE VERIFICATION DE LA REVOCACTION PAR LES UTILISATEURS DE CERTIFICATS.....	29
4.9.7	FREQUENCE D'ETABLISSEMENT DES LCR/LAR	29
4.9.8	DELAI MAXIMUM DE PUBLICATION D'UNE LCR/LAR.....	29
4.9.9	DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCACTION ET DE L'ETAT DES CERTIFICATS.....	29

4.9.10	EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION DES CERTIFICATS PAR LES UTILISATEURS DE CERTIFICATS	30
4.9.11	AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS	30
4.9.12	EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE.....	30
4.9.13	CAUSES POSSIBLES D'UNE SUSPENSION	30
4.9.14	ORIGINE D'UNE DEMANDE DE SUSPENSION.....	30
4.9.15	PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION.....	30
4.9.16	LIMITES DE LA PERIODE DE SUSPENSION D'UN CERTIFICAT	30
4.10	FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS	30
4.10.1	CARACTERISTIQUES OPERATIONNELLES	30
4.10.2	DISPONIBILITE DE LA FONCTION.....	31
4.10.3	DISPOSITIFS OPTIONNELS.....	31
4.11	FIN DE LA RELATION ENTRE L'ACD ET L'ACR	31
4.12	SEQUESTRE DE CLE ET RECOUVREMENT	31
4.12.1	POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES	31
4.12.2	POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR ENCAPSULATION DES CLES DE SESSION.....	31
5	MESURES DE SECURITE NON TECHNIQUES	32
5.1	MESURES DE SECURITE PHYSIQUE	32
5.1.1	SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES	32
5.1.2	ACCES PHYSIQUE	32
5.1.3	ALIMENTATION ELECTRIQUE ET CLIMATISATION	32
5.1.4	VULNERABILITE AUX DEGATS DES EAUX	33
5.1.5	PREVENTION ET PROTECTION INCENDIE	33
5.1.6	CONSERVATION DES SUPPORTS.....	33
5.1.7	MISE HORS SERVICE DES SUPPORTS	33
5.1.8	SAUVEGARDES HORS SITE	33
5.2	MESURES DE SECURITE PROCEDURALES.....	34
5.2.1	ROLES DE CONFIANCE.....	34
5.2.2	NOMBRE DE PERSONNES REQUISES PAR TACHES.....	34
5.2.3	IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE.....	34
5.2.4	ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS	35
5.3	MESURES DE SECURITE VIS-A-VIS DU PERSONNEL	35
5.3.1	QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES	35
5.3.2	PROCEDURES DE VERIFICATION DES ANTECEDENTS	35
5.3.3	EXIGENCES EN MATIERE DE FORMATION INITIALE	36
5.3.4	EXIGENCES ET FREQUENCE EN MATIERE DE FORMATION CONTINUE	36
5.3.5	FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS.....	36
5.3.6	SANCTIONS EN CAS D' ACTIONS NON AUTORISEES	36
5.3.7	EXIGENCES VIS-A-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES.....	37
5.3.8	DOCUMENTATION FOURNIE AU PERSONNEL	37
5.4	PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT	37
5.4.1	TYPE D'EVENEMENTS A ENREGISTRER	37
5.4.2	FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS	38
5.4.3	PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS.....	38
5.4.4	PROTECTION DES JOURNAUX D'EVENEMENTS	38
5.4.5	PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS	38
5.4.6	SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS.....	38
5.4.7	NOTIFICATION DE L'ENREGISTREMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT	38
5.4.8	EVALUATION DES VULNERABILITES	39
5.5	ARCHIVAGE DES DONNEES	39
5.5.1	TYPES DE DONNEES A ARCHIVER.....	39
5.5.2	PERIODE DE CONSERVATION DES ARCHIVES.....	39

5.5.3	PROTECTION DES ARCHIVES	39
5.5.4	PROCEDURE DE SAUVEGARDE DES ARCHIVES	40
5.5.5	EXIGENCES D'HORODATAGE DES DONNEES	40
5.5.6	SYSTEME DE COLLECTE DES ARCHIVES.....	40
5.5.7	PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES	40
5.6	CHANGEMENT DE CLE D'ACR.....	40
5.7	REPRISE SUITE A COMPROMISSION ET SINISTRE.....	41
5.7.1	PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS	41
5.7.2	PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET / OU DONNEES).....	41
5.7.3	PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE D'UNE COMPOSANTE.....	41
5.7.4	CAPACITES DE CONTINUTE D'ACTIVITE SUITE A UN SINISTRE	42
5.8	FIN DE VIE DE L'IGC.....	42
5.8.1	FIN DES ACTIVITES D'UNE ACR.....	42
5.8.2	FIN DE CONTRAT.....	42
6	MESURES DE SECURITE TECHNIQUES.....	43
6.1	GENERATION ET INSTALLATION DE BI CLES	43
6.1.1	GENERATION DES BI-CLES	43
6.1.2	TRANSMISSION DE LA CLE PRIVEE A L'ACD	44
6.1.3	TRANSMISSION DE LA CLE PUBLIQUE A L'ACR	44
6.1.4	TRANSMISSION DE LA CLE PUBLIQUE DE L'ACR AUX UTILISATEURS DE CERTIFICATS.....	44
6.1.5	TAILLES DES CLES	44
6.1.6	VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE.....	45
6.1.7	OBJECTIFS D'USAGE DE LA CLE	45
6.2	MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES.....	45
6.2.1	STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES	45
6.2.2	CONTROLE DE LA CLE PRIVEE PAR PLUSIEURS PERSONNES	46
6.2.3	SEQUESTRE DE LA CLE PRIVEE.....	46
6.2.4	COPIE DE SECOURS DE LA CLE PRIVEE.....	46
6.2.5	ARCHIVAGE DE LA CLE PRIVEE	46
6.2.6	TRANSFERT DE LA CLE PRIVEE VERS / DEPUIS LE MODULE CRYPTOGRAPHIQUE	46
6.2.7	STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE.....	46
6.2.8	METHODE D'ACTIVATION DE LA CLE PRIVEE	47
6.2.9	METHODE DE DESACTIVATION DE LA CLE PRIVEE.....	47
6.2.10	METHODE DE DESTRUCTION DES CLES PRIVEES	48
6.2.11	NIVEAU D'EVALUATION SECURITE DU MODULE CRYPTOGRAPHIQUE	48
6.3	AUTRES ASPECTS DE LA GESTION DES BI-CLES	48
6.3.1	ARCHIVAGE DES CLES PUBLIQUES	48
6.3.2	DUREES DE VIE DES BI-CLES ET DES CERTIFICATS.....	48
6.4	DONNEES D'ACTIVATION	49
6.4.1	GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION.....	49
6.4.2	PROTECTION DES DONNEES D'ACTIVATION	49
6.4.3	AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION	49
6.5	MESURES DE SECURITE DES SYSTEMES INFORMATIQUES	50
6.5.1	EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES INFORMATIQUES	50
6.5.2	NIVEAU D'EVALUATION SECURITE DES SYSTEMES INFORMATIQUES	50
6.6	MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE	50
6.6.1	MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES	50
6.6.2	MESURES LIEES A LA GESTION DE LA SECURITE	50
6.6.3	NIVEAU D'EVALUATION SECURITE DU CYCLE DE VIE DES SYSTEMES.....	51
6.7	MESURES DE SECURITE RESEAU.....	51
6.8	HORODATAGE / SYSTEME DE DATATION	51

7	PROFILS DES CERTIFICATS, OCSP ET DES LCR.....	52
7.1	PROFIL DES CERTIFICATS D'ACR.....	52
7.2	PROFIL DES CERTIFICATS D'ACD.....	52
7.3	PROFIL DES LCR/LAR.....	52
7.4	PROFIL OCSP	53
7.4.1	NUMERO DE VERSION	53
7.4.2	EXTENSIONS OCSP	53
8	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS.....	54
8.1	FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS	54
8.2	IDENTITES / QUALIFICATIONS DES EVALUATEURS.....	54
8.3	RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES	54
8.4	SUJETS COUVERTS PAR LES EVALUATIONS	54
8.5	ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS	54
8.6	COMMUNICATION DES RESULTATS	55
9	AUTRES PROBLEMATIQUES METIERS ET LEGALES	56
9.1	TARIFS	56
9.1.1	TARIFS POUR LA FOURNITURE OU LE RENOUELEMENT DE CERTIFICATS	56
9.1.2	TARIFS POUR ACCEDER AUX CERTIFICATS	56
9.1.3	TARIFS POUR ACCEDER AUX INFORMATIONS D'ETAT ET DE REVOCATION DES CERTIFICATS	56
9.1.4	TARIFS POUR D'AUTRES SERVICES	56
9.1.5	POLITIQUE DE REMBOURSEMENT.....	56
9.2	RESPONSABILITE FINANCIERE.....	56
9.2.1	COUVERTURE PAR LES ASSURANCES.....	56
9.2.2	AUTRES RESSOURCES	56
9.2.3	COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES.....	57
9.3	CONFIDENTIALITE DES DONNEES PROFESSIONNELLES.....	57
9.3.1	PERIMETRE DES INFORMATIONS CONFIDENTIELLES	57
9.3.2	INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES	57
9.3.3	RESPONSABILITES EN TERME DE PROTECTION DES INFORMATIONS CONFIDENTIELLES	57
9.4	PROTECTION DES DONNEES PERSONNELLES	57
9.4.1	POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES	57
9.4.2	INFORMATIONS A CARACTERE PERSONNEL	58
9.4.3	INFORMATIONS A CARACTERE NON PERSONNEL	58
9.4.4	RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES	58
9.4.5	NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES	58
9.4.6	CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES JUDICIAIRES OU ADMINISTRATIVES	58
9.4.7	AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES	58
9.5	DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE.....	59
9.6	INTERPRETATIONS CONTRACTUELLES ET GARANTIES	59
9.6.1	AUTORITES DE CERTIFICATION RACINE	59
9.6.2	SERVICE D'ENREGISTREMENT	60
9.6.3	BENEFICIAIRE DE CERTIFICATS.....	61
9.6.4	UTILISATEURS DE CERTIFICATS	61
9.6.5	AUTRES PARTICIPANTS	62
9.7	LIMITE DE GARANTIE	62
9.8	LIMITE DE RESPONSABILITE	63
9.9	INDEMNITES	63
9.10	DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC	63
9.10.1	DUREE DE VALIDITE	63
9.10.2	FIN ANTICIPEE DE VALIDITE	63

9.10.3	EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES	63
9.11	NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS	63
9.12	AMENDEMENTS A LA PC	63
9.12.1	PROCEDURES D'AMENDEMENTS	64
9.12.2	MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS	64
9.12.3	CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE	64
9.13	DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS	65
9.14	JURIDICTIONS COMPETENTES	65
9.15	CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS	65
9.16	DISPOSITIONS DIVERSES	65
9.16.1	ACCORD GLOBAL	65
9.16.2	TRANSFERT D'ACTIVITES	65
9.16.3	CONSEQUENCES D'UNE CLAUSE NON VALIDE	65
9.16.4	APPLICATION ET RENONCIATION	65
9.16.5	FORCE MAJEURE	66
9.17	AUTRES DISPOSITIONS	66
9.17.1	DISPOSITIONS PENALES	66
10	ANNEXE 1 : DOCUMENTS CITES EN REFERENCE	67
10.1	REGLEMENTATION	67
10.2	DOCUMENTS TECHNIQUES	67
11	ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'ACR.....	69
11.1	EXIGENCES SUR LES OBJECTIFS DE SECURITE	69
11.2	EXIGENCES SUR LA QUALIFICATION	69
12	ANNEXE 3 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'ACD.....	70
12.1	EXIGENCES SUR LES OBJECTIFS DE SECURITE	70
12.2	EXIGENCES SUR LA CERTIFICATION	70

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de CertiNomis. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisées préalablement par écrit par CertiNomis ou ses ayants droit, sont strictement interdites.

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

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

La Déclaration des Pratiques de Certification, propriété de la société CertiNomis peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

1 INTRODUCTION

1.1 PRESENTATION GENERALE

Une Infrastructure à Clé Publique (IGC) est un ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques.

La mise en place d'une IGC, nécessaire à la sécurité et à la confiance, ouvre une palette de services à valeur ajoutée pour les transactions électroniques (par exemple : courrier électronique, transactions commerciales, téléprocédures, protection locale des données, etc.).

Ils ont pour fonction d'assurer :

- l'intégrité des messages ;
- l'identification et l'authentification¹ ;
- la non répudiation de l'origine ;
- et la confidentialité.

La Politique de Certification définie dans le présent document est destinée à être utilisée par les entreprises, les associations, les ministères, les entités administratives ou gouvernementales et groupements de toute sorte, ainsi que les individus. Les personnes qui consultent et utilisent ce document peuvent s'informer auprès de l'AC émettrice afin d'obtenir plus de détails sur sa mise en œuvre.

La Politique de Certification couvre la gestion et l'utilisation de certificats, selon leurs classes, contenant les clés publiques servant aux fonctions de vérification, d'authentification, d'intégrité et de concordance des clés. Par exemple, les certificats délivrés en vertu de la présente politique pourraient servir à vérifier l'identité des correspondants s'échangeant du courrier électronique ou permettre l'accès distant à un système d'information, vérifier l'identité des individus ou d'autres personnes morales (de droit privée et de droit public), ou encore préserver l'intégrité des serveurs, des logiciels et des documents.

La Politique de Certification couvre aussi la gestion et l'utilisation de certificats contenant les clés publiques servant aux fonctions de confidentialité. Les certificats délivrés en vertu de la présente politique permettent d'assurer le secret d'informations, considérées comme privées ou sensibles par leur propriétaire, dans certaines applications comme le courrier électronique ou les communications par le Web. Les certificats ne servent pas à protéger les renseignements classifiés.

La délivrance d'un certificat de clé publique en vertu de la présente politique ne signifie pas que le client ou le bénéficiaire soit autorisé de quelque façon que ce soit à faire des transactions commerciales, ou autres, au nom de l'organisation qui exploite l'ACR.

L'ACR sera assujettie aux lois et règlements en vigueur sur le territoire de la République française, ainsi qu'aux normes européennes en vigueur et aux conventions internationales ratifiées par la France, et qui touchent à l'application, l'élaboration, l'interprétation et la validité des politiques de certification mentionnées dans le présent document.

L'ACR se réserve le droit de ne pas conclure d'accord de certification croisée avec une autorité de certification externe.

¹ Etant précisé que ce n'est pas au sens des actes authentiques, tels qu'ils sont régis par les articles 1317 et suivants du code civil, mais au sens technique d'authentification cryptographique

1.2 IDENTIFICATION DU DOCUMENT

Autorité de Certification Racine
<i>Politique de Certification</i>
<p>La désignation du numéro d'identification d'objet (OID) pour la présente politique est :</p> <p style="text-align: center;">1.2.250.1.86.2.2.0.1.1</p>

1.3 ENTITES INTERVENANT DANS L'IGC

Lorsqu'un prestataire fournit des services de certification, à savoir qu'il délivre des certificats ou qu'il fournit d'autres services liés aux signatures numériques, il convient de distinguer plusieurs métiers ou fonctions, desquels découlent des rôles et des responsabilités distincts.

Le processus de certification et la gestion du cycle de vie du certificat font appel à une grande diversité d'intervenants dans la chaîne de la confiance :

- Autorité de certification Racine,
- Autorité de certification Déléguée ; bénéficiaire des services de l'ACR,
- Autorité d'enregistrement,
- Sujet du certificat délivré par l'Autorité de Certification Racine,
- Tiers utilisateurs.

1.3.1 Autorités de Certification Racine

L'Autorité de Certification Racine (ACR) est responsable vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. A ce titre, elle édicte la Politique de Certification et valide les Déclarations de Pratique de Certification respectées par les différentes composantes de l'Infrastructure à Clé Publique.

La garantie apportée par l'Autorité de Certification Racine vient de la qualité de la technologie mise en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.

L'ACR a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

Les prestations de l'ACR sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats (cf. ci-dessous).

Autorité d'enregistrement (AE) - Cette fonction vérifie les informations d'identification du futur sujet d'une Autorité de Certification Déléguée, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC (cf. ci-dessous). L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du sujet du certificat lors du renouvellement du certificat de celui-ci.

Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'ACR) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du sujet provenant soit du bénéficiaire, soit de la fonction de génération des éléments secrets du bénéficiaire, si c'est cette dernière qui génère la bi-clé du certificat.

Fonction de génération des éléments secrets - Cette fonction génère les éléments secrets à destination de l'autorité déléguée, et les prépare en vue de leur remise. Ces éléments secrets sont directement la bi-clé du certificat, les codes (activation / déblocage) sont liés au dispositif de stockage de la clé privée de l'autorité déléguée.

Fonction de remise - Cette fonction remet à l'ACD au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'ACR (dispositif cryptographique, clé privée, codes d'activation,...).

Fonction de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'ACR, les certificats d'ACR et toute autre information pertinente destinée aux bénéficiaires et/ou aux utilisateurs de certificats, hors informations d'état des certificats.

Fonction de gestion des révocations - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers : LAR.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

Autorité de Certification Déléguée (ACD) - L'autorité identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.

Utilisateur de certificat - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du bénéficiaire du certificat.

Dans le cadre de ses fonctions opérationnelles, les exigences qui incombent à l'ACR en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Etre une entité légale au sens de la loi française.
- Etre en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des bénéficiaires de cette entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux bénéficiaires, aux utilisateurs de certificats,... qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mener une analyse de risque permettant 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. Elle élabore sa DPC en fonction de cette analyse.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions de la présente PC, notamment en matière de génération des certificats, de remise au bénéficiaire, de gestion des révocations et d'information sur l'état des certificats.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR). Diffuser ses certificats d'ACR aux utilisateurs de certificats.

1.3.2 Autorité d'enregistrement

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification Racine et l'Autorité de Certification Déléguée.

L'AE traite les demandes de certification et de révocation après en avoir vérifié la recevabilité ainsi que la complétude des dossiers. L'AE rend compte à l'ACR en cas de litige sur la recevabilité des demandes de certification, et systématiquement en cas de demande de révocation.

Sa responsabilité ne peut être engagée que par l'ACR. L'Autorité de Certification Racine a un devoir de contrôle et d'audit des Autorités d'Enregistrement.

1.3.3 Autorité de Certification Déléguée

L'autorité de Certification Déléguée utilise sa clé privée et le certificat correspondant dans le cadre de ses activités d'autorité de certification auprès de ses clients.

Certinomis peut opérer l'IGC de l'ACD ou cette ACD peut être opérée par ses propres moyens.

Dans tous les cas, l'ACD fournit sa PC/DPC à l'ACR. Si l'ACD possède sa propre DPC, celle-ci sera revue par l'ACR pour s'assurer de la cohérence avec les exigences de la PC de l'ACD et de l'ACR.

L'ACD doit déclarer à l'ACR les types de certificats émis, l'ACR s'assure que les types de certificats émis sont compatibles avec les PC de l'ACD et de l'ACR.

1.3.4 Utilisateurs de certificats

Avant d'accorder sa confiance au dit certificat, le tiers utilisateur doit impérativement vérifier sa validité auprès de Certinomis en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant sa validité intrinsèque, en particulier sa date d'expiration et sa signature, et la validité de tout certificat sur l'itinéraire de confiance. A défaut de remplir cette obligation, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, Certinomis ne garantissant, dès lors, plus aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

1.3.5 Autres participants

1.3.5.1 Composantes de l'IGC

La décomposition fonctionnelle de L'IGC est décrite dans la DPC

1.4 USAGE DES CERTIFICATS

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats émis

Les certificats émis en vertu de la présente politique sont appropriés pour établir le lien qui existe entre une identité et une clé publique.

Autorité de Certification Racine
<i>Usage du certificat</i>
<p>L'Autorité de Certification Racine signe son propre certificat X.509 d'AC (certificat auto-signé). L'ACR signe les certificats des AC Déléguées ainsi que la liste des certificats des AC Déléguées révoquées.</p> <p>Le certificat de l'ACR est utilisé par les utilisateurs pour vérifier l'authenticité d'une ACD.</p>

1.4.1.2 Bi-clés et certificats d'ACR et de composantes

L'ACR génère et signe différents types d'objets : certificats, LCR / LAR.

Pour signer ces objets, l'ACR dispose d'une bi-clé.

L'ACR dispose d'une seule bi-clé et le certificat correspondant est auto-signé.

Les bi-clés et certificats de l'ACR sont utilisés pour la signature de certificats, de LCR / LAR et uniquement utilisés qu'à cette fin. Ils ne sont pas utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

1.4.2 Domaines d'utilisation interdits

Aucunes utilisations autres que celles définies dans les chapitres 1.4.1.1 et 1.4.1.2 ne sont couvertes par la présente PC.

Une ACD dont le certificat est émis par l'ACR n'est pas autorisée à :

- Emettre des certificats non compatibles X.509
- De fournir des fonctions qui ne sont pas couvertes par la présente PC.
- De fournir des services qui ne sont pas déclarés dans la PC de l'ACD au moment de la signature du certificat de l'ACD. Sauf à mettre à jour la PC de l'ACD et d'en informer l'ACR pour approbation.

1.5 GESTION DE LA PC

1.5.1 Entité gérant la PC

La présente politique de certification est sous la responsabilité de la société Certinomis.

1.5.2 Point de contact

Le directeur général de Certinomis
10 avenue Charles de Gaulle
94220 Charenton Le Pont

Téléphone : (33) (0)1.56.29.72.60

Télécopieur : (33) (0)1. 56.29.72.67

Courrier électronique : politiquecertification@certinomis.com

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

La Direction de Certinomis détermine la conformité de la DPC avec la présente politique de certification, soit directement soit indirectement en faisant appel à des experts indépendants spécialisés dans le domaine de la sécurité et des IGC.

1.5.4 Procédures d'approbation de la conformité de la DPC

L'ACR est garante de l'application de la DPC avec la Politique de Certification.

L'ACR est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC suit le processus d'approbation mis en place. Toute nouvelle version de la DPC est publiée, conformément aux exigences du paragraphe 2.2 sans délai.

Une AGP peut demander l'examen de la DPC conformément aux procédures en vigueur.

1.6 DEFINITIONS ET ACRONYMES

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- ACD Autorité de Certification Déléguée
- ACR Autorité de Certification Racine
- AE Autorité d'Enregistrement
- AGP Autorité de Gestion des Politiques
- AH Autorité d'Horodatage
- DN Distinguished Name
- DPC Déclaration des Pratiques de Certification
- ETSI European Telecommunications Standards Institute
- IGC Infrastructure de Gestion de Clés.
- LAR Liste des certificats d'AC Révoqués
- LCR Liste des Certificats Révoqués

- OID Object Identifier
- PC Politique de Certification
- PSCE Prestataire de Services de Certification Electronique
- PSCo Prestataire de Services de Confiance
- RSA Rivest Shamir Adelman
- SP Service de Publication
- SSI Sécurité des Systèmes d'Information
- URL Uniform Resource Locator

1.6.2 Définitions

Autorité de Certification (AC) :

Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuier" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Autorité d'enregistrement (AE) : Cf. chapitre 1.3.1.

Autorité de Gestion de la Politique (AGP) :

L'Autorité de Gestion de la Politique, pour les usages qui la concerne, établit les besoins et les exigences en termes de sécurité dans l'ensemble du processus de certification et d'utilisation des certificats. Elle établit des lignes directrices, qui peuvent prendre la forme d'un canevas de Politique de Certification, que doivent respecter toutes les Autorités de Certification qu'elle accrédite. Elle valide et suit toute évolution des politiques de certification des Autorités de Certification qu'elle accrédite.

Son rôle est celui d'une autorité morale qui indique par l'accréditation la confiance que l'on peut accorder à une Autorité de Certification.

Certificat :

Attestation électronique liant les données afférentes au chiffrement ou à la vérification de signature, des échanges, messages et documents électroniques à un sujet, afin d'en assurer la confidentialité ou d'en assurer l'authentification et l'intégrité.

Sujet :

Identités portées dans le certificat. Le sujet peut contenir l'identité d'une personne, d'un serveur, d'une organisation.

Politique de Certification (PC) :

Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les bénéficiaires et les utilisateurs de certificats.

Déclaration des Pratiques de Certification (DPC) :

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

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des bénéficiaires et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Déléguées). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

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

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

La fonction de publication de l'ACR met à disposition l'information sur l'état des certificats par le biais de fichier « LAR ».

La LAR de l'ACR est accessible par internet suivant 2 protocoles :

- HTTP sur le serveur crl.certinomis.com
- LDAP sur le serveur ldap.certinomis.com

Les liens exacts sont définis dans l'extension « Point de distribution de la LCR » de chaque certificat émis par l'ACR.

Les LAR sont aussi accessibles en téléchargement, directement sur le serveur WEB public : www.certinomis.com dans la rubrique « Vérifiez un certificat ».

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

La Politique de Certification, les parties publiques de la DPC, les certificats d'ACR, sont soit disponibles sur le site WEB de l'ACR à l'adresse suivante <http://www.certinomis.com>, soit communiqués dans le cadre de la négociation commerciale.

Une copie peut également être obtenue par courrier électronique.

Les procédures, qui donnent, entre autres, le détail des moyens mis en œuvre pour assurer la protection des installations de l'ACR, ne sont pas publiées pour des raisons de sécurité liées au besoin d'en connaître.

Toutefois, l'ACR peut fournir, autant que de besoin, la liste complète des procédures, lors d'une demande d'un organisme autorisé (AGP, autre AC pour certification croisée...) à des fins de vérification, d'audit ou de contrôle, prévues à cet effet dans la présente déclaration, ainsi que dans le cadre du respect de la loi.

Si la DPC contient des informations touchant la sécurité de l'ACR ou des informations qu'elles considèrent confidentielles, la publication n'est pas effectuée. Il est possible de d'obtenir sur demande expresse un résumé ou des extraits de la DPC sous forme électronique.

La Liste des Certificats Révoqués est fournie par l'ACR qui en assure la publication sur son site public, dans la limite des éléments autorisés par ses clients et bénéficiaires.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les délais et les fréquences de publication dépendent des informations concernées :

Autorité de Certification Racine
<i>Délais de publication</i>
<p>Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'ACR.</p> <p>Pour les certificats d'ACR, ils sont diffusés préalablement à toute émission de certificats et/ou de LCR correspondants sous délai de 24 heures.</p> <p>Le site web de publication est disponible 24/24 ; 7/7.</p> <p>Pour les informations d'état des certificats d'ACD, les Listes de Certificats Révoqués seront mises à jour annuellement. Une fois la mise à jour effectuée, la LCR est publiée dans un délai maximum de 24 heures.</p>

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (authentification par certificat sur support).

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion des mots de passe.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509] l'ACR (issuer) et l'ACD (subject) sont identifiés par un "Distinguished Name" (DN) de type [X.501].

Des règles sur la construction du DN de ces champs sont précisées dans la DPC.

3.1.2 Nécessité d'utilisation de noms explicites

Le contenu des champs de nom Subject doit avoir un lien explicite avec l'ACD authentifiée.

Autorité de Certification Racine
<i>Noms explicites</i>
<p>Un nom distinctif doit contenir de manière obligatoire les champs suivants :</p> <ul style="list-style-type: none"> • le champ Country (C) ; • le champ Organisation (O) ; • le champ Organisational Unit (OU). • le champ Common Name (CN) ;

L'ACR définit sa politique de nommage et, à ce titre, elle se réserve le droit de prendre toutes décisions concernant les noms des organisations, qu'elles soient de droit public ou de droit privé, et de toutes autres entités identifiées dans le cadre des certificats signés. Une partie demandant un certificat doit être en mesure de prouver qu'elle a le droit d'utiliser un nom en particulier.

Une partie qui demande un certificat doit avoir le droit d'utiliser le nom qu'elle souhaite y voir figurer.

En cas de différend au sujet d'un nom dans un dépôt de documents dont elle n'a pas le contrôle, l'ACR s'assure qu'il existe, dans le contrat associé à ce dépôt, une procédure de règlement des différends au sujet des noms.

Toute AC déléguée est tenue de suivre et d'appliquer la politique de nommage de son AC Racine, si elle le demande.

3.1.3 Anonymisation ou pseudonymisation des identités

Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes.

L'identifiant de l'entité dans son certificat ne peut être un pseudonyme.

3.1.4 Règles d'interprétation des différentes formes de nom

Le document [PROFILS] fournit des règles à ce sujet.

3.1.5 Unicité des noms

Les noms distinctifs sont uniques pour toutes les entités identifiées d'une ACD.

3.1.6 Identification, authentification et rôle des marques déposées

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

L'ACR ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par les clients et bénéficiaires des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1 Méthode pour prouver la possession de la clé privée

Lorsque l'ACR ne génère pas les clés des ACD, celle-ci vérifie que le demandeur est véritablement en possession de la clé privée associée à la clé publique qui a été inscrite dans son certificat. Cette vérification peut être réalisée à partir d'un paquet de demande de certificat au standard PKCS#10 par vérification de la preuve de possession.

3.2.2 Validation de l'identité d'un organisme

L'AE vérifie l'identification de l'organisation, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'ACR ou de l'AE.

Lors de l'enregistrement, l'organisation doit apporter la preuve de son existence, la preuve de l'identité de son représentant légal ainsi que la chaîne des mandats conférant leur pouvoir aux mandataires de certification.

L'ACR ou l'AE archive toutes les informations pertinentes relatives à cet enregistrement.

La DPC précise les documents à fournir et les procédures d'enregistrement mises en œuvre par l'AE, en concertation avec l'ACR.

3.2.3 Validation de l'identité d'un individu

Sans objet.

3.2.4 Informations non vérifiées

Les certificats émis sous la présente PC ne comportent aucune information non vérifiée.

3.2.5 Validation de l'autorité du demandeur

Sans objet.

3.2.6 Critères d'interopérabilité

Il n'est prévu aucune interopérabilité avec d'autres AC.

3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUELEMENT DES CLES

Le renouvellement de la bi-clé d'un certificat entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni à l'ACD sans renouvellement de la bi-clé correspondante (cf. chapitre 5.6).

3.3.1 Identification et validation pour un renouvellement courant

Le renouvellement courant ne peut être demandé que par l'organisation ayant demandée initialement le certificat d'ACD.

Le renouvellement du certificat d'ACD se fait selon la procédure de Cérémonie de Clés détaillée dans la DPC de l'ACR.

3.3.2 Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, le renouvellement ne peut plus être effectué.

Si l'organisation responsable de l'ACD souhaite continuer l'activité de certification, l'ACD doit changer de nom.

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

La révocation ne peut être demandée que par l'organisation ayant demandée initialement le certificat d'ACD.

La révocation du certificat d'ACD se fait selon la procédure de Cérémonie de Clés détaillée dans la DPC de l'ACR.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

Le présent chapitre définit les pratiques opérationnelles relatives à la gestion des clés et des certificats.

4.1 DEMANDE DE CERTIFICAT

4.1.1 Origine d'une demande de certificat

Un certificat ne peut être demandé que par un représentant légal de l'entité de la future ACD.

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

Un document de spécification doit être établi par l'ACD pour permettre à l'ACR d'établir une procédure de cérémonie des clés.

Cette procédure décrit les conditions d'utilisation de la clé privée de l'ACR afin de signer le certificat de l'ACD.

Le gabarit complet du certificat de l'ACD est détaillé dans cette procédure, l'ACR vérifie sa conformité par rapport à la présente PC.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

Une demande de certificat n'oblige en aucune façon l'ACR à émettre un certificat numérique.

L'émission d'un certificat par une AC indique que celle-ci a définitivement et complètement approuvé la demande de certificat selon les procédures décrites dans la DPC.

L'AE conserve ensuite une trace des justificatifs d'identité présentés : sous la forme d'une photocopie signée à la fois par la future ACD et par l'AE, les signatures étant précédées de la mention "copie certifiée conforme à l'original".

4.2.2 Acceptation ou rejet de la demande

A la réception d'une demande de certificat, l'ACR :

- s'assure que la demande a bien été prise en compte par une AE qu'elle a reconnue et que ladite AE a traité la demande et fourni une trace imputable de son avis ;
- génère et signe le certificat.

4.2.3 Durée d'établissement du certificat

Une fois la demande de certificat validée, le certificat est émis suivant un planning déterminé entre les parties.

4.3 DELIVRANCE DU CERTIFICAT

4.3.1 Actions de l'AC concernant la délivrance du certificat

L'ACR vérifie que tous les champs du futur certificat d'ACD sont conformes au document de cérémonie des clés.

L'ACR active la clé privée en utilisant les données d'activation, pour signer le certificat de l'ACD.

La CSR de l'ACD est présentée, l'ACR signe le certificat. Le contenu du certificat d'ACD est vérifié.

L'ACR génère une nouvelle LAR pour publication sur son site web.

L'ACR désactive la clé privée.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

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

Le certificat généré est remis au représentant de l'ACD qui signe le procès verbal de cérémonie des clés.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 Démarche d'acceptation du certificat

La signature du procès verbal de cérémonie des clés vaut acceptation du certificat par l'ACD.

En acceptant un certificat, le bénéficiaire reconnaît expressément consentir aux termes et aux conditions d'utilisation contractuelles et, plus généralement, à tous les éléments publiés dans la Déclaration de Pratiques de Certification et dans la présente Politique de certification de l'ACR.

4.4.2 Publication du certificat

Les certificats émis sont publiés par l'ACR sur son site web.

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

Sans objet.

4.5 USAGES DE LA BI-CLE ET DU CERTIFICAT

4.5.1 Utilisation de la clé privée et du certificat par le bénéficiaire

Les ACD doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé sont par ailleurs indiqués dans le certificat lui-même, via les extensions concernant les usages des clés.

Autorité de Certification Déléguée

Utilisation de la clé privée

L'utilisation de la clé privée de l'ACD et du certificat associé est strictement limitée au service de signature de certificat et signature de liste de révocation.

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

Cf. chapitre précédent et chapitre 1.4.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 RENOUELEMENT D'UN CERTIFICAT

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

La présente PC impose que les certificats et les bi-clés correspondantes aient la même durée de vie, il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au bénéficiaire de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI- CLE

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

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des ACD, et les certificats correspondants, seront renouvelés au minimum tous les sept ans.

Par ailleurs, une bi-clé et un certificat ne pourront pas être renouvelés par anticipation, suite à la révocation du certificat (cf. chapitre 4.9, notamment le chapitre 4.9.1.1 pour les différentes causes possibles de révocation).

4.7.2 Origine d'une demande d'un nouveau certificat

Le traitement est identique à celui de la demande initiale.
Cf. chapitre 4.2.1.

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

Cf. chapitre 4.3.1.

4.7.4 Notification au bénéficiaire de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8 MODIFICATION DU CERTIFICAT

Nota -Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre 4.7) et autres que uniquement la modification des dates de validité (cf. chapitre 4.6).

La modification de certificat n'est pas autorisée dans la présente PC.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.8.4 Notification au bénéficiaire de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats des bénéficiaires

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat de l'ACD :

- les informations du sujet figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- l'ACD n'a pas respectée les modalités applicables d'utilisation du certificat ;
- l'ACD n'a pas respectée ses obligations découlant de la PC de l'ACR ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier de l'ACD.
- la clé privée de l'ACD est suspectée de compromission, est compromise, est perdue ou est volée,
- le représentant légal de l'ACD demande la révocation du certificat ;
- la cessation d'activité de l'entité de l'ACD.

Lorsqu'une des circonstances ci-dessus se réalise et que l'ACR en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

La connaissance de la compromission avérée ou soupçonnée de la clé privée par le client ou le bénéficiaire emporte obligation pour ces derniers de procéder sans délais à la vérification de la révocation du certificat associé et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

La connaissance de la modification d'une information contenue dans le certificat par le client ou le bénéficiaire emporte obligation pour ces derniers de procéder sans délais à la vérification de sa révocation et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

Outre les cas de révocation de certificats mentionnés plus haut, l'ACR peut révoquer le certificat de l'ACD dès lors qu'elle est en possession d'informations de nature à indiquer que la situation de l'ACD a subi des modifications qui ne lui ont pas été transmises par celle-ci, ou qu'elle a des soupçons graves quant à la compromission de la clé privée de l'ACD. Plus généralement, l'ACR peut, à sa discrétion, révoquer le certificat d'une entité identifiée lorsque le client ne respecte pas les obligations énoncées dans la présente politique de certification et dans tous documents contractuels ainsi que dans toute loi et règlement applicable.

4.9.1.2 Certificats d'une composante de l'IGC

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

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

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats des ACD

Seuls peuvent demander la révocation d'un certificat :

- le représentant légal de l'entité de l'ACD ;
- le personnel de l'ACR émettrice ; ou
- le personnel de l'AE qui a enregistré la demande du bénéficiaire.

4.9.2.2 Certificats d'une composante de l'IGC

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

La révocation des autres certificats de composantes est décidée par l'entité responsable de l'ACR.

4.9.3 Procédure de traitement d'une demande de révocation

Les motifs de la révocation d'un certificat donné ne sont jamais divulgués à des tiers sauf en cas d'accord écrit du bénéficiaire ou du client.

Dans le cadre des audits et contrôles auxquels l'ACR est soumise en vertu de la présente politique de certification, des éléments sur les motifs de révocation, non nominatifs et non liés à un certificat, pourront être fournis.

4.9.3.1 Révocation d'un certificat d'ACD

La demande de révocation contient au minimum:

- Le nom de l'entité responsable de l'ACD,
- Les nom/prénom du responsable administratif de l'ACD,
- L'identifiant de l'ACD (Cf. 3.1.1),
- Le numéro de série du certificat de l'ACD,
- La raison de révocation (optionnelle)

L'AE authentifie la demande de révocation.

L'AE transmet la demande à l'ACR.

L'ACR organise une cérémonie des clés pour l'activation des clés privées de l'ACR afin de signer une nouvelle ARL contenant le numéro de série du certificat de l'ACR révoquée.

Les clés privées du certificat de l'ACD sont ensuite détruites.

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

En cas de révocation d'un des certificats de la chaîne de certification, l'ACR informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des bénéficiaires concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE. Ces derniers devront informer les bénéficiaires de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le point de contact identifié sur le site : <http://www.references.modernisation.gouv.fr> est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

4.9.4 Délai accordé au bénéficiaire pour formuler la demande de révocation

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

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

4.9.5.1 Révocation d'un certificat d'ACD

Par nature une demande de révocation est traitée en urgence.

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

Ensuite l'ACR met tous les moyens en œuvre pour signer dans les meilleurs délais la révocation de l'ACD.

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

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'ACR qui a émis le certificat.

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

4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

Avant toute utilisation de certificats, notamment lorsque les dits certificats créent des effets juridiques, le tiers utilisateur doit impérativement vérifier la validité des certificats auxquels elle entend se fier auprès de Certinomis, en consultant les Listes des Certificats Révoqués valides les plus récentes ainsi qu'en contrôlant la validité intrinsèque du certificat, en particulier sa signature, et la validité du certificat de l'émetteur.

La validité d'une LCR est contrôlée par vérification de sa signature et vérification de la validité du certificat de l'émetteur.

4.9.7 Fréquence d'établissement des LCR/LAR

La fréquence de publication des LCR/LAR est au minimum de 12 mois.

Une publication de LCR est effectuée à chaque utilisation de la clé privée de l'ACR (signature ou révocation de certificat d'ACD).

4.9.8 Délai maximum de publication d'une LCR/LAR

La LCR est publiée dans un délai maximum de 24 heures.

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

Une publication complémentaire suivant le protocole LDAP est disponible.

Le service OSCP n'est pas disponible.

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

Cf. chapitre 4.9.6 ci-dessus.

4.9.11 Autres moyens disponibles d'information sur les révocations

Aucun autre moyen n'est disponible.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission avérée ou soupçonnée de la clé privée de signature d'une ACR, l'ACR avise sans tarder toutes les AGP qui l'accréditent.

La connaissance de la compromission avérée ou soupçonnée de la clé privée, par le client ou le bénéficiaire emporte obligation de procéder sans délais à la vérification de la révocation du certificat associé et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

La procédure de révocation d'une ACR est réalisée par une opération de cérémonie de clé, détaillée dans la DPC.

4.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.10.1 Caractéristiques opérationnelles

L'ACR fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est à dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'AC Racine.

Ces LCR / LAR sont des LCR au format V2, publiées au dans un annuaire accessible en protocole LDAP V3 et sur un serveur web accessible en protocole HTTP.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1h et une durée maximale totale d'indisponibilité par mois de 4h.

4.10.3 Dispositifs optionnels

Aucun dispositif optionnel n'est disponible.

4.11 FIN DE LA RELATION ENTRE L'ACD ET L'ACR

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'ACR et l'ACD, avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées d'ACR ne sont pas séquestrées.

Les clés privées des certificats émis ne sont pas séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

Les locaux techniques, qui accueillent les moyens de certification et notamment sa clé privée de signature, sont fortement protégés. Ils sont dans une zone à accès contrôlé, protégée contre tous les risques courants (incendie, inondation...).

Le niveau de protection des locaux techniques est essentiel dans la garantie de la sécurité des moyens de certification et de l'exploitation de ces moyens.

La DPC précise les conditions de sécurité physique et les règles appliquées aux – ainsi que dans les – locaux, en particulier sur les sujets suivants :

- Emplacement, construction et accès physique
- Système électrique et système de conditionnement d'air
- Dégâts causés par l'eau
- Prévention et protection-incendie
- Entreposage des supports
- Mise au rebut du matériel, destruction
- Sauvegarde à l'extérieur des locaux

5.1.1 Situation géographique et construction des sites

La présente PC ne formule pas d'exigence spécifique concernant la localisation géographique.

La construction des sites respecte les règlements et normes en vigueur et le cas échéant, des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...).

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'ACR, les accès aux locaux des différentes composantes de l'IGC sont contrôlés.

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logiques.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Nota -On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

5.1.3 Alimentation électrique et climatisation

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.

Elles permettent également de respecter les exigences de la présente PC, ainsi que les engagements pris par l'ACR dans sa DPC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC, ainsi que les engagements pris par l'ACR dans sa DPC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC, ainsi que les engagements pris par l'ACR dans sa DPC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités de l'IGC ont été identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.

5.1.7 Mise hors service des supports

En fin de vie, les supports devront être soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation sont conformes aux différents niveaux de confidentialité.

5.1.8 Sauvegardes hors site

En complément de sauvegardes sur sites, les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences de la présente PC et aux engagements de l'ACR dans sa DPC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres 4.9.5.1 et 4.10.2).

Les informations sauvegardées hors site respectent les mêmes exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, mettent en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 Rôles de confiance

Chaque composante de l'IGC distingue au moins les cinq rôles fonctionnels de confiance suivants :

Responsable de sécurité - Le responsable de sécurité 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'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

Responsable d'application - Le responsable d'application 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 - Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, l'ACR distingue également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC : cf. chapitres 6.1 et 6.2.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre 6)

La DPC précise les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter.

5.2.3 Identification et authentification pour chaque rôle

Tous les membres du personnel de l'ACR doivent faire vérifier leur identité et leurs autorisations avant :

- que leur nom soit ajouté à la liste d'accès aux locaux de l'ACR ; ou
- que leur nom soit ajouté à la liste des personnes autorisées à accéder physiquement au système de l'ACR.

Tous les intervenants sur le système de l'ACR, ou d'une autre composante de l'IGC, doivent faire vérifier leur identité et leur autorisation avant :

- qu'un certificat leur soit délivré pour accomplir le rôle qui leur est dévolu ; ou
- qu'un compte soit ouvert en leur nom dans le système.

Chacun de ces certificats et comptes (à l'exception des certificats de signatures de l'ACR) :

- est attribué directement à une personne ;
- ne doit pas être partagé ;
- doit être utilisé seulement pour les tâches **autorisées** pour le rôle assigné ; un mécanisme de contrôle est mis en place.

Les opérateurs distants intervenant sur le système de l'ACR doivent être identifiés au moyen de mécanismes cryptographiques forts.

L'ACR et les composantes de l'IGC s'assurent que tout processus de vérification qu'elles utilisent permet de superviser toutes les activités des personnes qui en leur sein détiennent des rôles privilégiés.

5.2.4 Rôles exigeant une séparation des attributions

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

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

Les attributions associées à chaque rôle sont décrites dans la DPC correspondant à cette PC.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

5.3.1 Qualifications, compétences et habilitations requises

Le responsable de l'ACR s'assure que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une ACR, qu'ils dépendent de l'ACR directement, de l'AE :

- sont nommés à un poste faisant l'objet d'une description détaillée par écrit ;
- sont liés par contrat ou par la loi aux postes qu'ils occupent ;
- ont reçu toute la formation nécessaire pour accomplir leurs tâches ;
- sont tenus par contrat ou par la loi de ne pas divulguer de renseignements ayant trait à la sécurité de l'ACR, aux clients ou aux bénéficiaires ; une clause de confidentialité est expressément inscrite dans les contrats de travail des membres du personnel de l'ACR ;

Des obligations identiques sont portées à la charge du responsable de l'AE et d'en communiquer le résultat à l'ACR.

5.3.2 Procédures de vérification des antécédents

Toutes les vérifications des antécédents sont faites conformément à la politique de l'ACR en matière de sécurité.

Le salarié s'engage sur l'honneur sur l'exactitude de toutes les informations fournies lors de la phase d'embauche.

Des obligations identiques sont portées à la charge du responsable de l'AE et d'en communiquer le résultat à l'ACR.

5.3.3 Exigences en matière de formation initiale

L'ACR s'assure que tous les membres du personnel qui accomplissent des tâches touchant à l'exploitation d'une AC ou d'une AE ont reçu une formation complète concernant :

- les principes de fonctionnement et les mécanismes de sécurité de l'ACR ou de l'AE.

Le personnel de l'ACR suit un programme de formation pour accomplir correctement ses fonctions. Il porte :

- sur les différentes applications et versions d'applications auxquelles il pourrait avoir accès dans le cadre de ses fonctions au sein du système de l'ACR ;
- sur toutes les tâches qu'il devra accomplir dans le cadre de l'IGC ;
- sur le matériel et les systèmes d'exploitation formant l'environnement opérationnel de l'ACR ;
- sur le plan de secours de l'ACR après un sinistre et les procédures de maintien des activités.

Avant l'entrée en fonction, il sera procédé à une familiarisation aux règles de sécurité en vigueur.

Des obligations identiques sont portées à la charge de l'AE et de leur personnel.

5.3.4 Exigences et fréquence en matière de formation continue

Les exigences décrites à la section 5.3.3 sont tenues à jour afin de refléter les changements apportés au système de l'ACR.

Des cours de formation professionnelle sont offerts en fonction des besoins, et l'ACR revoit ses exigences au moins une fois par an.

Le personnel de l'ACR participe régulièrement à des séances de formation sur la sécurité.

Des obligations identiques sont portées à la charge de l'AE et de leur personnel.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Aucune exigence particulière.

5.3.6 Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation d'une ACR ou d'une AE, l'ACR peut lui interdire l'accès au système.

En outre, si les faits sont avérés, elle peut prendre toutes sanctions disciplinaires adéquates.

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

L'ACR s'assure que les personnels des entreprises cocontractantes peuvent accéder à ses locaux conformément aux indications de l'article 5.1.1.

Les exigences relatives au personnel des entreprises cocontractantes sont identiques à celles relatives aux employés, en particulier à celles décrites aux articles 5.3, 5.3.2 et 5.3.6.

Des obligations identiques sont portées à la charge du responsable de l'AE et d'en communiquer le résultat à l'ACR.

5.3.8 Documentation fournie au personnel

L'ACR met à la disposition des membres du personnel de l'ACR et de l'AE les Politiques de Certification qu'elle accepte, ainsi que toute loi, toute politique ou tout contrat qui s'appliquent aux postes qu'ils occupent.

Tout le personnel de l'ACR a accès à des manuels complémentaires relatifs à leurs responsabilités. Ces manuels portent sur l'ensemble des procédures en vigueur.

Des obligations identiques sont portées à la charge l'AE et de son personnel.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

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

5.4.1 Type d'évènements à enregistrer

L'ACR et l'AE consignent dans les registres de vérification tous les événements ayant trait à la sécurité de son système, notamment :

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

Tous les registres et journaux, qu'ils soient électroniques ou papiers, contiennent la date et l'heure de l'évènement, prise auprès d'une source de temps suffisamment fiable, et indiquer l'entité en cause.

L'ACR recueille et collige, par des moyens électroniques ou papiers, de l'information sur la sécurité qui n'est pas produite par le système de l'ACR, notamment :

- journaux des accès physiques ;
- maintenance et changements de la configuration du système ;
- changements apportés au personnel ;

- registres sur la destruction des supports contenant des clés, des données d'activation ou des renseignements personnels sur les bénéficiaires.

La DPC détaille le type d'information qu'il faut consigner.

Afin de faciliter le processus décisionnel, toutes les ententes et toute la correspondance touchant les services de l'ACR sont recueillis et colligées par des moyens électroniques ou manuels, et regroupées en un seul et même endroit.

5.4.2 Fréquence de traitement des journaux d'évènements

L'ACR et l'AE s'assurent que ses journaux sont revus par son personnel au moins chaque semaine, et que tous les éléments importants sont expliqués dans un résumé. A cette fin, L'ACR vérifie notamment si la liste a été falsifiée, et vérifie brièvement toutes les entrées et, plus en détail, les mises en garde et les irrégularités. Sont comparées les listes papiers et électroniques connexes de l'ACR et de l'AE si une mesure est considérée suspecte.

Les mesures prises à la suite de ces examens sont documentées.

5.4.3 Période de conservation des journaux d'évènements

L'ACR et l'AE conservent (en les rendant accessibles dès première demande) les journaux pendant au moins un mois et ensuite les archivent conformément aux instructions indiquées à l'article 5.5.

5.4.4 Protection des journaux d'évènements

Le système des journaux électroniques touchant directement les opérations de certification comprennent des mécanismes de protection contre les tentatives non autorisées de modification et de suppression des journaux.

L'information de vérification obtenue par des moyens manuels est également protégée contre les tentatives non autorisées de modification et de destruction.

Le système de datation des évènements respecte les exigences du chapitre 6.8.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux et leur résumé sont sauvegardés, ou copiés (photocopie ou numérisation) s'ils sont sur support papier.

5.4.6 Système de collecte des journaux d'évènements

L'ACR indique dans la DPC quels systèmes elle utilise pour recueillir les données de vérification.

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

Lorsqu'un évènement est consigné par le système de collecte des données de vérification, il n'est pas requis d'en aviser la personne, l'organisation, le dispositif ou l'application qui en est la cause.

5.4.8 Evaluation des vulnérabilités

Les événements qui surviennent dans le processus de vérification sont consignés, en partie, afin de contrôler les points vulnérables du système. L'AE et l'ACR s'assurent qu'une évaluation de ces points vulnérables est effectuée, revue et révisée, après examen de ces événements.

5.5 ARCHIVAGE DES DONNEES

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont également prises par l'ACR. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données archivées sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les accords contractuels avec d'autres ACR ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les justificatifs d'identité des bénéficiaires et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Les certificats de signature électronique, ainsi que les LCR produites par l'ACR, sont conservés pendant au moins cinq (5) ans après l'expiration des clés.

Seront conservées pendant cinq (5) ans après l'expiration des clés les renseignements liés à la gestion du cycle de vie des certificats, en particulier tous les renseignements liés à l'enregistrement.

Outre les données papier susmentionnées, présentes par exemple dans les dossiers d'enregistrement, sont aussi conservées, sous forme papier et électronique, et ce pour une durée de cinq (5) ans après leur expiration ou leur fin de validité :

- toutes les versions et révisions des DPC applicables par l'ACR ou une composante de l'IGC
- tous les accords signés par Certinomis avec d'autres ACR et composantes de l'IGC

5.5.3 Protection des archives

Une copie de tout le matériel informatique archivé ou sauvegardé est protégée soit par des mesures de sécurité physique seulement, soit par une combinaison de mesures physiques et cryptographiques. Le site d'archivage protège adéquatement le matériel contre les dangers naturels, par exemple les excès de température, d'humidité et de magnétisme.

L'ACR vérifiera l'intégrité de ses archives au moins tous les six (6) mois.

De plus, les informations conservées ou sauvegardées par l'ACR peuvent être assujetties aux lois et règlements en vigueur et applicables à l'archivage et la conservation.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes est équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6 Système de collecte des archives

Le système de collecte des archives, qu'il soit interne ou externe, respecte les exigences de protection des archives concernées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérables dans un délai inférieur à 2 jours ouvrés, sachant que seule l'ACR peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 CHANGEMENT DE CLE D'ACR

L'ACR ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'ACR.

Pour cela la période de validité de ce certificat de l'ACR est supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'ACR est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

Le certificat ne peut être prorogé au delà de sa date de validité. Donc, l'émission d'un nouveau certificat nécessitera un renouvellement des clés.

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

Toutes les procédures à suivre lors de la compromission de la clé privée de l'ACR, des composantes de l'IGC et du personnel de l'ACR sont documentées.

De même, les mesures en cas de désastre ou autres catastrophes naturelles pour les données, les équipements et les logiciels de l'ACR sont documentées.

Dans l'hypothèse d'un déclassement ou d'une réduction du niveau de reconnaissance d'une ACR, son certificat sera révoqué. Un nouveau certificat sera émis, qui correspondra à ce déclassement.

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

La seule activité critique que l'ACR maintienne en fonctionnement est la prise en compte et la publication des révocations de certificats.

L'ACR établit des procédures visant à assurer le maintien des activités et décrit, dans ces procédures, les étapes prévues en cas de corruption ou de perte des ressources informatiques, logicielles ou de données nécessaires. Lorsque le dépôt de documents ne relève pas de l'ACR, celle-ci s'assure que tous les contrats conclus avec le dépositaire prévoient la mise en place, par celui-ci, de procédures visant à la préservation des données.

L'ACR prévoit un plan de secours et de redémarrage de ses activités (PCA/PRA).

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

La connaissance de la compromission avérée ou soupçonnée de la clé privée par un membre d'une composante de l'IGC emporte obligation de procéder sans délais à la vérification de la révocation du certificat associé, et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

En cas de compromission de la clé de signature électronique d'une ACR, et avant de redéfinir un certificat au sein de l'IGC, l'ACR révoque sa clé publique.

S'il faut révoquer le certificat de signature électronique d'une ACR, celle-ci avise dans les plus brefs délais :

- les AGP qui l'accréditent ;
- toutes les AE ; et
- tous les bénéficiaires, tous les clients ;

En outre, l'ACR :

- publie le numéro de série du certificat dans la LCR appropriée ;
- révoque tous les certificats signés au moyen du certificat de signature électronique révoqué.

Après avoir corrigé les problèmes ayant motivé la révocation, l'ACR peut :

- produire une nouvelle bi-clé de signature et publier les certificats associés ; et
- émettre de nouveaux certificats à toutes les entités.

Une nouvelle identité sera utilisée par l'ACR pour éviter toute confusion avec le certificat révoqué.

S'il est nécessaire de révoquer le certificat de signature électronique de toute autre entité, l'ACR suivra les directives de l'article 4.9.

5.7.4 Capacités de continuité d'activité suite à un sinistre

L'AC définit dans un plan anti-sinistre les mesures à prendre pour rétablir une installation sécuritaire en cas de catastrophe naturelle ou de tout autre type de sinistre. L'ACR s'assure qu'il est précisé, dans tous contrats qui auraient été conclus avec des partenaires, qu'un plan anti-sinistre doit être mis en place et documenté par le dépositaire.

5.8 FIN DE VIE DE L'IGC

5.8.1 Fin des activités d'une ACR

Si l'ACR interrompt ses activités, elle avise dans les plus brefs délais ses bénéficiaires et ses clients, et prend toutes les dispositions nécessaires pour que les clés et l'information de l'ACR continuent d'être archivées.

En cas de changements dans la gestion des activités de l'ACR, celle-ci avise toutes les entités pour lesquelles elle a émis des certificats ainsi qu'à tout organisme étatique ; dans ce dernier cas, elle fournira, en temps utile, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité.

Dans le cas où une composante de l'IGC autre que l'ACR interrompt ses activités, l'ACR reprend à sa charge ou faire porter sur une autre entité les obligations de cette composante.

Les archives de l'ACR sont conservées selon les indications et la période stipulées à l'article 4.7.

5.8.2 Fin de contrat

Le contrat court tant que le certificat est en cours de validité ou qu'il a été renouvelé.

La personne qui entend mettre fin prématurément à son contrat doit demander la révocation de son certificat.

La révocation constitue une fin de contrat, elle n'ouvre droit à aucun remboursement.

Les personnes qui peuvent demander la fin de contrat sont les mêmes que celles pouvant demander la révocation du certificat conformément aux dispositions de l'article 5.7.3.

Les procédures de fin de contrat sont identiques à celles prévues pour la révocation du certificat, conformément aux dispositions de l'article 4.9.3

6 MESURES DE SECURITE TECHNIQUES

Le présent chapitre a pour objet de définir les dispositions de gestion des bi-clés de l'ACR, du personnel de l'ACR, des AE déléguées, et des bénéficiaires.

6.1 GENERATION ET INSTALLATION DE BI CLES

6.1.1 Génération des bi-clés

Le principe de séparation des clés est appliqué à toutes les clés utilisées dans le cadre du système technique de l'ACR. La séparation des clés indique qu'une bi-clé ne peut être utilisée que pour une fonction cryptographique donnée, à savoir :

- une bi-clé dédiée à la création et à la vérification de signature ;
- une bi-clé dédiée à la confidentialité.

L'ACR produit son propre bi-clé de signature électronique au moyen d'un algorithme de cryptographie et selon une procédure impliquant plusieurs rôles.

6.1.1.1 Clés d'ACR

La génération des clés de signature d'ACR est effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'ACR sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'ACR est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. Chapitre 5.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'ACR s'accompagne de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'ACR, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'ACR.

Ces parts de secrets sont générées suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer le secret), Ce secret permet de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'ACR sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets sont remis à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'ACR. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même ACR à un moment donné. Chaque part de secrets est mise en œuvre par son porteur.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'ACR et est impartial.

Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.1.2 Clés d'ACD générées par l'ACR

La génération des clés des ACD est effectuée dans un environnement sécurisé (cf. chapitre 5).

Autorité de Certification Délégée
Clés ACD générées par l'ACR
Les bi-clés des ACD sont générées au sein des dispositifs matériels destinés à conserver et à mettre en œuvre ces bi-clés, sous contrôle de l'Autorité d'Enregistrement.

6.1.1.3 Clés ACD générées au niveau du serveur de l'ACD

Dans le cas où la bi-clé est générée au niveau du serveur, cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré. L'ACR s'en assure auprès du responsable de l'entité de l'ACD, au travers d'un engagement contractuel du responsable du serveur vis-à-vis de l'ACR.

Autorité de Certification Racine
Clés ACD générées par le responsable du serveur
Les bi-clés sont générées par le responsable du serveur de l'ACD, qui fournit la clé publique à l'Autorité Racine pour certification.

6.1.2 Transmission de la clé privée à l'ACD

Dans le cas où la bi-clé est générée au niveau de l'ACR, la clé privée est transmise au responsable du serveur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité.

6.1.3 Transmission de la clé publique à l'ACR

En cas de transmission de la clé publique de l'ACD vers une composante de l'ACR, celle dernière doit être remise sous la forme d'une requête (PKCS10) attestant de la possession de la clé privée correspondante. La transmission via une connexion sécurisée assure l'intégrité de bout en bout. Cette clé publique est alors transmise à l'IGC qui vérifie son intégrité.

6.1.4 Transmission de la clé publique de l'ACR aux utilisateurs de certificats

La clé publique de vérification de l'ACR est diffusée sous la forme d'un certificat numérique qui est téléchargeable sur le site web de l'ACR.

6.1.5 Tailles des clés

Les clés d'ACR et de porteurs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) du document [PROFILS].

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

Le moyen de génération de la bi-clé doit utiliser des paramètres respectant les normes internationales de sécurité propres à l'algorithme considéré.

Les choix suivants seront retenus par Certinomis :

- l'exposant public sera 65537 ;
- le choix des premiers p et q peut être aléatoire ou fort, sous réserve d'appliquer les recommandations applicables du document cité en référence.

6.1.7 Objectifs d'usage de la clé

Les différents usages possibles des clés publiques sont définis et ainsi contraints par l'utilisation d'une extension de certificat X.509 v.3 (champ KeyUsage).

La clé publique de vérification de l'ACR est la seule clé utilisable pour vérifier la signature des certificats.

L'utilisation d'une clé privée d'ACR et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. chapitre 1.4.1.2 et 7.1.2).

L'utilisation de la clé privée et du certificat émis associé est strictement limitée au service définis dans les chapitres 1.4.1.1, 4.5 et 7.2.2.

6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

Le bénéficiaire doit protéger ses clés privées afin qu'elles ne soient pas divulguées. Il lui appartiendra de s'assurer qu'une maintenance particulière est réalisée sur le poste utilisé ; en particulier de la stabilité du système, de l'absence de virus, vers et chevaux de Troie. Il lui appartient également de choisir le matériel et les logiciels offrant une sécurité suffisante pour la protection et l'utilisation de ses clés privées conformément aux dispositions du présent chapitre 6.

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'ACR

Les modules cryptographiques, utilisés par l'ACR, pour la génération et la mise en œuvre des ses clés de signature, ainsi que le cas échéant pour la génération des clés des futurs certificats, sont des modules cryptographiques répondant au minimum aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

Le module cryptographique utilisé par l'ACR fait l'objet d'une qualification, au niveau renforcé selon le processus décrit dans le [RGS].

6.2.1.2 Dispositifs cryptographique des ACD

Les dispositifs d'utilisation et de protection de clés privées des ACD, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre 12 ci-dessous.

L'ACR s'assure auprès du responsable du serveur de la conformité du dispositif mis en œuvre par le serveur, au travers d'un engagement contractuel clair et explicite de l'ACD vis-à-vis de l'ACR.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'ACR pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre 6.1.1.1, l'activation de la clé privée au chapitre 6.2.8 et sa destruction au chapitre 6.2.10.

Plusieurs personnes contrôlent les opérations de production des clés de l'ACR. Les données utilisées pour leur création sont partagées par plusieurs personnes. Le partage du secret permettant la génération ou la régénération de la clé de l'AC est fait entre trois (3) personnes.

6.2.3 Séquestre de la clé privée

Ni les clés privées d'ACR, ni les clés privées des certificats émis ne sont en aucun cas séquestrées.

6.2.4 Copie de secours de la clé privée

Une entité identifiée peut sauvegarder ses propres clés de signature électronique ou de confidentialité sous sa seule, exclusive et entière responsabilité. Le cas échéant, les clés sauvegardées doivent être enregistrées sous forme chiffrée et être protégées logiquement ou physiquement contre tout accès illicite. Les mesures de protection prises sur la clé sauvegardée doivent être au moins du même niveau que celles prises pour la clé d'origine.

6.2.5 Archivage de la clé privée

Les clés privées de l'ACR ne sont en aucun cas archivées.

Les clés privées des certificats émis ne sont en aucun cas archivées ni par l'ACR ni par aucune des composantes de l'IGC.

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

6.2.6.1 Clés privées de l'ACR:

Pour les clés privées d'ACR, tout transfert se fait sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.6.2 Clés privées des ACD :

Autorité de Certification Racine
<i>Transfert de la clé privée vers l'ACD</i>
Dans tous les cas un dispositif cryptographique est utilisé, les bi-clés sont générées sous contrôle de l'Autorité d'Enregistrement, directement au sein du dispositif matériel de l'ACD.

6.2.7 Stockage de la clé privée dans un module cryptographique

La procédure de mise à la clé et la procédure de mise sous contrôle des secrets sont spécifiées comme suit :

- Les clés privées de l'ACR sont générées dans le module cryptographique en utilisant des données fixes ou aléatoires introduites depuis l'extérieur ; elles sont conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.
- Les clés privées des entités identifiées sont tant que possible générées par un moyen local. S'il s'avère nécessaire pour le service de recouvrement d'introduire une bi-clé depuis l'extérieur, celle-ci sera introduite chiffrée et sera déchiffrée en local, et au sein même de la ressource cryptographique, si elle existe. Les clés privées des entités identifiées sont tant que possible conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'ACR

La méthode d'activation des clés privées d'ACR dans un module cryptographique permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

L'activation des clés privées d'ACR dans le module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).

L'activation est précisée au niveau de la DPC.

6.2.8.2 Clés privées des ACD

La méthode d'activation des clés privées d'ACD dans un module cryptographique permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

L'activation des clés privées d'ACD dans le module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).

L'activation doit être précisée au niveau de la DPC de l'ACD.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'ACR

La désactivation des clés privées d'ACR dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Une clé privée d'ACR peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

La désactivation est précisée au niveau de la DPC.

6.2.9.2 Clés privées des ACD

La désactivation des clés privées d'ACD dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Une clé privée d'ACD peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

La désactivation doit être précisée au niveau de la DPC de l'ACD.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'ACR

Lorsque l'ACR procède à la destruction de sa clé privée, elle réinitialise le module cryptographique, ce qui implique la réécriture complète de toute forme de mémoire dans le module cryptographique. Elle détruit aussi tous les secrets de génération qui ont été partagés.

Pour détruire une clé privée, il faut écraser toutes les copies des clés privées quel qu'en soit le support. Les procédures de destruction des clés privées sont décrites dans la DPC.

En cas où la réinitialisation n'est pas possible suite à une panne du matériel, celui-ci est détruit. Cette destruction est tracée par un PV de destruction.

6.2.10.2 Clés privées des ACD

Lorsque l'ACD procède à la destruction de sa clé privée, elle réinitialise le module cryptographique, ce qui implique la réécriture complète de toute forme de mémoire dans le module cryptographique. Elle détruit aussi tous les secrets de génération qui ont été partagés.

Pour détruire une clé privée, il faut écraser toutes les copies des clés privées quel qu'en soit le support. Les procédures de destruction des clés privées doivent être décrites dans la DPC de l'ACD.

En cas où la réinitialisation n'est pas possible suite à une panne du matériel, celui-ci est détruit. Cette destruction est tracée par un PV de destruction.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

La ressource cryptographique matérielle de l'ACR est évaluée au niveau EAL 4+, selon les Critères Communs et qualifiée à un niveau renforcé.

Les dispositifs cryptographiques des bénéficiaires sont évalués au niveau correspondant à l'usage visé, tel que précisé au chapitre 12 ci-dessous. Se reporter au chapitre 6.2.1.2.

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1 Archivage des clés publiques

L'ACR émettrice archive ou fait archiver toutes les clés publiques de vérification conformément à l'article 5.5.

6.3.2 Durées de vie des bi-clés et des certificats

L'utilisation d'une longueur particulière de clé est déterminée conformément à l'évaluation de la menace et des risques prenant en compte l'évolution des technologies d'attaque.

La durée de vie des clés est définie dans le document [PROFILS], chapitre 5.3

Autorité de Certification Racine
<i>Durée de vie des certificats</i>
L'utilisation des clés ACR (4096 bits) pour l'émission de certificat est limitée à vingt (20) ans.
La durée de vie maximale d'un certificat émis par l'ACR est de douze (12) ans.

6.4 DONNEES D'ACTIVATION

6.4.1 Génération et installation des données d'activation

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

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se fait lors de la phase d'initialisation et de personnalisation de ce module. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre 5.2.1).

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée des ACD

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se fait lors de la phase d'initialisation et de personnalisation de ce module. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre 5.2.1).

6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'ACR

Les données d'activation qui sont générées par l'ACR pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des ACD

Les données d'activation qui sont générées par l'ACD pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.3 Autres aspects liés aux données d'activation

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

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes de l'IGC mis à disposition de l'ACR offrent les fonctions suivantes, selon le rôle imparti à l'opérateur :

- contrôle de l'accès aux services de l'IGC ;
- distinction rigoureuse des tâches ;
- utilisation de la cryptographie pour assurer la sécurité des communications ;
- protection contre les virus informatiques, y compris les vers et chevaux de Troie ;
- fonctions d'audits, assurant l'imputabilité et la connaissance de la nature des actions réalisées ;
- archivage des historiques et des journaux de vérification de l'IGC ;
- vérification des événements relatifs à la sécurité ;
- gestion de reprise sur erreur.

Ces fonctions peuvent être fournies par le système d'exploitation, ou par une combinaison de fonctions offertes par le système d'exploitation, le système de l'IGC et des mécanismes de protection physique.

L'interface entre l'IGC et l'ACR est également être sécurisée pour éviter toute altération ou intrusion pendant la transmission des données entre les deux.

L'ACR s'engage à mettre en conformité ses pratiques avec les documents de la DCSSI relatifs à la protection du poste de l'application de l'AE et du poste de l'ACR.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Le niveau minimal d'assurance dans la sécurité offerte est défini dans la DPC.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée et respecter dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système, des composantes, ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

6.6.2 Mesures liées à la gestion de la sécurité

L'ACR applique une méthode de gestion de la configuration pour installer le cœur cryptographique de l'ACR et en assurer la maintenance. La première fois qu'il est chargé, le logiciel de l'AC fournit une méthode permettant à l'ACR ou à toute personne habilitée expressément de vérifier si le logiciel installé sur le système :

- vient de la société qui l'a mis au point ;
- n'a pas été modifié avant d'être installé ;
- correspond bien à la version voulue.

L'ACR ou toute personne habilitée expressément prévoit un mécanisme permettant de vérifier périodiquement l'intégrité des logiciels.

L'ACR ou toute personne habilitée expressément met également en place des mécanismes et (ou) des politiques lui permettant de contrôler et de surveiller la configuration du système de l'IGC.

Toute évolution est documentée et apparaît dans les procédures de fonctionnement interne et est conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

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

6.7 MESURES DE SECURITE RESEAU

Les systèmes de l'IGC sont protégés contre les attaques provenant de tout réseau, en particulier les réseaux ouverts. Une telle protection est assurée par l'installation de passerelles de sécurité configurées de façon à permettre la seule utilisation des protocoles et des commandes nécessaires à la bonne marche de l'IGC.

L'ACR définit les protocoles et commandes dans la DPC.

6.8 HORODATAGE / SYSTEME DE DATATION

L'ACR précise les modalités techniques permettant l'horodatage des événements liés à l'activité des composantes de l'IGC dans la DPC.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

Ce chapitre contient les règles et directives relatives à l'utilisation de certains types de certificats X.509, des champs, des extensions des LCR conformes aux normes PKIX.

Le contenu des certificats et des LCR, sont conformes aux exigences de la RFC 5280 : « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ».

7.1 PROFIL DES CERTIFICATS D'ACR

Les champs suivants sont renseignés par le logiciel de l'ACR :

- version : version du certificat X.509
- serialNumber : numéro de série unique du certificat
- signature : identifiant de l'algorithme de signature de l'AC
- issuer : nom de l'AC émettrice
- validity : dates d'activation et d'expiration du certificat
- subject : nom distinctif de l'entité identifiée
- subjectPublicKeyInfo : identifiant de l'algorithme d'usage de la clé publique contenue dans le certificat, et valeur de la clé publique
- extensions : les extensions du certificat définies en 7.1.2.

Le format précis des certificats d'AC est donné dans le document [PROFILS], chapitre 2.1.

7.2 PROFIL DES CERTIFICATS D'ACD

Cf. chapitre 7.1

7.3 PROFIL DES LCR/LAR

Les LCR contiennent les champs de base tels que spécifiés dans la recommandation X 509 CRL V2.

Ces champs sont les suivants :

- version : version de la liste de certificats révoqués X.509.
- signature : identifiant de l'algorithme de signature de l'AC
- issuer : nom de l'AC émettrice
- thisUpdate : date d'émission de cette LCR
- nextUpdate : date limite d'émission de la prochaine LCR
- revokedCertificates : liste d'enregistrement de révocation
- userCertificate : numéro de série unique du certificat révoqué
- revocationDate : date de la révocation
- crlEntryExtensions : extensions propres à cette révocation (motif de révocation, comportement souhaitable face à cette révocation...)
- crlExtensions : extensions générales de la LCR

Le format précis des certificats émis est donné dans le document [PROFILS], chapitre 3.

7.4 PROFIL OCSP

Le service OCSP n'est pas disponible.

7.4.1 Numéro de version

Sans objet.

7.4.2 Extensions OCSP

Sans objet.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre ne concerne que les audits et évaluation de la responsabilité de l'ACR afin de s'assurer du bon fonctionnement de son IGC.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'ACR procède à un contrôle de conformité de cette composante.

L'ACR procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence de 1 fois tous les 2 ans.

Des contrôles internes sont effectués pour s'assurer du bon fonctionnement de l'IGC entre 2 audits de conformité.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

Le contrôle d'une composante est assigné par l'ACR à 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 EVALUATEURS ET ENTITES EVALUEES

L'équipe d'audit ne peut pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

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 qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis 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 à l'ACR 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 l'ACR et doit respecter ses politiques de sécurité internes.

- En cas de résultat "A confirmer", l'ACR 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, l'ACR confirme à la composante contrôlée la conformité aux exigences de la présente PC et la DPC associée.

8.6 COMMUNICATION DES RESULTATS

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'ACR.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Des frais d'émission de certificat seront facturés selon une échelle de tarifs négociés dans le cadre d'un contrat commercial.

9.1.2 Tarifs pour accéder aux certificats

Des frais d'accès au certificat peuvent être facturés par l'ACR selon une échelle de tarifs diffusés ou négociés avec l'ACR.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Des frais de vérification de validité des certificats peuvent être facturés par l'ACR selon une échelle des tarifs diffusés ou négociés avec l'ACR.

Un moyen gratuit de contrôle du statut du certificat est toujours laissé à la disposition du tiers utilisateur.

9.1.4 Tarifs pour d'autres services

Aucun frais ne sera facturé pour l'accès en direct à cette Politique de Certification ou à la DPC. Cependant, des frais peuvent être facturés pour des copies sur support papier ou par voie électronique.

9.1.5 Politique de remboursement

Aucune exigence particulière.

9.2 RESPONSABILITE FINANCIERE

9.2.1 Couverture par les assurances

La garantie associée au certificat est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs de l'IGC ne peut être engagée vis-à-vis des clients, bénéficiaires et tiers utilisateurs.

9.2.2 Autres ressources

Aucune exigence particulière.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Les certificats garantis par la présente PC comportent un niveau d'assurance garanti, précisé par contrat et accessible à la partie utilisatrice.

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- la partie non-publique de la DPC de l'ACR,
- les clés privées de l'ACR, des composantes et des certificats émis,
- les données d'activation associées aux clés privées de l'ACR et des certificats émis²,
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- le dossier d'enregistrement du client,
- les causes de révocation, sauf accord explicite de publication.

9.3.2 Informations hors du périmètre des informations confidentielles

Aucune exigence particulière.

9.3.3 Responsabilités en terme de protection des informations confidentielles

L'ACR applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au §9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage. Lors d'échange de ces données, l'intégrité est garantie par un moyen adapté au type d'information (chiffrement, signature, enveloppe sécurisée...).

L'ACR peut mettre à disposition les dossiers d'enregistrement des ACD à des tiers dans le cadre de procédures légales. Ces dossiers sont aussi accessibles au ACD conformément au §9.4.1.

9.4 PROTECTION DES DONNEES PERSONNELLES

9.4.1 Politique de protection des données personnelles

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à tous les documents détenus ou transmis par l'AC ou par une des composantes de l'IGC (site de la CNIL <http://www.cnil.fr>).

En vertu de la loi, les clients et les bénéficiaires disposent d'un droit d'accès, de rectification et d'opposition à la cession de toute information qui les concerne. Ce droit peut s'exercer par l'intermédiaire du service agent, en particulier l'AE, ayant recueilli ces informations, à l'adresse figurant sur le site WEB de l'ACR.

² La confidentialité des données d'activation des clés privées des certificats émis est garantie par l'AC tant qu'elle les détient.

L'ACR respecte rigoureusement toutes les prescriptions légales applicables et expliquer sur son site WEB, les modalités concrètes d'application de la loi, notamment dans les rubriques « mentions légales » et « droit d'accès ».

La Politique de Certification respecte les principes fondamentaux en matière de protection des données à caractère personnel consacrés dans la loi, la directive européenne 2002/58/CE et toute autre convention internationale entrée en vigueur.

9.4.2 Informations à caractère personnel

Toutes les données collectées et détenues par l'ACR ou une AE sur une personne physique ou morale (par exemple : procédure d'enregistrement, révocation, autres événements consignés, correspondances échangées entre le bénéficiaire et l'ACR ou l'AE, etc.) sont considérées comme confidentielles et ne peuvent pas être divulguées sans avoir obtenu le consentement préalable du bénéficiaire.

Les renseignements concernant l'identification ou d'autres données à caractère personnel, du bénéficiaire, apparaissant sur les certificats sont considérés comme étant confidentiels, sauf si le bénéficiaire a donné son consentement exprès et préalable à toute diffusion.

Les Listes des Certificats Révoqués ne contiennent que les numéros d'enregistrement des certificats, et leur date de révocation. Les causes de révocation des certificats sont réputées demeurer strictement confidentielles

9.4.3 Informations à caractère non personnel

Aucune exigence particulière.

9.4.4 Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

9.4.5 Notification et consentement d'utilisation des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

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

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

9.4.7 Autres circonstances de divulgation d'informations personnelles

Le secret des correspondances émises par voie des télécommunications est garanti par la loi française. En cas d'atteinte, toute violation est punie par l'article 226-15 du code pénal pour celles

commises par un particulier et par les articles 432-9 et 432-17 du code pénal pour celles commises par une personne dépositaire de l'autorité publique.

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

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

Tous les droits de propriété intellectuelle détenus par Certinomis sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non respect. Par exemple, conformément à la loi n°98-536 du 1^{er} juillet 1998 (Journal officiel du 2 juillet 1998, p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données réalisées par Certinomis sont protégées. Le texte de la loi peut être consulté sur le site suivant : <http://www.legifrance.gouv.fr>

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Ce chapitre contient des dispositions relatives aux obligations respectives de l'ACR, du personnel de l'ACR, des diverses entités composant l'IGC, des clients, des bénéficiaires et des tiers utilisateurs. Elle contient aussi des dispositions juridiques, relatives notamment à la loi applicable et à la résolution des litiges.

Les différentes composantes de l'IGC doivent :

- protéger leurs clés privées et leur éventuelle donnée d'activation en intégrité et en confidentialité ;
- n'utiliser leurs clés publiques et privées qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elle s'engage ;
- documenter leurs procédures internes de fonctionnement ;
- respecter et appliquer les termes de la présente PC et de la DPC qu'elle reconnaît ;
- accepter le résultat et les conséquences d'un contrôle de conformité, et en particulier remédier aux non-conformités qui pourraient être révélées ; et
- respecter les conventions qui les lient aux autres entités composantes de l'IGC.

9.6.1 Autorités de Certification Racine

L'ACR est responsable vis-à-vis de ses clients, bénéficiaires, mandataires de certification et tiers utilisateurs des opérations relatives aux services de certification réalisées par l'une quelconque des composantes de l'IGC. Elle garantit le lien qui existe entre une entité identifiée et une bi-clé.

L'ACR veille à ce que les AE qui agissent en son nom se conforment à toutes les modalités pertinentes de la présente Politique de Certification, concernant le fonctionnement des AE.

L'ACR veille à ce que les mandataires de certification aient connaissance et approuvé des obligations et responsabilités endossées dans le cadre de leurs fonctions.

L'ACR et le responsable de l'ACR se conforment à toutes les exigences de la présente Politique de Certification et de la DPC associée. L'ACR et le personnel de l'ACR doivent respecter les droits des clients, bénéficiaires et tiers utilisateurs de certificats eu égard aux lois et règlements en vigueur.

L'ACR informe les tiers utilisateurs de la révocation du certificat d'un bénéficiaire ou d'une composante de l'IGC en transmettant dans les plus brefs délais la révocation du certificat auprès de l'IGC qui a en charge de publier les Listes de Certificats Révoqués ;

L'ACR est responsable de la transmission de l'information à l'IGC pour ses clients, ses mandataires de certification et ses bénéficiaires des procédures à suivre au cours du cycle de vie des certificats ; cela concerne, notamment, l'émission, la révocation, le retrait des certificats.

L'ACR valide la génération des certificats, transmet les informations concernant la révocation des certificats et transmet les informations nécessaires au renouvellement des certificats au bénéfice des utilisateurs.

Le personnel de l'ACR, ainsi que l'ensemble du personnel des AE, doit se conformer à toutes les exigences pertinentes de la présente Politique de Certification et de la DPC associée. Il doit respecter les droits des clients, des bénéficiaires et des tiers utilisateurs de certificats eu égard aux lois et règlements en vigueur et doit informer l'ACR de tout problème constaté quant à la disponibilité du site www.Certinomis.com.

Les membres du personnel de l'ACR, et des AE, à qui sont assignés des rôles relatifs à l'IGC (responsable de l'ACR, responsable de la sécurité de l'ACR...) doivent être personnellement responsables de leurs actes. L'expression « *personnellement responsable* » signifie que l'on puisse prouver qu'une telle personne a bel et bien fait une telle action.

9.6.2 Service d'enregistrement

Une AE se conforme à toutes les exigences de la présente politique de certification et de la DPC associée. En outre, une AE:

- traite les demandes de certificat ;
- vérifie les données personnelles d'identification et les données contenues dans le certificat ;
- transmet à l'ACR les demandes de génération, révocation, renouvellement des certificats qu'elle aurait traité favorablement ;
- transmet à l'ACR une trace imputable de la validité de cette vérification ;
- transmet en toute confidentialité des supports physiques ou des codes d'activation aux bénéficiaires ; et
- conserve et protège en confidentialité et en intégrité toutes les données à caractère personnel et d'identification collectées lors des procédures d'enregistrement.

L'AE se soumet à tout contrôle technique et audits de qualité des procédures que pourrait demander l'ACR ou les AGP qui l'accréditent.

9.6.2.1 Obligations du mandataire de certification

Le mandataire de certification doit se conformer à toutes les exigences de la présente Politique de Certification et des éléments de la DPC diffusés par l'ACR.

Il s'engage à respecter le contrat qui le lie à l'ACR.

Il garantit que les informations qu'il fournit à l'ACR ou à une AE, pour l'identification de l'entité identifiée ou du bénéficiaire, sont exactes, complètes et que les documents transmis ou présentés sont valides.

Le mandataire de certification doit établir et faire respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les certificats.

S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'ACR dans les plus brefs délais et selon les instructions données par celle-ci.

Il doit protéger en confidentialité et en intégrité ses clés privées, ses codes d'activation ou d'accès. Il doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée.

9.6.3 Bénéficiaire de certificats

Le bénéficiaire doit se conformer à toutes les exigences de la présente Politique de Certification et des éléments de la DPC diffusés par l'ACR.

Il s'engage à respecter le contrat qui le lie à l'ACR.

Il garantit que les informations qu'il fournit à l'ACR ou à une AE, pour son identification, celle du bénéficiaire ou de l'entité identifiée, sont exactes, complètes et que les documents transmis ou présentés sont valides.

Si le bénéficiaire est une organisation, il doit établir et faire respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les certificats.

S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'ACR dans les plus brefs délais et selon les instructions données par celle-ci.

En aucun cas le bénéficiaire n'acquiert la propriété du certificat émis par l'ACR. Il n'en acquiert que le droit d'usage. Par conséquent, tous les certificats demeurent la propriété de l'ACR qui les a émis.

9.6.4 Utilisateurs de certificats

L'utilisateur doit se conformer à toutes les exigences de la présente Politique de Certification et des éléments de la DPC diffusés par l'ACR. Le bénéficiaire doit exclusivement utiliser ses clés privées et certificats à des fins autorisées par la présente Politique de Certification, ainsi que dans le respect des lois et règlements en vigueur.

Il garantit que les informations qu'il fournit à l'ACR ou à une AE, pour son identification ou celle de l'entité identifiée, sont exactes, complètes et que les documents transmis ou présentés sont valides.

Il doit protéger en confidentialité et en intégrité ses clés privées, ses codes d'activation ou d'accès conformément à l'article 6.2. Il doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée. Il s'engage à suivre toute prescription du client en matière de politique de sécurité dans le cadre de l'usage du certificat.

S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'ACR dans les plus brefs délais et selon les instructions données par celle-ci.

9.6.5 Autres participants

9.6.5.1 Obligation du tiers utilisateur

Le tiers utilisateur d'un certificat doit se conformer à toutes les exigences mentionnées dans le cadre de la présente Politique de Certification et des éléments de la DPC diffusés par l'ACR émettrice du dit certificat, documents contractuels qu'il reconnaît expressément avoir lus et approuvés.

Avant toute utilisation de certificats, notamment lorsque lesdits certificats créent des effets juridiques, le tiers utilisateur doit impérativement avoir un comportement raisonnable : vérifier la validité des certificats auxquels il entend se fier auprès de Certinomis, en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant leur date d'expiration et leur validité intrinsèque, en particulier sa signature, et la validité de tout certificat sur l'itinéraire de confiance. A défaut de remplir cette obligation, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, Certinomis ne garantissant aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

En outre, lors de la vérification d'une signature électronique, le tiers utilisateur doit aussi vérifier que la clé publique du certificat correspond à la clé privée de signature utilisée.

Le tiers utilisateur doit toujours vérifier que le certificat est utilisé à des fins pertinentes et conformément aux applications autorisées.

Un tiers utilisateur ne doit utiliser les certificats que conformément à la procédure de validation de l'itinéraire de confiance, procédure qui est spécifiée dans les normes X. 509 et PKIX et déterminée par la recommandation ISO/IEC 9594-8.

9.7 LIMITE DE GARANTIE

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

En conséquence de quoi, les bénéficiaires, les mandataires de certification, les clients et les tiers utilisateurs de certificat sont des personnes juridiquement et financièrement indépendantes et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'ACR ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'ACR ou de l'une des composantes de l'IGC. Les services de certification ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre. Le contrat ne constitue ni une association, ni une société ou autre groupement, ni un mandat donné par l'une des parties à l'autre.

Le fait que le nom d'une organisation soit dans un certificat de signature électronique ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur du bénéficiaire.

La garantie associée au certificat est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs de l'IGC ne peut être engagée vis-à-vis des clients, bénéficiaires et tiers utilisateurs.

9.8 LIMITE DE RESPONSABILITE

L'ACR, le personnel de l'ACR, les composantes de l'IGC, les clients, les bénéficiaires, les tiers utilisateurs sont responsables pour tous dommages et intérêts découlant du non-respect de leurs obligations respectives telles que définies aux termes de la présente Politique de Certification et de la DPC associée.

L'ACR détaille le périmètre des limites de responsabilité dans sa DPC.

9.9 INDEMNITES

Aucune exigence particulière.

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1 Durée de validité

La présente PC reste en application 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'ACR de faire évoluer sa DPC correspondante.

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 à la sécurité.

9.10.3 Effets de la fin de validité et clauses restant applicables

Aucune exigence particulière.

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE 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.
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12 AMENDEMENTS A LA PC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente politique de certification.

9.12.1 Procédures d'amendements

L'ACR devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la PC type PRIS et des éventuels documents complémentaires de la PRIS. En cas de changement important, l'ACR fera appel à une expertise technique pour en contrôler l'impact.

9.12.2 Mécanisme et période d'information sur les amendements

9.12.2.1 Délais de préavis

- Le responsable de l'ACR donne un préavis de trente (30) jours aux bénéficiaires et aux tiers utilisateurs avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact majeur sur eux.
- Le responsable de l'ACR donne un préavis de quinze (15) jours aux bénéficiaires et aux tiers utilisateurs avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact mineur sur eux.
- Le responsable de l'ACR donne un préavis aux bénéficiaires et aux tiers utilisateurs dans les sept (7) jours d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, à condition que ce changement ait un impact sur eux.
- Le responsable de l'ACR peut modifier la présente politique sans préavis aux bénéficiaires et aux tiers utilisateurs lorsque, selon l'évaluation du responsable de la politique, ces modifications n'ont aucun impact sur eux.

9.12.2.2 Forme de diffusion des avis

Dans les cas nécessitant un préavis, le responsable de l'ACR avise les clients, les bénéficiaires, des modifications apportées à la politique, en diffusant les changements sur le site WEB du responsable de la politique et par message électronique.

Lorsque l'avis est à destination des bénéficiaires et des clients, le préavis est communiqué par message électronique si les changements ont un impact majeur, et diffusé sur le site web de l'ACR et du responsable de la présente politique dans tous les autres cas.

9.12.2.3 Période de commentaires

Les personnes désirant se prononcer sur les modifications doivent faire parvenir leurs commentaires au responsable de la politique dans des délais inférieurs à la moitié des délais de préavis fixés à l'article 9.12.2.1.

9.12.2.4 Traitement des commentaires

Aucune exigence particulière.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Si un changement de politique a, selon l'évaluation du responsable de la politique, un impact majeur sur un nombre important de clients, des bénéficiaires et/ou de tiers utilisateurs, le responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

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

9.14 JURIDICTIONS COMPETENTES

La présente politique de certification est expressément élaborée, régie, appliquée et interprétée selon les lois et règlements français, bien que les activités qui découlent de la présente Politique de Certification puissent avoir des effets juridiques en-dehors du territoire de la République française.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.16 DISPOSITIONS DIVERSES

9.16.1 Accord global

Aucune exigence particulière.

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

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

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

9.16.4 Application et renonciation

Toute notification devant être donnée au titre de la présente politique sera censée avoir été donnée si elle est envoyée par lettre recommandée avec avis de réception ou par télécopie adressée au domicile élu tel qu'indiqué en entête du contrat de services et sera censée avoir été reçue sept (7) jours après la date de cachet de la Poste dans le cadre de la lettre recommandée avec avis de réception et un (1) jour après la date d'envoi dans le cadre de la télécopie.

9.16.5 Force majeure

Dans un premier temps, les cas de force majeure suspendront l'exécution du contrat. Si les cas de force majeure ont une durée supérieure à celle indiquée dans le contrat, le contrat est résilié automatiquement, sauf accord contraire entre les parties. L'exécution des obligations reprendra son cours normal dès que l'évènement constitutif de la force majeure aura cessé.

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

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, des clauses contractuelles contenues dans la Déclaration des Pratiques associée et toutes autres conventions liant les parties (par exemple le contrat) :

Grève totale ou partielle, lock-out, émeute, trouble civil, insurrection, guerre civile ou étrangère, risque nucléaire, embargo, confiscation, capture ou destruction par toute autorité publique, intempérie, épidémie, blocage des moyens de transport ou d'approvisionnement pour quelque raison que ce soit, tremblement de terre, incendie, tempête, inondation, dégâts des eaux, restrictions gouvernementales ou légales, modifications légales ou réglementaires des formes de commercialisation, panne d'ordinateur, blocage des communications électroniques, y compris des réseaux de télécommunications, toute découverte scientifique majeure remettant en cause en totalité ou en partie les principes de la cryptographie asymétrique, toute conséquence d'une évolution technologique, non prévisible par l'ACR, remettant en cause les normes et standards de sa profession et tout autre cas indépendant de la volonté des parties empêchant l'exécution normale du présent contrat.

9.17 AUTRES DISPOSITIONS

9.17.1 Dispositions pénales

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 2 à 5 ans d'emprisonnement et d'une amende allant de 30.000 à 375.000 euros pour les personnes morales.

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

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 REGLEMENTATION

Renvoi	Document
[CNIL]	<i>Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004</i>
[DIRSIG]	<i>Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.</i>
[LCEN]	<i>Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.</i>
[ORDONNANCE]	<i>Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives</i>
[QPSCe]	<i>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</i>
[DécretRGS]	<i>Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005.</i>
[SIG]	<i>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.</i>

10.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[RGS]	<i>Référentiel Général de Sécurité – version 1.0</i>
[PROFILS]	<i>Profils de certificats / LCR / OSCP et Algorithmes Cryptographiques DT-FL-1001-001-PC-PROFILS-1.2.doc – version 1.2</i>
[RGS_A]	<i>RGS – Ensemble de document sur les Fonction de sécurité et les Politiques de Certification Types.</i>
[RGS_B]	<i>RGS – Ensemble de document sur Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.</i>
[CWA14167-1]	<i>CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1</i>
[CWA14167-2]	<i>CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.</i>
[CWA14167-3]	<i>CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)</i>
[CWA14167-4]	<i>CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.</i>
[CWA14169]	<i>CWA 14169 (2002-04) Secure Signature Creation Devices (SSCD). Ce PP a été certifié EAL4+.</i>

[ETSI_QCP]	<i>ETSI TS 101 456 V1.4.3 (mai 2007) Policy Requirements for Certification Authorities issuing qualified certificates</i>
[ETSI_NQCP]	<i>ETSI TS 102 042 V2.1.1 (mai 2009) Policy Requirements for Certification Authorities issuing public key certificates</i>
[ETSI_SigPol]	<i>ETSI TR 102 272 - ASN.1 format for signature policies V1.1.1 (décembre 2003) ETSI TR 102 038 - XML format for signature policies V1.1.1 (avril 2002)</i>
[PROG_ACCRED]	<i>COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf www.cofrac.fr</i>
[RFC3647]	<i>IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003</i>
[X.509]	<i>Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complete par les correctifs techniques n° 1 d'octobre 2001, n° 2 d'avril 2002 et n° 3 d'avril 2004)</i>
[PP_HORO]	<i>DCSSI - Profil de Protection - Systèmes d'horodatage EAL3+ DCSSI PP 2008/07</i>
[972-1]	<i>DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003</i>

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

11.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le module cryptographique, utilisé par l'ACR pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des certificats émis, doit répondre aux exigences de sécurité suivantes :

- si les bi-clés des certificats émis sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- si les bi-clés des certificats émis sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques lorsqu'elles sont sous la responsabilité de l'ACR et pendant leur transfert vers le dispositif cryptographique du bénéficiaire et assurer leur destruction sûre après ce transfert ;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'ACR durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'ACR, qui ne révèle pas les clés privées de l'ACR et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privée de l'ACR 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.

Le module cryptographique de l'ACR détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.

11.2 EXIGENCES SUR LA QUALIFICATION

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

12 ANNEXE 3 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'ACD

12.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Cf. chapitre 11.1

12.2 EXIGENCES SUR LA CERTIFICATION

Cf. chapitre 11.2