



CENTRE NATIONAL D'ÉTUDES SPATIALES

Politique de certification
de l'AC Racine
de l'IGC du CNES

Référence : DCS//SI-2010.26059



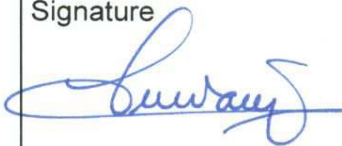
Version : 1.0

Date : 30/11/2010

Nb de pages : 42

DIRECTION CENTRALE DE LA SECURITE

**POLITIQUE DE CERTIFICATION DE L'AC RACINE
DE L'IGC DU CNES**

Préparé par	Jérôme CLERY Rapporteur du groupe de travail le : 27/01/2011 DCS/SI	Signature 
Approuvé par	Valérie ZORZI le : 27.01.2011 DCS/SI	Signature 
Autorisé pour application par	Bernard LUCIANI le : 3/2/11 DCS/D	Signature 

Page d'analyse documentaire

Classe (Confidentialité) : Tout Public		
Mots clés : Sécurité, Politique de Certification		
Rédacteurs : Direction Centrale de la Sécurité		
Résumé :		
<p>Ce document représente la Politique de Certification appliquée à l'Autorité de Certification Racine de l'Infrastructure de Gestion des Clés du CNES.</p> <p>Cette Autorité de Certification Racine de l'IGC du CNES a pour vocation de garantir des certificats des composantes de l'IGC du CNES.</p> <p>Cette Politique suit le plan recommandé par le <i>Référentiel Général de Sécurité</i>. A ce titre, elle vise à y être conforme dans sa forme et dans toutes ses exigences fondamentales.</p>		
Gestion en configuration : Non	A dater du : Date de parution	Par :
Contrat : Sans Objet		
Logiciel(s) hôte : Word 2003	Nombre de pages supplémentaires : 0	

Historique des modifications

Version	Date	Référence DM / Nature de l'évolution / Chapitres modifiés (si nécessaire)
	Août 2008	Création de la PC de l'IGC CNES
1.0	Sept 2010	Refonte de l'architecture documentaire de l'IGC : création de la PC de l'AC Racine

SOMMAIRE

1	INTRODUCTION.....	5
1.1	Présentation générale	5
1.2	Identification du document	6
1.3	Entités intervenant dans l'IGC	6
1.4	Usage des certificats	8
1.5	Gestion de la PC	8
1.6	Définitions et acronymes	9
2	RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	11
2.1	Entités chargées de la mise à disposition des informations	11
2.2	Informations devant être publiées	11
2.3	Délais et fréquences de publication	11
2.4	Contrôle d'accès aux informations publiées	11
3	IDENTIFICATION ET AUTHENTIFICATION	12
3.1	Nommage	12
3.2	Validation initiale de l'identité	13
3.3	Identification et validation d'une demande de renouvellement des clés	13
3.4	Identification et validation d'une demande de révocation	13
4	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS ..	14
4.1	Demande de certificat	14
4.2	Traitement d'une demande de certificat	14
4.3	Délivrance du certificat	14
4.4	Acceptation du certificat	15
4.5	Usages de la bi-clé et du certificat	15
4.6	Renouvellement d'un certificat	15
4.7	Délivrance d'un nouveau certificat suite à changement de la bi-clé	15
4.8	Modification du certificat	16
4.9	Révocation et suspension des certificats	16
4.10	Fonction d'information sur l'état des certificats	18
4.11	Fin de la relation entre une AC Fille et l'AC Racine	19
4.12	Séquestre de clé et recouvrement	19
5	MESURES DE SECURITE NON TECHNIQUES	20
5.1	Mesures de sécurité physique	20
5.2	Mesures de sécurité procédurales	21
5.3	Mesures de sécurité vis-à-vis du personnel	22
5.4	Procédures de constitution des données d'audit	23
5.5	Archivage des données	24
5.6	Changement de clé d'AC	25
5.7	Reprise suite à compromission et sinistre	25
5.8	Fin de vie de l'IGC	26
6	MESURES DE SECURITE TECHNIQUES	27
6.1	Génération et installation de bi clés	27

6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	27
6.3	Autres aspects de la gestion des bi-clés	29
6.4	Données d'activation	29
6.5	Mesures de sécurité des systèmes informatiques	29
6.6	Mesures de sécurité des systèmes durant leur cycle de vie	29
6.7	Mesures de sécurité réseau	30
6.8	Horodatage / Système de datation	30
7	PROFILS DES CERTIFICATS, OCSP ET DES LCR	31
7.1	Profil des certificats	31
7.2	Profil des LAR	33
7.3	Profil OCSP	34
8	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	35
8.1	Fréquences et / ou circonstances des évaluations	35
8.2	Identités / qualifications des évaluateurs	35
8.3	Relations entre évaluateurs et entités évaluées	35
8.4	Sujets couverts par les évaluations	35
8.5	Actions prises suite aux conclusions des évaluations	35
8.6	Communication des résultats	36
9	AUTRES PROBLEMATIQUES METIERS ET LEGALES	37
9.1	Tarifs	37
9.2	Responsabilité financière	37
9.3	Confidentialité des données professionnelles	37
9.4	Protection des données personnelles	37
9.5	Droits sur la propriété intellectuelle et industrielle	37
9.6	Interprétations contractuelles et garanties	37
9.7	Limite de garantie	38
9.8	Limite de responsabilité	38
9.9	Indemnités	38
9.10	Durée et fin anticipée de validité de la PC	38
9.11	Notifications individuelles et communications entre les participants	38
9.12	Amendements à la PC	38
9.13	Dispositions concernant la résolution de conflits	39
9.14	Juridictions compétentes	39
9.15	Conformité aux législations et réglementations	39
9.16	Dispositions diverses	39
9.17	Autres dispositions	40
10	ANNEXE 1 : VARIABLES DE TEMPS	41
11	ANNEXE 2 : DOCUMENTS APPLICABLES ET DE REFERENCE	42

1 INTRODUCTION

1.1 PRESENTATION GENERALE

Une Infrastructure de Gestion des Clés (IGC) est un ensemble de composants physiques tels que le HSM, des cartes à puce, des éléments cryptographiques, de procédures humaines telles que la vérification et la validation de l'identité et de logiciels, le tout permettant de gérer le cycle de vie des certificats.

L'IGC fournit des services tels que la génération, le renouvellement, la révocation, la publication de certificats, la publication des listes de révocation (LCR) ou la journalisation d'événements et le séquestre des clés de chiffrement.

L'Infrastructure de Gestion des clés (IGC) du CNES se décompose en une AC Racine et trois AC Filles. L'AC Racine a pour rôle d'approuver les AC Filles qui vont fournir les certificats d'authentification, de chiffrement et de signature aux porteurs.

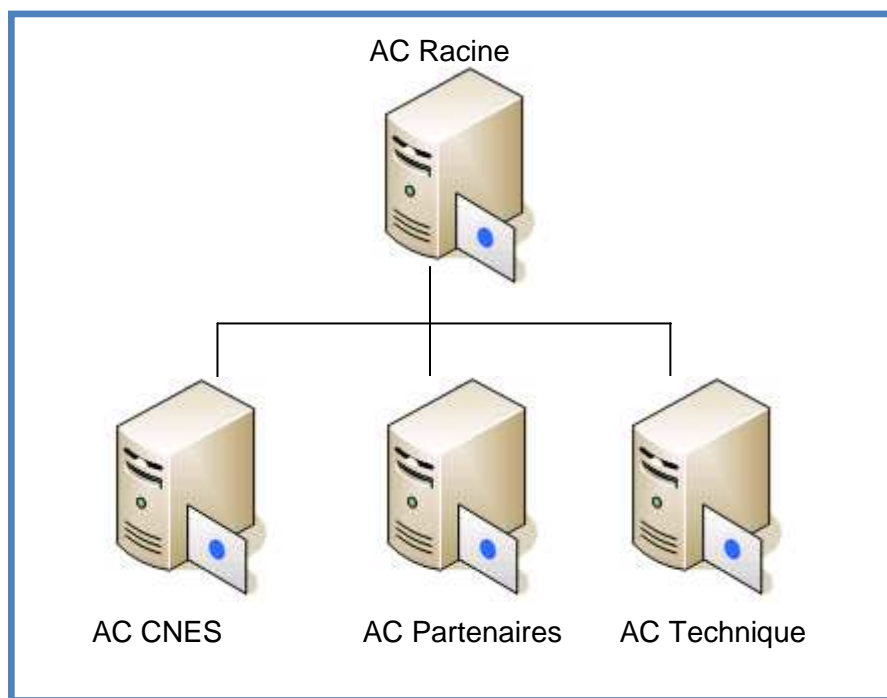


Figure 1 : Hiérarchie des AC de l'IGC du CNES

Ce document décrit la Politique de Certification (PC) de l'Autorité de Certification Racine (ACR) de l'Infrastructure de Gestion des Clés (IGC) du CNES. Cette Autorité de Certification (AC) est mise en œuvre pour délivrer des certificats aux AC Filles de l'IGC.

La présente Politique de Certification s'appuie sur les préconisations émises et la structure recommandée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour des Politiques répondant aux exigences du Référentiel Général de Sécurité (RGS).

1.2 IDENTIFICATION DU DOCUMENT

Chaque Politique de Certification est identifiée de façon unique par un nom de référence et un Identifiant Objet (OID). Un Identifiant d'Objet (OID) est une série de nombres organisée en arborescence et que l'on associe à un « objet » (généralement informatique).

- La branche OID CNES est enregistrée auprès de l'AFNOR : 1.2.250.1.12 ;
Le code en 6ième position désigne une application (1) ou une structure (2) ; le 7ième est un numéro chrono d'application ou de structure. Ils sont attribués par le service de gestion centrale ;
Les deux codes attribués à l'IGC du CNES sont : .1.1 ;
iso(1) member-body(2) fr(250) type-org(1) cnes(12) application(1) igc(1) ;
- Les trois derniers digits de l'arborescence sont gérés par l'application IGC ;
L'antépénultième digit est l'identifiant de la composante d'IGC. L'avant dernier digit indique l'identifiant du document. Le dernier digit indique la version du document. Elle complète l'OID précédent comme suit: composante (c) document (d) version (v) ;
Pour les Politiques de Certification des AC, l'identifiant du document sera toujours 1.

L'OID de la PC de l'AC Racine CNES est 1.2.250.1.12.1.1.1.1.1.

1.3 ENTITES INTERVENANT DANS L'IGC

La notion d'Autorité de Certification (AC) telle qu'utilisée dans la présente PC est définie au chapitre 1.3.1 ci-dessous.

L'AC 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).

Le schéma suivant rappelle le périmètre de couverture de la présente PC :

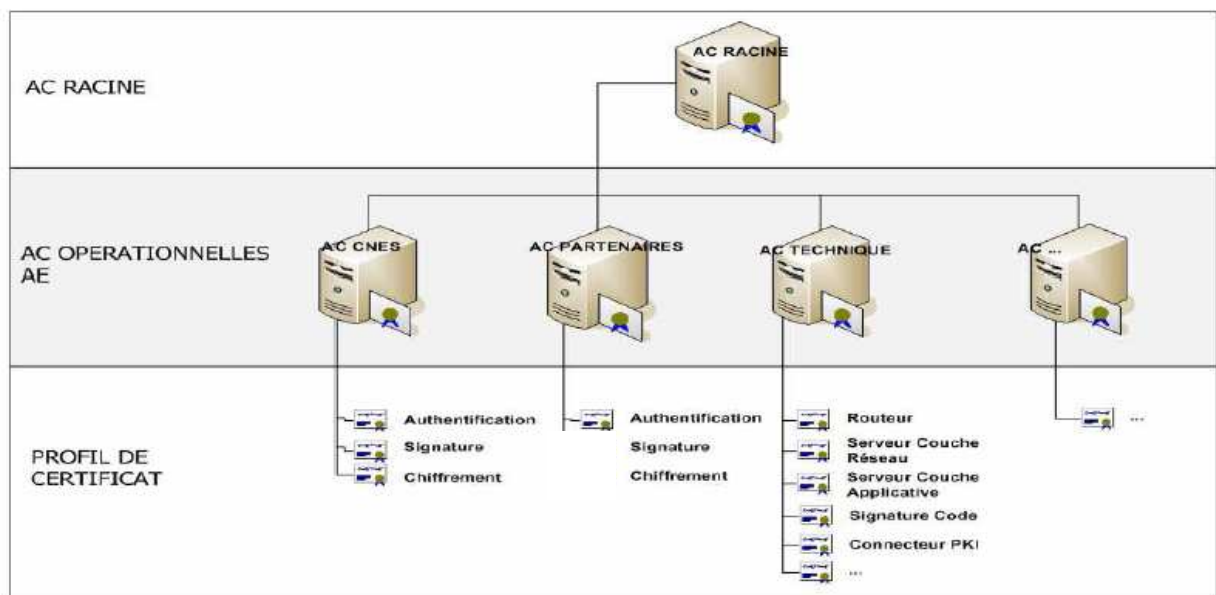


Figure 2 : Couverture de la présente PC

1.3.1 Autorité de Certification (AC)

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux porteurs, 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 ;
- Mettre en œuvre les différentes fonctions identifiées dans cette PC, correspondant au minimum aux fonctions obligatoires, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats ;
- Elaborer, mettre en œuvre et maintenir les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels ;
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans cette PC, notamment en termes de fiabilité, de qualité et de sécurité. A ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure ;
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LAR et de réponses OCSP) ;
- Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.

1.3.2 Autorité d'Enregistrement (AE)

L'AC Racine ne possède pas d'Autorité d'Enregistrement pour sa propre création et la création des AC Filles.

Il n'y a pas de processus d'enregistrement ni de service d'enregistrement pour les AC : la création d'une nouvelle AC Racine ou Fille fait l'objet d'une décision formelle prise par la Direction de l'AC qui définit le nom de l'AC correspondante.

1.3.3 Direction de l'AC

La Direction de l'AC est responsable de la validation et de la gestion de la Politique de Certification. Conformément au RGS, la notion de Direction de l'AC n'a pas de connotation hiérarchique. Celle-ci a pour rôle de définir et de faire appliquer la Politique de Certification et la Déclaration des Pratiques de Certification associée.

Elle garantit la validité et la cohérence de la Politique de Certification et elle initialise et coordonne la mise en œuvre des fonctions critiques de l'IGC : cérémonie de clés, accès au séquestre, création et révocation d'AC Filles, révisions de PC ou de DPC, ...

1.3.4 Porteurs de certificats

Compte-tenu du domaine d'application, les porteurs des certificats générés sont l'AC Racine et les AC opérationnelles.

1.3.5 Utilisateurs des certificats

Compte tenu du domaine d'application, les utilisateurs des certificats générés par l'AC Racine sont :

- les Autorités de Certification Filles ;
- les utilisateurs de ces AC Filles qui vérifient la chaîne de certification.

1.3.6 Autres participants

Sans objet.

1.4 USAGE DES CERTIFICATS

1.4.1 Domaines d'utilisation applicables

Les certificats couverts par cette Politique de Certification sont les suivants :

- le certificat de l'AC Racine (certificat auto-signé) utilisé pour :
 - la signature des certificats des AC Filles ;
 - la signature de la Liste des Autorités Révoquées (LAR).
- les certificats des AC Filles signés par l'AC Racine et utilisés pour :
 - la signature des certificats des porteurs ;
 - la signature de la Liste des Certificats Révoqués (LCR).

Les certificats d'Autorité de Certification doivent être utilisés uniquement pour de la signature de certificats et de LAR/LCR.

1.4.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5. L'AC doit respecter ces restrictions et imposer leur respect par ses porteurs et ses utilisateurs de certificats.

A cette fin, elle doit communiquer à tous les porteurs et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

1.5 GESTION DE LA PC

1.5.1 Entité gérant la PC

La Direction de l'AC est responsable de la validation et de la gestion des Politiques de Certification.

1.5.2 Point de contact

Le point de contact est le suivant : CNES - DCS/SI - 2 place Maurice Quentin - 75001 Paris.

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

La conformité entre la présente PC et la Déclaration des Pratiques de Certifications est établie par la Direction d'AC.

1.5.4 Procédures d'approbation de la conformité de la DPC

Sans objet.

1.6 DEFINITIONS ET ACRONYMES

Les acronymes utilisés dans la présente PC sont les suivants :

TERME	DEFINITION
AC (en : CA)	Autorité de Certification (en : Certification Authority) Entité responsable de la signature de certificats X509
ACR	Autorité de Certification Racine
AE (en : RA)	Autorité d'Enregistrement (en : Registration Authority) Entité responsable du contrôle des demandes de certificats
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
HSM	Hardware Security Module Module Cryptographique matériel permettant le tirage et la protection de clés privées
HTML	HyperText Markup Language Langage de construction des pages Web, à base de balises. C'est le langage compris et « décodé » par le navigateur web
HTTP	HyperText Transfer Protocol. Protocole utilisé pour la transmission des pages web (HTML) du serveur vers le navigateur de l'internaute
HTTPS	HTTP Secure Protocole HTTP qui offre en plus la sécurisation du transport des données entre un serveur Web et un navigateur client en mettant en œuvre des mécanismes de chiffrement Le protocole HTTPS peut également être utilisé pour échanger des informations entre des serveurs
IAM	Identity & Access Management
IETF	Internet Engineering Task Force
IGC (en : PKI)	Infrastructure de Gestion de Clé (en : Public Key Infrastructure) Système logiciel permettant la gestion du cycle de vie des certificats X509
ISO	International Organization for Standardization
LAR (en : ARL)	Liste des Autorités Révoquées (en : Authority Revocation List)
LCR (en : CRL)	Liste de Certificats Révoqués (en : Certificate Revocation List)
OCSP	Online Certificat Status Protocol
OID	Object Identifier
PC	Politique de Certification
RFC	Request For Comments Document de référence qui peut présenter une documentation, la spécification d'une norme ou d'un protocole
RGS	Le référentiel général de sécurité (RGS) est prévu par l'ordonnance no 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives Ce référentiel fixe, selon le niveau de sécurité requis, les règles que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage
X500	X.500 désigne l'ensemble des normes informatiques sur les services d'annuaire définies par l'UIT-T (anciennement appelé CCITT)
X501	Modèle d'annuaire LDAP
X509	La norme X.509 définit ce qui concerne l'authentification, elle spécifie un format standard pour les certificats de clés publiques

1.6.1 Termes et définitions

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une Autorité de Certification, d'un opérateur de certification, d'une Autorité d'Enregistrement centralisée et/ou locale, d'une entité d'archivage, d'une entité de publication, etc.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Qualification d'un produit de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les services de sécurité objets de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS].

Système d'information - Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

1.6.2 Termes spécifiques ou complétés/adaptés pour la présente PC

Autorité de Certification (AC) - Une Autorité de Certification a en charge l'application d'au moins une Politique de Certification et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du certificat), dans les certificats émis au titre de cette Politique de Certification.

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC, le terme « certificat électronique » désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé d'authentification, de signature et de chiffrement, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, ...).

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

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 et en conformité avec la ou les Politiques de Certification qu'elle s'est engagée à respecter.

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 porteurs et les utilisateurs de certificats.

Porteur - Cf. chapitre 1.3.4.

Utilisateur de certificat - Cf. chapitre 1.3.5.

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

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

L'AC Racine doit mettre en œuvre au sein de l'IGC une fonction de publication des certificats et une fonction d'information sur l'état des certificats. La fonction de publication et d'information sur l'état des certificats s'appuie sur la génération d'une LAR.

L'AC Racine étant hors ligne, toutes les actions de publication se font de manière manuelle.

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

L'AC Racine a pour obligation de publier au minimum les informations suivantes à destination des porteurs et des utilisateurs de certificats :

- Sa Politique de Certification ;
- Ses LAR ;
- Les certificats de l'AC Racine et des AC Filles en cours de validité.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

La PC de l'AC Racine est publiée lors de sa création puis lors de chaque modification majeure. Le délai de publication de cette PC est de 7 jours [VT::T_PUB_PC] à compter de sa validation.

Les LAR de l'AC Racine doivent être publiées annuellement ou sur demande. Le délai de publication de cette LAR est de 7 jours [VT::T_PUB_LAR].

Les certificats produits par l'AC Racine doivent être publiés avant la création d'un certificat de porteur par les AC Filles. Le délai de publication des certificats signés par l'AC Racine est de 7 jours [VT::T_PUB_C_RACINE].

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

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

L'accès aux interfaces permettant la modification de ces informations doit mettre en œuvre au minimum une authentification de type login/mot 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 X509v3, l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un « Distinguished Name » DN de type X.501.

Ce DN est encodé en UTF8String.

Une identification de l'entité à laquelle le porteur est rattaché est obligatoire : elle se fait par le numéro de SIREN. Le SIREN du CNES est 775 665 912.

L'attribut countryName (C) est présent et indique le pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère, ...).

L'attribut organizationName (O) est présent et contient le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes.

Une instance de l'attribut organizationalUnitName (OU) est présente et contient l'identification de cette entité.

Pour cela, cette instance (OU) est structurée conformément à la norme ISO 6523. Le format retenu est :

- L'ICD est sur 4 caractères ;
- L'identification de l'organisation sur 35 caractères ;
- Le séparateur entre les deux chaînes est un espace.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms utilisés dans les champs « issuer » et « subject » des certificats d'AC Racine et des AC Filles sont explicites dans le périmètre du CNES. Ces noms sont définis au chapitre 7 du présent document. Ils sont renseignés et validés lors de la Cérémonie des Clés de l'AC Racine.

3.1.3 Anonymisation ou pseudonymisation des porteurs

Sans objet.

3.1.4 Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

L'unicité des noms des AC Racine et Filles est assurée au cas par cas lors de la validation de chaque demande de certificat par la Direction de l'AC.

3.1.6 Identification, authentification et rôle des marques déposées

Sans objet.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1 Méthode pour prouver la possession de la clé privée

La génération des clés d'AC doit être effectuée dans des circonstances parfaitement contrôlées dans le cadre d'une « Cérémonies de Clés » apportant la garantie sur la possession d'une clé privée.

3.2.2 Validation de l'identité d'un organisme

Sans objet.

3.2.3 Validation de l'identité d'un individu

Sans objet.

3.2.4 Informations non vérifiées du porteur

Sans objet.

3.2.5 Validation de l'autorité du demandeur

La validation de l'autorité du demandeur est assurée dans le cadre d'une Cérémonies de Clés dont le déroulement est décrit dans le document Guide pour la Cérémonie des Clés de l'IGC du CNES.

Seule la Direction de l'AC a autorité pour initier une Cérémonie des Clés. La Direction de l'AC est également garante de la validation de l'autorité du demandeur lors de la demande de certificat d'une AC Fille.

3.2.6 Critères d'interopérabilité

La Direction de l'AC gère et documente les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité de l'IGC.

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

Le renouvellement de la bi-clé d'une AC entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni sans renouvellement de la bi-clé correspondante.

Le renouvellement des clés et certificats des AC doit s'effectuer au cours d'une Cérémonie des Clés.

3.3.1 Identification et validation pour un renouvellement courant

Sans objet.

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

Tout acteur du Système d'Information du CNES peut formuler une demande de révocation. Néanmoins, toute révocation d'une AC doit être préalablement validée par la Direction de l'AC.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1 Origine d'une demande de certificat

Les besoins de création d'une AC Fille sont soumis à l'appréciation de la Direction de l'AC.

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

Si la Direction de l'AC juge le besoin justifié, elle initialise la Cérémonie des Clés correspondante.

Le processus est décrit dans le document Guide pour la Cérémonie des Clés de l'IGC du CNES.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

La Direction de l'AC doit valider la demande lors de la Cérémonie des Clés correspondante.

Le processus est décrit dans le document Guide pour la Cérémonie des Clés de l'IGC du CNES.

4.2.2 Acceptation ou rejet de la demande

Le traitement réservé à la demande doit être notifié. En cas de rejet, le détail de la cause du rejet doit être indiqué.

4.2.3 Durée d'établissement du certificat

Le temps imparti pour valider une demande de certificat et lancer une nouvelle Cérémonie des Clés est de 2 semaines [VT::T_ETAB_C_RACINE].

4.3 DELIVRANCE DU CERTIFICAT

Le certificat de l'AC Racine est délivré au cours de la Cérémonie des Clés correspondante suivant le processus décrit dans le document Guide pour la Cérémonie des Clés de l'IGC du CNES.

Les certificats des AC Filles sont délivrés lors d'une Cérémonie des Clés suivant le processus décrit dans le document Guide pour la Cérémonie des Clés de l'IGC du CNES.

Les acteurs de la Cérémonie des Clés attestent du bon déroulement de la cérémonie par rapport aux processus pré-établis.

4.3.1 Actions de l'AC concernant la délivrance du certificat

Sans objet.

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

Sans objet.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 Démarche d'acceptation du certificat

Les certificats de l'AC Racine et des AC Filles sont acceptés au cours de la Cérémonie des Clés.

4.4.2 Publication du certificat

Dans la mesure où l'AC Racine est hors ligne, la publication des certificats doit se faire de manière manuelle.

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

L'AC Racine étant hors ligne, sa bi-clé ne doit être utilisée que lors de la mise en service de cette AC Racine, à partir des secrets partagés entre différents porteurs. La clé privée de l'AC ne doit être utilisée que pendant la période de validité du certificat pour la signature de certificats d'AC Filles et de LAR.

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

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats définis dans la présente PC au chapitre 1.4. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 RENOUELEMENT D'UN CERTIFICAT

Le renouvellement du certificat d'une AC n'est pas autorisé dans le cadre de la présente PC.

Si des modifications de date de validité doivent être apportées, il est nécessaire d'effectuer une nouvelle demande.

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

4.7.1 Causes possibles de changement d'une bi-clé

La durée de validité des bi-clés de l'AC Racine est égale à la durée de validité des certificats associés à savoir 29 ans [VT::T_C_AC_Racine].

La fin de validité du certificat entraîne la génération d'une nouvelle bi-clé et du certificat associé pour chaque AC. Cette fin de validité peut avoir plusieurs origines :

- révocation du certificat pour des problèmes de sécurité provoquant un renouvellement anticipé de la bi-clé ;

- fin de vie du certificat provoquant le renouvellement de la bi-clé, dans le cas où le service doit continuer à être assuré.

Aussi, les bi-clés de chaque AC doivent être périodiquement renouvelées afin de minimiser les risques d'attaques cryptographiques.

4.7.2 Origine d'une demande d'un nouveau certificat

En cas de fin de vie d'un certificat d'AC, la procédure de création et de demande initiale de certificats doit être utilisée.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.7.5 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

Sans objet.

4.8 MODIFICATION DU CERTIFICAT

La modification de certificat n'est pas autorisée dans la présente PC. Si des modifications doivent être apportées, il est nécessaire d'effectuer une nouvelle demande.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1 Causes possibles d'une révocation

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

- compromission ou suspicion de compromission de la clé privée correspondante ou des éléments secrets protégeant cette clé ;
- perte ou vol des supports de conservation contenant les éléments secrets ;
- cessation d'activité de l'AC Racine ;
- par anticipation : par exemple, en cas de risque de mise en péril de l'IGC suite à l'apparition d'une faiblesse des clés ou algorithmes utilisés.

4.9.2 Origine d'une demande de révocation

Tout utilisateur du SI du CNES est en droit d'effectuer une demande de révocation qui doit nécessairement être validée par la Direction de l'AC.

4.9.3 Procédure de traitement d'une demande de révocation

La procédure de traitement doit inclure les étapes suivantes :

- vérification de l'origine de la demande ;
- vérification de l'applicabilité de la cause de révocation invoquée ;
- validation de la demande par la Direction de l'AC ;
- transmission de la demande à l'AC ;
- révocation effective ;
- révocation de l'AC Racine ;
- révocation des AC Filles ;
- publication de la LAR ;
- retrait du point de confiance (Certificat de l'AC Racine) ;
- plan de communication avec tous les moyens disponibles auprès de la « communauté d'utilisateurs ».

La révocation de l'AC Racine doit être suivie, dans les plus brefs délais, d'une annonce auprès des utilisateurs du SI du CNES et auprès des partenaires qui utilisent des certificats gérés par les AC Filles au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

De plus, un retour d'expérience doit être élaboré afin de procéder à l'analyse du traitement de la situation et si besoin, améliorer les procédures ou processus existants.

4.9.4 Délai accordé pour formuler une demande de révocation

De part la nature critique des certificats objets de la présente PC, une demande de révocation doit être formulée dans les meilleurs délais dès l'identification d'une cause possible de révocation.

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

Par nature, une demande de révocation pour une AC doit être traitée en urgence et dans un délai inférieur à 48h [VT::T_REV_TRAIT] sauf en cas de force majeure.

La fonction de gestion des révocations doit être disponible 24h/24, 7j/7 [VT::T_INF_DISP] et le service doit être assuré du lundi au vendredi 8h-18h [VT::T_AMP_SERV] avec :

- une durée maximale d'indisponibilité de 6h [VT::T_INDISP_MAX] ;
- un nombre d'indisponibilités maximum par mois de 2 [VT::NB_INDISP_MOIS] ;
- un nombre maximum d'indisponibilités par an de 8 [VT::NB_INDISP_AN].

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

L'utilisateur d'un certificat d'AC est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

La vérification peut être effectuée par vérification des LAR/LCR publiées.

4.9.7 Fréquence d'établissement des LAR

Dans un mode nominal, la fréquence de publication des LAR doit être de tous les ans [VT::F_PUB_LAR].

En revanche, lorsqu'une AC Fille est révoquée, la LAR doit être générée sur demande.

4.9.8 Délai maximum de publication d'une LAR

Les LCR doivent être publiées dans un délai de 7 jours [VT::T_PUB_LAR].

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

La fonctionnalité répondeur OCSP est disponible dans la solution implémentée mais n'est pas utilisée pour le moment en raison de problèmes de compatibilité avec certains équipements. Le service est prévu à terme, la PC s'engage donc uniquement sur la publication des certificats révoqués sur les LAR.

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

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Sans objet.

4.9.13 Causes possibles d'une suspension

La présente PC n'autorise pas la suspension de certificats.

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'AC Racine doit fournir 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.

La fonction d'information sur l'état des certificats doit au moins mettre à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LAR. Ces LAR doivent être des LCR au format V2, publiées au moins dans un annuaire accessible en protocole LDAP V3.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats doit être disponible 24h/24, 7j/7 [VT::T_INF_DISP]. Le service est assuré du lundi au vendredi 8h-18h [VT::T_AMP_SERV] avec :

- une durée maximale d'indisponibilité de 6h [VT::T_INDISP_MAX] ;
- un nombre d'indisponibilités maximum par mois de 2 [VT::NB_INDISP_MOIS] ;
- un nombre maximum d'indisponibilités par an de 8 [VT::NB_INDISP_AN].

4.10.3 Dispositifs optionnels

Sans objet.

4.11 FIN DE LA RELATION ENTRE UNE AC FILLE ET L'AC RACINE

En cas de fin de relation entre l'AC Racine et une AC Fille avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat d'AC Fille doit être révoqué.

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées d'AC ne doivent en aucun cas être 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

Ce chapitre traite des mesures de sécurité non techniques (c'est-à-dire concernant la sécurité physique, les procédures et la gestion du personnel) appliquées dans le but de sécuriser les fonctions de génération de clé, de délivrance des certificats, de révocation des certificats, d'audit et d'archivage.

5.1.1 Situation géographique et construction des sites

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

La construction des sites doit respecter les règlements et normes en vigueur au sein du CNES.

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'AC Racine, les accès aux locaux hébergeant le matériel (hors support des porteurs de secrets) nécessaire à la mise en service de l'AC Racine doivent être contrôlés.

L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée.

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 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

Idem chapitre 5.1.3 : les moyens de protection mis en place permettent de respecter le besoin de sécurité auquel répond l'IGC du CNES.

5.1.5 Prévention et protection incendie

Idem chapitre 5.1.3 : les moyens de protection mis en place permettent de respecter le besoin de sécurité auquel répond l'IGC du CNES.

5.1.6 Conservation des supports

Les supports (papier, disque dur, clé USB, CD, etc.) utilisés dans les activités de l'AC Racine doivent être traités et conservés afin de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations contenues.

5.1.7 Mise hors service des supports

Des procédures dédiées seront appliquées pour garantir l'effacement des éléments sensibles [DA3].

5.1.8 Sauvegardes hors site

Une sauvegarde est effectuée dans un local différent du local des serveurs de l'IGC en complément de la sauvegarde principale afin de permettre une reprise rapide des fonctions de l'IGC en cas d'incident.

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 Rôles de confiance

Les rôles de confiance suivants doivent être identifiés au sein de l'IGC pour l'AC Racine :

- **Responsable de la sécurité** : Le responsable de sécurité de l'IGC est chargé de la mise en œuvre de la Politique du CNES pour la Sécurité du Système d'Information [DA1]. Il a en charge la validation des habilitations d'accès à l'IGC ;
- **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 services rendus par cette application et des performances correspondantes ;
- **Opérateur** : Un opérateur au sein de l'AC Racine réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par l'AC Racine ;
- **Contrôleur** : Personne désignée par la Direction de l'AC et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'AC Racine par rapport à la Politique de Certification ;
- **Porteur de parts de secrets** : Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leurs sont confiées. Les porteurs retenus sont 3 directeurs du CNES.

Les opérations de sécurité de l'AC doivent être séparées des opérations normales. Les responsabilités des opérations de sécurité incluent :

- les procédures et responsabilités opérationnelles ;
- la protection contre les logiciels malicieux ;
- les opérations de maintenance ;
- la surveillance active des journaux d'audit, l'analyse des événements et leur traitement ;
- la manipulation et la sécurité des supports ;
- l'échange de données et de logiciels.

Ces responsabilités peuvent être réalisées par du personnel opérationnel non spécialiste dès lors que leurs activités sont dûment procédurées et encadrées.

Des mesures doivent être mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de chaque AC soient sortis du site sans autorisation.

5.2.2 Nombre de personnes requises par tâches

La DPC de l'IGC précise quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

5.2.3 Identification et authentification pour chaque rôle

La vérification de l'identité et de l'autorisation des personnes doit être effectuée dans les cas suivants :

- ajout d'une personne à la liste des personnes habilitées à accéder à l'AC Racine ou aux locaux l'hébergeant ;
- ouverture d'un compte à son nom dans un système.

Chaque attribution d'un rôle à un membre doit donner lieu à une trace écrite.

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. Pour les rôles de confiance, il est néanmoins nécessaire qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées :

- Responsable Sécurité et Opérateur ;
- Contrôleur et tout autre rôle ;
- Opérateur et Porteur de Secret.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

5.3.1 Qualifications, compétences et habilitations requises

Toutes les personnes amenées à travailler sur les composantes de l'AC Racine doivent être soumises à une clause de confidentialité du CNES.

Le personnel doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'AC Racine.

Toute personne intervenant dans des rôles de confiance de l'AC Racine doit être informée :

- de ses responsabilités relatives aux services de l'AC Racine ;
- des procédures liées à la sécurité du système.

5.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de son personnel amené à travailler au sein de la composante. Ce personnel ne doit notamment pas avoir de condamnation de justice en contradiction avec ses attributions.

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

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement, à la fréquence de tous les 3 ans [VT::F_V_ANT], par la Direction de l'AC.

5.3.3 Exigences en matière de formation initiale

Le personnel, lors de sa prise de fonction, est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions. Ce point est vérifié par le Contrôleur lors de ses activités.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

La DPC de l'IGC précise les procédures garantissant le maintien en sécurité de chacun des rôles. Plus particulièrement, lors de changements d'attribution de rôle, des conditions d'accès / identification, etc.

5.3.6 Sanctions en cas d'actions non autorisées

Toutes les personnes effectuant des actions non autorisées s'exposent à des sanctions conformément au règlement interne du CNES.

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du présent chapitre 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel doit disposer au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques à l'AC Racine qu'il utilise et met en œuvre.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

5.4.1 Type d'évènements à enregistrer

Toute opération sensible, c'est à dire manipulant des biens protégés, fait l'objet d'une trace fiable et auditable. La journalisation des événements est sous la responsabilité de l'AC Racine.

Ainsi, les événements suivants liés à l'AC Racine doivent être journalisés :

- Actions sur l'AC Racine :
 - validation / rejet d'une demande de certificat ;
 - génération des certificats d'AC ;
 - publication et mise à jour des informations liées à l'AC (PC, certificats d'AC) ;
 - validation / rejet d'une demande de révocation ;
 - génération puis publication des LAR ;
- Sécurité physique / organisation :
 - les accès physiques aux locaux hébergeant le matériel (hors support des porteurs de secrets) nécessaire à la mise en service de l'AC Racine ;
 - les changements apportés aux porteurs de secrets ;
 - les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, secrets, ...).

5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'évènements sont utilisés pour analyser les causes et origines de toute tentative, réussie ou non, d'actions non autorisées identifiées. Les journaux d'évènements sont traités et contrôlés à la fréquence tous les quinze jours [VT::F_CONT_JOUR].

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés durant 1 mois [VT::T_CONS_JOUR], puis archivés durant 6 mois [VT::T_ARCH_JOUR].

5.4.4 Protection des journaux d'évènements

Les journaux d'évènements font l'objet de mesures de protection afin de garantir leur confidentialité, leur traçabilité et leur intégrité. Le système de datage des événements est basé sur le serveur temps du CNES.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les mesures mises en œuvre sont décrites dans la DPC.

5.4.6 Système de collecte des journaux d'évènements

La politique de gestion des traces du CNES [DA2] impose la centralisation, la protection et l'exploitation des traces à fin de surveillance des systèmes. Le système de collecte des journaux d'évènements doit être conforme à cette politique.

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

La présente PC ne formule pas d'exigence particulière.

5.4.8 Evaluation des vulnérabilités

La présente PC ne formule pas d'exigence particulière.

5.5 ARCHIVAGE DES DONNEES

5.5.1 Types de données à archiver

Les données archivées sont :

- la PC ;
- les logiciels et fichiers de configuration des différentes composantes ;
- Les journaux d'évènements ;
- les certificats produits par l'AC Racine ;
- les LAR.

5.5.2 Période de conservation des archives

Les archives sont conservées pendant une durée minimale de 6 ans [T_CONS_ARCH].

5.5.3 Protection des archives

Pendant toute la durée de conservation, les archives, et leurs sauvegardes, doivent :

- être protégées en intégrité ;
- n'être accessibles qu'aux personnes autorisées.

La DPC de l'IGC précise les moyens mis en œuvre pour archiver les données de manière sécurisée.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

La présente PC ne formule pas d'exigence particulière.

5.5.6 Système de collecte des archives

La présente PC ne formule pas d'exigence particulière.

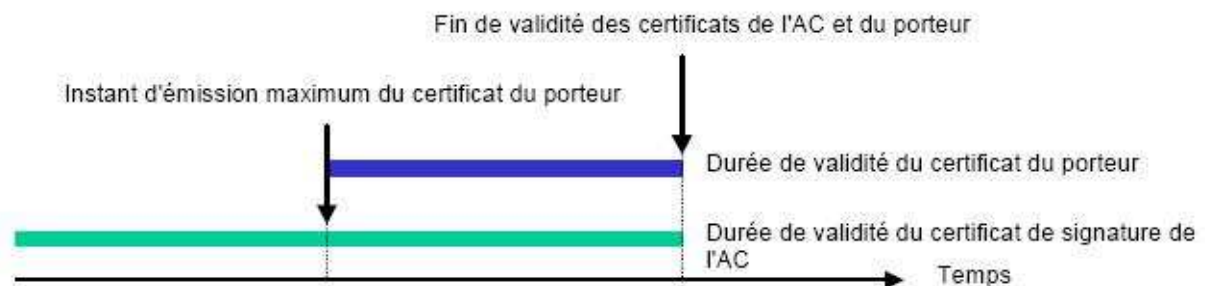
5.5.7 Procédures de récupération et de vérification des archives

Les archives (papiers et électroniques) doivent pouvoir être récupérées dans un délai inférieur à 2 jours ouvrés [VT::T_REC_ARCH].

5.6 CHANGEMENT DE CLE D'AC

L'AC Racine ne peut pas générer des certificats pour les AC Filles dont la date de fin serait postérieure à la date d'expiration du certificat de l'AC Racine.

De ce fait, la période de validité du certificat d'AC Racine est supérieure à celle des certificats des AC Filles. Lorsqu'un nouveau certificat pour l'AC Racine est émis, le certificat précédent ne doit plus être utilisé pour quelque usage que ce soit.



5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.

Dans le cas d'incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de clé privée d'AC, l'évènement déclencheur est le constat de l'incident au niveau de la composante concernée, qui doit en informer immédiatement le responsable de sécurité, le responsable d'application et la Direction de l'AC.

Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans le meilleur délai, par tout moyen utile et disponible (presse, site Internet, récépissé, ...).

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

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

Ce plan doit être testé au minimum 1 fois par an [VT::F_TEST_PLAN].

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

En cas de révocation d'une AC pour compromission de clés, suspicion de compromission, perte ou vol, l'ensemble des certificats signés par cette AC sont révoqués.

La révocation de toute composante de l'IGC pour ce type de cause entraîne la mise hors service de l'IGC.

La Direction d'AC proposera un contrôle de vérification et prononcera la remise en service de l'IGC et de la composante.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Cf. chapitre 5.7.2.

5.8 FIN DE VIE DE L'IGC

Une composante en fin de vie s'engage à :

- Remettre ses archives à la Direction de l'AC ;
- Communiquer à ses utilisateurs et à la Direction de l'AC de l'IGC son intention de cessation d'activité un mois avant la date de cessation ;
- Mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires (utilisateurs finaux, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité ;
- Faire révoquer son certificat par une Autorité de Certification supérieure.

La fin de vie de l'IGC fait suite à la fin de vie des toutes ses AC.

6 MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI CLES

6.1.1 Génération des bi-clés

Les bi-clés de l'AC Racine sont générées dans un environnement parfaitement contrôlé lors de la Cérémonie des Clés, à partir d'une souche logicielle. Les bi-clés sont ensuite « éclatées » à l'aide de l'algorithme de Shamir et conservées sur des supports répartis au minimum sur 2 acteurs.

6.1.2 Transmission de la clé privée à une AC Fille

Sans objet.

6.1.3 Transmission de la clé publique d'une AC Fille à l'AC Racine

La clé privée d'une AC Fille est transmise pour signature lors de la cérémonie des clés. La clé doit être protégée en intégrité et son origine doit être authentifiée.

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

La clé publique de vérification de signature de l'AC Racine doit être diffusée auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doit pouvoir être récupérée aisément par les utilisateurs de certificats.

6.1.5 Taille des clés

Les bi-clés des AC sont des clés RSA de taille 2048 bits.

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

Les bi-clés générées doivent être conformes aux exigences indiquées dans le chapitre 7 (taille et algorithmes notamment).

6.1.7 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LAR/LCR.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

L'AC Racine n'utilise pas de module cryptographique pour la génération des clés.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC Racine doit être assuré par au moins deux personnes parmi le personnel de confiance (porteurs de secrets de l'IGC).

6.2.3 Séquestre de la clé privée

Les clés privées d'AC ne doivent en aucun cas être séquestrées.

6.2.4 Copie de secours de la clé privée

Les supports des porteurs de secrets de l'AC Racine doivent faire l'objet d'une copie de secours.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne doivent en aucun cas être archivées.

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

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

Sans objet.

6.2.8 Méthode d'activation de la clé privée

La clé privée de l'AC Racine ne doit être activée que dans les cas suivants :

- signature d'une LAR ;
- signature des certificats des AC Filles.

L'activation est réalisée lors de la cérémonie des clés, en présence d'au moins 2 porteurs des secrets permettant de reconstituer la clé privée de l'AC Racine.

6.2.9 Méthode de désactivation de la clé privée

La désactivation de la clé privée de l'AC Racine est réalisée lors de la mise hors ligne de l'AC Racine.

6.2.10 Méthode de destruction des clés privées

La destruction de la clé privée est opérée par la destruction d'au moins un support permettant l'activation de l'AC Racine ainsi que leurs copies de secours éventuelles.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées

Sans objet.

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1 Archivage des clés publiques

Les clés publiques des porteurs sont archivées pendant 6 ans [VT:: T_CONS_ARCH].

6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats de l'AC Racine doivent avoir une durée de vie identique. Cette durée de vie est égale à 29 ans [VT:: T_C_AC_Racine].

La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats porteurs qu'elle émet.

6.4 DONNEES D'ACTIVATION

6.4.1 Génération et installation des données d'activation

Les données d'activation de l'AC Racine sont générées lors de la cérémonie des clés. Ces données d'activation ne doivent être 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

Les données d'activation de l'AC Racine doivent être protégées en intégrité et en confidentialité. Le porteur de secret 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 particulière.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Le PC et les logiciels (live CD) servant à l'exécution de l'AC Racine doivent être conservés de manière à assurer leur intégrité et leur disponibilité.

Les mécanismes mis en œuvre sont une combinaison de moyens techniques et organisationnels décrits dans la DPC.

6.5.2 Niveau de qualification des systèmes informatiques

Le SI intervenant au niveau de l'AC Racine étant hors ligne, la présente PC ne formule pas d'exigence particulière.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.6.1 Mesures de sécurité liées au développement des systèmes

Le fournisseur du système utilisé par l'IGC du CNES est engagé dans une démarche de certification de son produit auprès de l'ANSSI. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées (DPC).

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'AC Racine doit être signalée à la Direction de l'AC pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée.

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

La présente PC ne formule pas d'exigence particulière.

6.7 MESURES DE SECURITE RESEAU

L'AC Racine étant hors ligne, aucune mesure particulière de sécurité réseau n'est à mettre en œuvre. Aucune connexion réseau de l'AC Racine n'est autorisée lorsque celle-ci est activée.

6.8 HORODATAGE / SYSTEME DE DATATION

Sans objet.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

Les chapitres suivants donnent la description du profil des certificats de l'AC Racine.

La terminologie suivante est utilisée pour indiquer l'utilisation d'un champ :

- M : Mandatory (Obligatoire) – le champ doit être présent ;
- O : Optional (Optionnel) -le champ est optionnel ;
- X : Interdit – le champ ne doit pas être renseigné ;
- C : Critique.

7.1 PROFIL DES CERTIFICATS

Le tableau ci-dessous détaille le contenu du certificat de l'AC Racine :

Champ défini dans la norme	Utilisation du champ	Exigences sur le contenu	Commentaires
Certificate	M		
TBSCertificate	M		
Version	M	2	« 2 » pour la version 3 Les certificats utilisés dans le cadre de la présente PC doivent respecter la recommandation X509v3
SerialNumber	M		Le numéro de série généré doit être unique
Signature	M	Sha-1WithRSAEncryption	OID de l'algorithme de signature Cette valeur doit être identique à celle enregistrée dans le champ « AlgorithmIdentifier ». Cette structure donne des informations sur l'algorithme de signature utilisé par l'AC pour signer les certificats
Issuer	M	CN=AC RACINE, OU=0002 775665912, O=CNES, C=FR	
Validity	M	NotBefore "date de creation" NotAfter "date de création + T_C_AC_Racine"	Le format UTCTime est utilisé Aucun certificat généré ne doit comporter un numéro de seconde égal à 00. l'IETF ainsi que l'ISO recommandent d'utiliser l'UTCTime jusqu'en 2049. Après, le type Generalized Time doit être utilisé
Subject	M	CN=AC RACINE, OU=0002 775665912, O=CNES, C=FR	Ce champ est identique à « issuer » dans le cas d'un certificat autosigné
SubjectPublicKeyInfo	M		Ce champ est une structure contenant les informations sur la clé publique du certificat de l'AC Racine (algorithme <i>rsaEncryption</i> + valeur de la clé publique)
AlgorithmIdentifier	M	RSAEncryption (Parameter = NULL)	
subjectPublicKey	M	clé publique de 2 048 bits + exp. Pub	
IssuerUniqueID	X		La présente PC imposant l'unicité des DN des champs issuer et subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés
SubjectUniqueID	X		
Extension	M	Voir 7.1.2	
SignatureValue	M	Signature du certificat, calculée avec la clé privée de l'AC Racine	Ce champ contient une signature numérique calculée à partir du codage ASN.1 DER de la structure <i>tobeSigned</i> . Le code ASN.1 DER de la structure <i>tobeSigned</i> est utilisé comme une entrée à la fonction de signature

7.1.1 Numéro de version

Le numéro de version doit être positionné à 2 pour utilisation de certificats de type X509v3.

7.1.2 Extensions du certificat

Le tableau ci-dessous décrit les extensions pour le certificat d'AC Racine :

Nom de l'extension	Utilisation du champ	Exigences sur le contenu	Commentaire
AuthorityKeyIdentifier	M	0	L'utilisation de cette extension permet d'accélérer la recherche du certificat de clé publique utilisé par l'AC pour signer un certificat
SubjectKeyIdentifier	M	Ce champ contient un identificateur unique de certificat de la clé publique certifiée (SHA1 de subjctPublicKey)	
KeyUsage	MC		
digitalSignature	X		
nonRepudiation	X		
keyEncipherment	X		
dataEncipherment	X		
keyAgreement	X		
keyCertSign	M		Signature de certificat
cRLSign	M		Signature de LCR
encipherOnly	X		
decipherOnly	X		
CertificatePolicies	M		
policyIdentifier CPSuri	M	1.2.250.1.12.1.1.1.1 http://www.cnes.fr/igc/PC_acracine.pdf	Ce champ contient l'identificateur de la PC de l'AC Racine utilisée pour émettre le certificat
Authority Information Access	X		
SubjectAltName	X		
IssuerAltName	X		
SubjectDirectoryAttributes	X		
BasicConstraints	MC		
cA	M	True	Ce champ indique que le certificat est un certificat d'AC
pathLenConstraint	X		
NameConstraints	X		
PolicyConstraints	X		
ExtKeyUsage	X		
serverAuth	X		
clientAuth	X		
codeSigning	X		
emailProtection	X		
timeStamping	X		
OCSPSigning	X		
Microsoft Smart Card Login	X		
InhibitAnyPolicy	X		
FreshestCRL	X		
PrivateInternetExtensions	X		
crlDistributionPoint	X		

7.1.3 OID des algorithmes

Les identificateurs d'algorithmes sont inscrits auprès du registre international ISO. Les algorithmes suivants sont utilisés par l'AC Racine :

Algorithme	Type	Identificateur d'objet
RSA	Asymétrique	
SHA-1	Hachage	

7.1.4 Forme des noms

Tous les DN doivent être au format UTF-8.

7.1.5 Contraintes sur les noms

Les dispositions relatives aux contraintes de noms sont celles édictées au chapitre 3.1.1.

7.1.6 OID des PC

L'AC Racine doit s'assurer que l'OID de la Politique de Certification est contenu dans les certificats qu'elle délivre. L'identificateur d'objet de la PC est référencé au chapitre 1.2.

7.1.7 Utilisation de l'extension « contraintes de politique »

Les certificats émis par l'AC Racine n'utilisent pas d'extension de contraintes de politique.

7.1.8 Sémantique et syntaxe des qualifiants de politique

Sans objet.

7.1.9 Sémantiques de traitement des extensions critiques de la PC

Conformément à la norme X.509v3, le caractère critique doit être traité de la façon suivante selon que l'extension est critique ou non :

- si l'extension est non critique, alors :
 - si l'application ne sait pas la traiter, l'extension est abandonnée mais le certificat est accepté ;
 - si l'application sait la traiter, alors :
 - si l'extension est conforme avec l'usage que l'application veut en faire, l'extension est traitée ;
 - si l'extension n'est pas conforme avec l'usage que l'application veut en faire, l'extension est abandonnée, mais le certificat est accepté ;
- si l'extension est critique, alors :
 - si l'application ne sait pas la traiter, le certificat est rejeté ;
 - si l'application sait la traiter, alors :
 - si l'extension est conforme avec l'usage que l'application veut en faire, l'extension est traitée ;
 - si l'extension n'est pas conforme avec l'usage que l'application veut en faire, le certificat est rejeté.

7.2 PROFIL DES LAR

Le profil des LAR de l'AC Racine est le suivant :

Champ défini dans la norme	Utilisation du champ	Contenu	Commentaire
CertificateList	M		
toBeSigned	M		
Version	M	« 1 » (pour version 2)	
Signature	M	Sha-1WithRSAencryption	OID de l'algorithme de signature Cette valeur doit être identique à celle enregistrée dans le champ « AlgorithmIdentifier » Cette structure donne des informations sur l'algorithme de signature utilisé par le fournisseur de la LAR pour signer cette même LAR



CENTRE NATIONAL D'ÉTUDES SPATIALES

Politique de certification de l'AC Racine de l'IGC du CNES

Référence : DCS//SI-2010.26059

Version : 1.0

Date : 30/11/2010

Page : 34/42

Champ défini dans la norme	Utilisation du champ	Contenu	Commentaire
Issuer	M	CN=AC RACINE, OU=0002775665912, O=CNES, C=FR	Ce champ contient le nom de l'AC ayant signé la LAR
thisUpdate	M	« date / heure d'émission de la LCR » (Date encodée au format UTF8)	Ce champ renseigne la date à laquelle la LAR a été émise, c'est-à-dire la date à laquelle le fournisseur désigné dans le champ « issuer » a signé la LAR
nextUpdate	M	« date / heure d'émission + T_VAL_LAR prévue de la prochaine LAR » (Date encodée au format UTF8)	Ce champ contient la date prévue de génération prochaine d'une LAR
revokedCertificates	M	Liste de certificats révoqués, avec pour chaque entrée : - userCertificate - revocationDate - crlEntryExtensions (optionnel)	Cette séquence contient une liste de certificats révoqués avec leur date effective de révocation par l'AC Racine
crlExtensions	M	Cf. chapitre 7.2.2	Une extension de LAR qualifie la liste de certificats révoqués dans son ensemble
algorithmIdentifier	M	Sha-1WithRSAEncryption	Ce champ est une structure contenant les informations sur l'algorithme utilisé pour signer la LAR
signatureValue	M	Signature de la LCR, calculée avec la clé de l'AC Racine	Ce champ contient une signature numérique calculée à partir du codage ASN.1 DER de la structure tobeSigned. Le code ASN.1 DER de la structure tobeSigned est utilisé comme une entrée à la fonction de signature. La valeur de cette signature est ensuite encodée en ASN.1 comme un « BIT STRING » et incluse dans le champ de signature de la LAR

7.2.1 Numéro de version

Le numéro de version doit être positionné à 1.

7.2.2 Extensions de LAR et d'entrées de LAR

Les extensions suivantes sont utilisées :

Nom de l'extension	LCR	Contenu	Commentaire
AuthorityKeyIdentifier	M	SHA1 Clé privée de l'AC Racine	L'utilisation de cette extension permet d'accélérer la recherche du certificat de clé publique utilisé par l'AC pour signer un certificat

7.3 PROFIL OCSP

Sans objet.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et évaluations ont pour objectif de s'assurer que l'implémentation faite de l'AC Racine est conforme aux dispositions écrites dans la présente PC.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Un premier audit est effectué après la première mise en service de l'AC Racine.

Un contrôle partiel de conformité à la PC est réalisé tous les ans [VT::F_REV_PC] et un contrôle total est effectué tous les 3 ans [VT::F_REV_PC_TOTAL].

Les audits de conformité peuvent être anticipés dans certains cas exceptionnels :

- évolution majeure de la PC ou de l'infrastructure technique ;
- incident majeur de sécurité.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

Le contrôle d'une composante doit être assigné par la Direction de l'AC 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 est nommée par la Direction de l'AC au sein de la Direction Centrale de la Sécurité ou d'un autre service n'appartenant pas à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante. Elle est 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 définies.

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à la Direction de 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 la Direction de l'AC 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 la Direction de l'AC et doit respecter ses politiques de sécurité internes ;
- En cas de résultat « A confirmer », la Direction de l'AC 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'AC confirme à la composante contrôlée la conformité aux exigences de la PC.

8.6 COMMUNICATION DES RESULTATS

Les résultats de l'audit doivent être communiqués au minimum à la Direction de l'AC.

Les résultats sont tenus à disposition des personnes accréditées, en lecture.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

Sans objet.

9.2 RESPONSABILITE FINANCIERE

Sans objet.

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

Sans objet.

9.4 PROTECTION DES DONNEES PERSONNELLES

Sans objet.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

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

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

9.6.1 Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs (chapitre 1.3.5) qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat ;
- Garantir et maintenir la cohérence de la DPC avec les PC ;
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

9.6.2 Service d'enregistrement

Sans objet.

9.6.3 Porteurs de certificats

Sans objet.

9.6.4 Utilisateurs de certificats

Les utilisateurs de certificats doivent pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation).

9.6.5 Autres participants

Sans objet.

9.7 LIMITE DE GARANTIE

Sans objet.

9.8 LIMITE DE RESPONSABILITE

Sans objet.

9.9 INDEMNITES

Sans objet.

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1 Durée de validité

La présente PC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

L'arrêt d'activité de l'AC Racine, programmée ou suite à un sinistre majeur, entraîne la fin de validité de la présente PC.

9.10.3 Effets de la fin de validité et clauses restant applicables

La fin de validité de cette PC rend caducs les engagements qui y sont portés.

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

La présente PC ne formule pas d'exigence particulière.

9.12 AMENDEMENTS A LA PC

9.12.1 Procédures d'amendements

Un contrôle partiel de conformité à la PC est réalisé tous les ans [VT::F_REV_PC] et un contrôle total est effectué tous les 3 ans [VT::F_REV_PC_TOTAL] afin de s'assurer de sa conformité aux bonnes pratiques du marché.

Les évolutions de la PC sont de 2 types :

- évolutions mineures ;
- évolutions majeures.

Le numéro de version de PC est défini sous la forme X.YY ou X défini le numéro de version principal et YY le numéro de version mineur.

Toute évolution majeure de la PC doit être validée par la Direction de l'AC.

9.12.2 Mécanisme et période d'information sur les amendements

La présente PC ne formule pas d'exigence particulière.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Une évolution majeure de la PC doit entraîner une évolution de l'OID associé.

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

La présente PC ne formule pas d'exigence particulière.

9.14 JURIDICTIONS COMPETENTES

Tout tribunal compétent sur le territoire français.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

L'AC est soumise aux dispositions prévues par l'article 31 de la LSQ concernant la remise des clés privées des porteurs, si celles-ci sont séquestrées par l'AC.

9.16 DISPOSITIONS DIVERSES

9.16.1 Accord global

La présente PC ne formule pas d'exigence particulière.

9.16.2 Transfert d'activités

La présente PC ne formule pas d'exigence particulière.

9.16.3 Conséquences d'une clause non valide

Au cas où une clause de la présente PC s'avère être non valide au regard de la loi, ceci ne remet pas en cause la validité et l'applicabilité des autres clauses.

9.16.4 Application et renonciation

La présente PC ne formule pas d'exigence particulière.

9.16.5 Force majeure

Sont considérés comme cas de force majeure tous les cas habituellement retenus par les tribunaux français.

9.17 AUTRES DISPOSITIONS

La présente PC ne formule pas d'exigence particulière.



CENTRE NATIONAL D'ÉTUDES SPATIALES

Politique de certification de l'AC Racine de l'IGC du CNES

Référence : DCS//SI-2010.26059

Version : 1.0

Date : 30/11/2010

Page : 41/42

10 ANNEXE 1 : VARIABLES DE TEMPS

Variable	§PC	Description	Valeur
T_INF_DISP	4.9.5	Disponibilité de la fonction de publication des informations	24h/24 7j/7
T_AMP_SERV	4.9.5	L'amplitude où le service est assuré d'après le SLA appliqué à l'IGC	Du lundi au vendredi 8h-18h
T_INDISP_MAX	4.9.5	Temps d'indisponibilité maximum	6h
NB_INDISP_MOIS	4.9.5	Nombre maximum d'indisponibilités par mois	2
NB_INDISP_AN	4.9.5	Nombre maximum d'indisponibilité par an	8
T_REV_TRAIT	4.9.5	Délai maximum de traitement d'une demande de révocation	48h
F_V_ANT	5.3.2	Fréquence de revue des antécédents	Tous les 3 ans
F_CONT_JOUR	5.4.2	Fréquence de contrôle des journaux d'événements	Tous les quinze jours
T_ARCH_JOUR	5.4.3	Durée d'archivage des journaux d'événements	6 mois
T_CONS_JOUR	5.4.3	Durée de conservation des journaux d'événements	1 mois
T_CONS_ARCH	5.5.2	Durée de conservation des archives	6 ans
T_REC_ARCH	5.5.7	Délai de récupération des archives	2 jours ouvrés
F_REV_PC	8.1	Fréquence de revue des PC	Tous les ans
F_REV_PC_TOTAL	8.1	Fréquence de revue totale des PC	Tous les 3 ans
AC Racine			
T_PUB_C_RACINE	2.3	Délai de publication des certificats de l'AC Racine	7 jours
T_ETAB_C_RACINE	4.2.3	Durée d'établissement d'un certificat de l'AC Racine	2 semaines
T_PUB_PC	2.3	Délai de publication de la PC de l'AC Racine	7 jours
T_PUB_LAR	2.3	Délai de publication des LAR	7 jours
F_PUB_LAR	4.9.7	Fréquence de publication des LAR	Tous les ans
T_VAL_LAR	7.2	Durée de validité d'une LCR	1 an
F_TEST_PLAN	5.7.2	Fréquence de test du plan de continuité	1 fois par an
T_C_AC_Racine	6.3.2	Durée de vie des certificats de l'AC Racine	29 ans
T_C_AC	6.3.2	Durée de vie d'un certificat d'AC	10 ans

11 ANNEXE 2 : DOCUMENTS APPLICABLES ET DE REFERENCE

DA1	Politique du CNES pour la Sécurité du Système d'Information
DA2	Directive pour la gestion des traces
DA3	Directive pour la protection des informations non classifiées de défense