Politique de Certification AC RACINE ALMERYS

ALMERYS ROOT CA

P

Procédure

Référentiel :	Sous-Référentiel :	Référence :	Statut :
securite	PKI	1.2.250.1.16.12.5.41.1.1.1	
Approuvé par :	**Fonction :**	**Date :**	**Signature :**
MMI	Responsable sécurité des services de confiance	30/11/2012	
Validé par :	**Fonction :**	**Date[•] :**	**Signature :**
JMT	Autorité de Gouvernance	30/11/2012	
Diffusion auprès de:			
En accès pour :			
Localisation :			

Sommaire

Date de péremption			Responsable de l'actualisation	
Version	**Date**	**Modifications**		**Auteur**
v1.1	30/08/2012	Création		MMI
v1.2	30/11/2012	Création		MMI

[•] Date d'entrée en vigueur

Documents de référence

Référence	Version	Titre du document

Sommaire détaillé

1. INTRODUCTION

1.1 PRESENTATION GENERALE

Le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification Racine Almerys nommée dans ce document «ALMERYS AC ROOT» ou « ACR ».

Sa structure est conforme au document [RFC3647].

L'objectif de ce document est de définir la Politique de Certification (PC) de l'Infrastructure de Gestion de Clés (IGC) d'Almerys et en particulier les exigences concernant les certificats d'Autorité de Certification (AC) de cette IGC émis par l'ACR, dans toutes les phases de leur cycle de vie.

L'émission de certificats d'AC a les objectifs suivants :

- favoriser le succès des services offerts par Almerys et principalement renforcer la sécurité des échanges et offrir des services de confiance (authentification, signature) dans le cadre de ses activités auprès de ces clients et notamment les organismes de remboursement complémentaires santé : mutuelles, assurances, institutions de prévoyance et assureurs sociaux ;
- répondre à des besoins de sécurité internes : fonctionnalité de chiffrement SSL pour les serveurs, signature et chiffrement de mail, authentification forte des utilisateurs, etc.

L'infrastructure de l'IGC s'appuie sur l'ACR qui peut produire les certificats d'une ou plusieurs AC intermédiaires (encore appelées AC Filles). Ceci permet de développer d'autres IGC mutualisées autour de cette racine commune, laquelle offre un modèle commun d'architecture de confiance permettant de garantir l'identité des AC délivrant des certificats au nom d'Almerys.

Les AC intermédiaires ne produisent pas de certificats d'AC, mais seulement des certificats finaux (personnes physiques, serveurs), ce sont donc des AC opérationnelles : chaque AC intermédiaire produit des certificats dans un cadre de service et pour des usages clairement définis. La description de ces usages est disponible dans les différentes PC de ces AC opérationnelles.

1.2 IDENTIFICATION DU DOCUMENT

La présente PC est dénommée « Infrastructure de Gestion de Clés Almerys – Politique de Certification de l'AC Racine « ALMERYS AC ROOT» (PC ACR).

La référence interne de ce document est : PAL035

L'identifiant d'objet (OID) du présent document est : 1.2.250.1.16.12.5.41.1.1.1

1.3 ENTITES INTERVENANT DANS L'AC RACINE D'ALMERYS

1.3.1. Autorité de Certification (AC)

L'Autorité de Certification (AC) est une entité morale au nom de laquelle sont émis des certificats. Elle a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et est à ce titre identifiée dans ses certificats en tant qu'émetteur.

Dans le cas de l'IGC Almerys, on considère une AC Racine (ACR), unique, dont l'objet est exclusivement de signer des certificats d'AC de rang inférieur Filles (ACF), sans production de certificats destinés à des entités finales (personnes physiques, serveurs).
Le certificat de l'AC Racine de l'IGC Almerys est auto-signé et représente le socle de la confiance en l'IGC Almerys. La hiérarchie de confiance de l'IGC Almerys est représentée dans la figure suivante :

La mise en œuvre opérationnelle de l'ACR Almerys est principalement à la charge de:

- L'Autorité de Gouvernance de l'AC Racine (AG-ACR) qui est l'autorité responsable de l'ensemble des services de l'IGC, elle a un pouvoir décisionnaire au sein de l'IGC. Elle définit les PC et vérifie la conformité des DPC par rapport aux PC. Sur le périmètre couvert par chaque AC Fille.

Les autres intervenants participant à la mise en œuvre opérationnelle de l'AC Racine Almerys sont définis dans le §1.3.5 « Autres participants ».

Remarque importante : chaque fois que, dans le présent document, les paragraphes concernent une AC générique, le terme « AC » est utilisé, dans les autres cas, il est clairement précisé « AC Racine Almerys » (ACR Almerys) ou AC intermédiaire de premier niveau encore appelée « AC Fille » (ACF).

Fonctions d'une IGC

Afin de clarifier et faciliter l'identification des exigences de l'AC Racine, la décomposition fonctionnelle des fonctions génériques d'une IGC à mettre en œuvre par l'OC, est la suivante :

- fonction de génération et signature de certificats ;
- fonction de génération des éléments secrets ;
- fonction de publication ;
- fonction de gestion des révocations ;
- fonction d'information sur l'état des certificats.

1. **Fonction de génération et signature de certificats d'AC**

Cette fonction génère les certificats à partir des informations transmises par l'Autorité d'Enregistrement (ci-dessous, § 1.3.2) et de la clé publique de l'AC Fille à certifier (création du format, signature électronique avec la clé privée de l'AC Racine).

2. **Fonction de génération des éléments secrets d'AC**

Cette fonction n'est pas assurée par l'AC Racine Almerys car elle ne génère pas d'autre élément secret que sa propre bi-clé. Chaque AC Fille doit générer sa bi-clé en respectant les exigences définies dans l'annexe §11 « Exigences de sécurité du module cryptographique de l'AC ».

3. **Fonction de publication**

Cette fonction met à disposition des différentes parties concernées, les politiques voir conditions générales et pratiques publiées par l'AC Racine, les certificats d'AC et toute autre information pertinente destinée aux représentants des AC Filles et/ou aux utilisateurs de certificats d'AC, hors informations d'état des certificats.

4. **Fonction de gestion des révocations**

Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) soumises par l'Autorité de Gouvernance d'une AC Fille à lAC Racine, demandes avalisés par l'AG de l'ACR Almerys. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

5. **Fonction d'information sur l'état des certificats**

Cette fonction fournit aux utilisateurs de certificats d'AC des informations sur l'état des certificats d'AC (valides, révoqués, suspendus). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (Liste des certificats d'AC Révoqués).

La mise en œuvre opérationnelle de ces fonctions peut être effectuée par une ou plusieurs composante(s) de l'IGC (opérateurs techniques et/ou autorités tel que AG, AE, …).

1.3.2. Autorité d'Enregistrement (AE)

L'AE est un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC Racine Almerys et les représentants des AC Filles.
Les demandes de rattachement d'ACF sont soumises à l'AG ACR qui est habilitée à traiter le dossier, approuver la demande de certification de l'ACF et initier le processus de génération des certificats.
Le rôle d'AE de l'ACR Almerys est, de fait, tenu par l'AG-ACR.

1.3.3. Porteurs de Certificats

Sans objet (seules les AC Filles gèrent les relations avec les utilisateurs finaux pour lesquels elles émettent des certificats).

1.3.4. Utilisateurs de Certificats

Les seuls certificats produits par l'ACR Almerys étant des certificats d'AC, les utilisateurs sont les processus qui vérifient le chemin de certification des AC Filles et des certificats qu'elles délivrent.

1.3.5. Autres participants

La mise en œuvre opérationnelle de l'AC Racine Almerys est effectuée par plusieurs composantes :

1.3.5.1. Autorité de Gouvernance (AG)

Voir §1.3.1 pour la définition de l'Autorité de Gouvernance.
Cette entité est pilotée par le Responsable de l'Autorité de Gouvernance (RAG).

1.3.5.2. Responsable services de confiance

Directement rattaché à l'AG, Il est en charge des services de confiance Almerys.

Le responsable des services de confiance est en charge :

- De toutes les politiques de certification des AC Almerys et fait valider les politiques par l'autorité de gouvernance,
- veille au respect de la conformité des DPC, et des procédures IGC avec les PC,
- la gestion des certifications des services de confiance,
- la gestion des fournisseurs de produits de sécurité intervenant dans la construction de l'IGC Almerys.

1.3.5.3. Détenteurs de Secrets (DS)

Les Détenteurs de Secret sont sélectionnés, avant la Cérémonie des Clés, par l'Autorité de Gouvernance, au sein des personnes ayant une responsabilité dans l'Infrastructure de Gestion de Clés d'Almerys (Autorité de Gouvernance, personnel Almerys, etc.).
Leur nombre et leur engagement assure la disponibilité et la confidentialité des éléments permettant la remise en service de l'AC Racine.

1.3.5.4. Huissier, témoins

Un Huissier est mandaté lors de la Cérémonie des Clés de l'AC Racine (il peut aussi être requis pour les Cérémonies des Clés des AC Filles). Il a pour rôle de valider officiellement que le déroulement de la procédure est conforme à ce qui est décrit dans [KCR].

Des témoins peuvent être aussi invités à assister à tout ou partie des procédures, afin d'attester aussi de leur exécution comme prévu.

1.3.5.5. Agents de sécurité

Ces agents assurent le contrôle d'accès aux locaux. Ils sont nécessaires lors des Cérémonies des Clés organisées par l'ACR Almerys (voir [KCR] § 3.5) ainsi qu'à chaque remise en service de l'AC Racine.

1.4 USAGES DE CERTIFICATS

1.4.1. Domaines d'utilisation applicables

Les certificats générés par l'AC Racine Almerys sont destinés aux AC Filles d'Almerys qu'elle fédère.
Ces AC peuvent être des Autorités de Certification hors ligne ou en ligne.

Les domaines d'utilisation des certificats internes de l'IGC se répartissent en deux catégories :

- la bi-clé et le certificat d'AC de l'AC Racine Almerys (certificat auto-signé unique), utilisés pour signer les certificats des AC Filles rattachées à l'AC Racine, et signer la Liste des Certificats d'AC Révoqués (LCR, ou plus précisément LAR) ;
- les bi-clés et les certificats d'AC des AC Filles signés par l'AC Racine Almerys. Ils sont utilisés uniquement pour la signature des certificats utilisateurs finaux, chacun de ces certificats peut être utilisé sur le domaine défini dans le dossier de demande proposé par l'AG de chaque AC Fille et validé par l'AG-ACR.

1.4.2. Domaines d'utilisation interdits

Toute autre utilisation des bi-clés et des certificats d'AC que les utilisations prévues dans cette PC (§4.5) est interdite.
L'AC Racine Almerys doit respecter ces restrictions et imposer leur respect par les AC Filles concernées.

1.5 GESTION DE LA PC

1.5.1. Entité gérant la PC

L'Autorité de Gouvernance, responsable de la présente PC, est Almerys.

1.5.2. Point de contact

L'AG est l'entité à contacter pour toutes questions concernant la présente PC.

Autorité de Gouvernance IGC ALMERYS
Téléphone : 04 73 74 58 90
Almerys – 46 rue du Ressort – 63967 CLERMONT-FERRAND CEDEX 9

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

L'entité déterminant la conformité d'une DPC associée à cette PC est l'Autorité de Gouvernance de l'IGC Almerys.

1.5.4. Procédures d'approbation de la conformité de la DPC

La procédure d'approbation de la conformité de la DPC est décrite dans cette DPC.

1.6 ACRONYMES ET DEFINITIONS

1.6.1. Acronymes

Les acronymes utilisés dans le référentiel de l'IGC Almerys sont les suivants :

AA	Autorité d'Archivage [Archived Authority (AA)]
AC	Autorité de Certification [Certification Authority (CA)]
ACF	Autorité de Certification Fille (Autorité de Certification opérationnelle)
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement [Registration Authority (RA)]
AG	Autorité de Gouvernance [Governance Authority (GA)]
AH	Autorité d'Horodatage [Time-stamping Authority (TA)]
ALE	Autorité Locale d'Enregistrement [Local Registration Authority (LRA)]
AR	Autorité de Recouvrement [Recovery Authority]
CC	Critères Communs [Common Criteria (CC)]
CEN	Comité Européen de Normalisation
CSP	Cryptographic Service Provider
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification [Certification Practice Statement (CPS)]
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IAM	Identity Acces Managment
IGC	Infrastructure de Gestion de Clés [Public Key Infrastructure (PKI)]
KC	Cérémonie des Clés (Key Ceremony)
LAR	Liste des certificats d'AC Révoqués [Authority Revocation List]
LCR	Liste des Certificats Révoqués [Certificate Revocation List (CRL)]
MC	Mandataire de Certification
OC	Opérateur de Certification [Certification Operator (CO)]
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification [Certification Policy (CP)]
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure – X 509
PP	Profil de Protection [Protection Profile (PP)]
PSCE	Prestataire de Services de Certification Electronique
RAE	Responsable d'Autorité d'Enregistrement
RAG	Responsable de l'Autorité de Gouvernance
ROC	Responsable de l'Opérateur de Certification
RSA	Rivest Shamir Adelman
SSI	Sécurité des Systèmes d'Information [Information Technology Security (ITS)]
URL	Uniform Resource Locator

1.6.2. Définitions

Les termes utilisés dans le référentiel de la politique de l'IGC Almerys sont les suivants :

Applications utilisatrices :
Services applicatifs exploitant les certificats émis par l'Autorité de Certification, par exemple, pour des besoins d'authentification ou de signature à partir des cartes Cleyris.

Authentification [Authentication] :
L'authentification vise à renforcer selon le besoin, le niveau de confiance entre l'identifiant et la personne associée (exemples : le mot de passe est un authentifiant faible, la carte à puce associé à un code PIN est un authentifiant fort).

Autorité de Certification (AC) [Certificate Authority (CA)] :
Entité qui délivre et est responsable des certificats électroniques signés en son nom.

Remarque :
L'AC Almerys assure elle-même l'exploitation de l'IGC, elle dispose de locaux sécurisés, du personnel et de l'infrastructure technique qui lui permettront de réaliser l'ensemble des tâches de gestion des certificats.

Autorité d'Enregistrement (AE) [Registration Authority (RA)] :
L'AE est un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC et les porteurs de certificats.
L'AE a pour rôle de vérifier l'identité du futur porteur de certificat.

Autorité de Gouvernance (AG) [Governance Authority (GA)] :
L'entité, responsable de l'ensemble des fonctions de l'IGC avec pouvoir décisionnaire, L'AG ALMERYS est responsable de toutes les ACs ALMERYS..

Autorité de Recouvrement (AR) [Recovery Authority] :
L'AR a pour rôle de séquestrer et de recouvrer les clés des porteurs de certificat.

Bi-clé [Key Pair] :
Couple clé publique / clé privée (utilisé dans des algorithmes de cryptographie asymétrique).

Cérémonie des Clés ou Key Ceremony (KC) : réunion spéciale des personnes autorisées pour générer le certificat d'une Autorité de Certification. La bi-clé de ce certificat doit être générée avec toutes les précautions nécessaires (voir la DPC) pour éviter sa compromission.

Certificat électronique [Digital Certificate] :
Fichier électronique attestant qu'un bi-clé appartient à la personne physique ou morale ou à l'élément matériel 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 et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Chiffrement [Encryption] :
Transformation cryptographique d'un ensemble de données (clair) en vue de produire un ensemble chiffré (dit cryptogramme).

Composante de l'IGC
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.

Confidentialité [Confidentiality] :
Propriété d'une information ou d'une ressource de n'être accessible qu'aux utilisateurs autorisés (création, diffusion, sauvegarde, archivage, destruction).

Déchiffrement [Decryption] :
Transformation d'un cryptogramme en vue de retrouver les données originelles en clair.

Déclaration des Pratiques de Certification (DPC) [Certification Pratice Statement (CPS)] :
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.

Dispositif de protection de clés privées
Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre ses clés privées.

Hardware Security Module (HSM) : voir Module matériel de sécurité

Horodatage [Time-stamping] :
Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé (fonction décrite dans la norme « procédure d'horodatage prévue dans la norme NF Z 42-013).

Infrastructure de Gestion de Clés (IGC) [Public Key Infrastructure (PKI)] :
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, de mandataires de certification, d'une entité d'archivage, d'une entité de publication…

Intégrité [Integrity] :
Propriété d'exactitude et de complétude des informations et des fonctions de l'information traitée. Celles-ci ne doivent pouvoir être modifiées que par un acte volontaire et légitime.

Liste des certificats d'AC Révoqués (LAR) :
Liste de certificats d'AC révoqués c'est-à-dire invalidés avant leur terme.

Liste de Révocations de Certificats (LRC) ou Liste de Certificats Révoqués (LCR) [Certificate Revocation List (CRL)] :
Liste de certificats révoqués c'est à dire invalidés avant leur terme.

Mandataire de Certification (MC) :
Personne physique en charge de l'ALE.

Module matériel de sécurité : matériel dédié à la génération, au stockage et à la destruction d'éléments cryptographiques sensibles (clés privées, secrets). L'usage d'un Module matériel de sécurité rend très difficile la compromission des éléments qu'il contient (divulgation, altération) grâce à des protections physiques et cryptographiques.

Non-répudiation [Non-repudiation] :
Impossibilité pour un utilisateur de nier sa participation à un échange d'information ; cette participation porte tant sur l'origine de l'information (imputabilité) que sur son contenu (intégrité).

Online Certificate Status Protocol (OSCP) :
Protocole permettant à une personne de vérifier la validité d'un certificat, en particulier s'il a été révoqué.

PKI (Public Key Infrastructure) : cf. Infrastructure de Gestion de Clés (IGC).

PKIX (Public Key Infrastructure – X509) :
Groupe de travail de l'IETF (Internet Engineering Task Force) visant à faciliter la genèse d'IGC basées sur la norme X.509 pour des applications Internet. PKIX a produit des normes telles que les extensions de X.509 pour l'Internet, OCSP, etc.

Politique de Certification (PC) [Certification Policy (CP)] :
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 de certificat [Subscriber] :
Un porteur de certificats ne peut être qu'une personne physique.
Le porteur respecte les conditions qui lui incombent définies dans la PC de l'AC.

Prescripteur de Services de Certification Electronique (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 porteurs et utilisateurs de ces certificats (cf. Opérateur de Certification).

Produit de sécurité
Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaire 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.

Voir également Module matériel de sécurité, ou HSM

Promoteur d'application
Un fournisseur d'une offre de service sécurisé (échanges dématérialisés).

Responsable d'Autorité d'Enregistrement (RAE) :
Personne physique en charge de l'AE.

Réseau Privé Virtuel (RPV) [Virtual Private Network (VPN)] :
Réseau privé d'entreprise multi-sites utilisant les réseaux d'opérateur pour leur interconnexion.

Signature numérique [Digital signature] :
Transformation électronique permettant d'assurer l'authentification du signataire et éventuellement celle d'un document signé par lui. .

Tiers de confiance [Trusted Third Party (TTP)] :
Organisme chargé de maintenir et gérer pour un tiers, dans le respect des droits des utilisateurs, les clés de chiffrement ou d'authentification.

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

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Les informations publiées le sont en direction exclusivement des AC Filles ALMERYS; ces AG-ACF ne publient ces informations vers d'autres entités qu'avec l'accord exprès de l'AG de l'AC Racine Almerys.

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

Les informations à publier par l'AC Racine Almerys à destination des d'AC Filles sont :

- la politique de certification;
- la Liste des Certificats d'AC Révoqués (LAR) ;
- les certificats émis par l'AC Racine y compris son propre certificat autosigné ;
- la liste des AC avec lesquelles l'ACR Almerys a des accords de reconnaissance, la nature et le contenu synthétique de ces accords ainsi que les certificats croisés résultant de ces accords.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Toute nouvelle version des informations et documents relatifs à l'AC Racine Almerys doit faire l'objet d'une publication. Certaines informations doivent être publiées avec une fréquence déterminée ; en particulier, une nouvelle LAR est émise en fin de chaque Cérémonie des Clés.
Le certificat AC racine est préalablement à toute émission de certificats et/ou de LCR correspondants sous délai minimum de 72 heures.
Pour les Listes de Certificats Révoqués sont mises à jour tous les 6 mois minimum. Une fois la mise à jour effectuée, la LCR est publiée dans un délai maximum de 2 heures.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'IGC Almerys pouvant nécessiter une visibilité à l'extérieur, l'ensemble des informations publiées est du niveau de confidentialité « Diffusion libre ». Ce niveau de confidentialité doit être respecté par les Autorités de Gouvernances des AC de l'IGC Almerys qui seront amenées à publier une partie de ces informations.
L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC (cf. §1.3.1), au travers d'un contrôle d'accès adapté.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1. Convention de noms d'AC

Les noms utilisés dans les certificats émis par l'AC Racine Almerys sont conformes aux spécifications de la norme X.500.
Dans chaque certificat X.509v3, le champ « issuer » (AC émettrice, soit l'AC Racine d'Almerys) et le champ « subject » (AC Fille) sont identifiés par un « Distinguish Name ».
Les noms utilisés pour l'AC Racine Almerys elle-même sont définis dans la section 7.

3.1.2. Nécessité d'utilisation de noms d'AC explicites

Les noms utilisés dans les champs « issuer » et « subject » d'un certificat d'AC sont explicites pour Almerys, ses clients et partenaires, i.e. qu'ils identifient sans ambiguïté la Société Almerys comme émettrice de ce certificat. Ces champs contiennent en particulier son code SIREN.

3.1.2.1. AC RACINE

Pour l'AC Racine Almerys, le format exact du DN du certificat d'AC est précisé au paragraphe 7.1« Profil du certificat de l'AC Racine « Almerys Root CA »:

- CN=Almerys Root CA
- OU=0002 432701639
- O=ALMERYS
- C=FR

Etant autosigné, les champs « issuer » et « subject » de ce certificat d'AC Racine Almerys sont identiques.

3.1.2.2. AC FILLE

Pour les AC fille, le format exact du DN du certificat d'AC est précisé au paragraphe 7.2 « Profil du certificat de l'AC Fille :
Les ACs services avancées :

- CN= "Non de l'AC Fille"
- OU=ADVANCED SERVICES
- OU=0002 432701639
- O=ALMERYS
- C=FR

Les ACs Trust services :

- CN= "Non de l'AC Fille"
- OU=TRUST SERVICES
- OU=0002 432701639
- O=ALMERYS
- C=FR

3.1.3. Anonymisation ou pseudonymisation des AC

L'anonymisation ou la pseudonymisation des certificats d'AC de l'IGC Almerys est interdite.

3.1.4. Règles d'interprétation des différentes formes de nom

Les noms utilisés sont conformes aux standards X.500.

3.1.5. Unicité des noms

L'AC racine Almerys veille à l'unicité des noms distinctifs des ACs générés dans son domaine.

3.1.6. Identification, authentification et rôle des marques déposées

L'Autorité de Gouvernance de l'AC Racine est responsable de l'unicité des noms d'AC (AC Racine comme AC Fille(s)) et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1. Méthode pour prouver la possession de la clé privée

La bi-clé de l'AC Racine Almerys et le certificat d'AC associé sont générés lors de la Cérémonie des Clés de l'AC Racine Almerys et sont stockés conformément à la procédure [KCR].
Pour chaque AC Fille, la bi-clé de l'AC Fille et le certificat d'AC associé sont également générés lors de la Cérémonie des Clés de cette AC Fille.
La preuve de procession de la clé privée de l'AC fille repose sur la vérification de la signature numérique de la requête de certificat de l'AC fille.

3.2.2. Validation de l'identité d'un organisme

L'identité de l'organisme (entités, statut, portée et identification telles qu'attendues et présentées dans le certificat d'AC) est validée préalablement par l'Autorité de Gouvernance.

3.2.3. Validation de l'identité d'un individu

Sans objet pour les certificats d'AC, les seuls manipulés par l'AC Racine Almerys.

3.2.4. Informations non vérifiées du porteur

Sans objet pour les certificats d'AC, les seuls manipulés par l'AC Racine Almerys.

3.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la procédure d'acceptation de rattachement à l'AC Racine Almerys d'une AC Fille.

3.2.6. Critères d'interopérabilité

L'Autorité de Gouvernance de l'AC Racine Almerys gère et documente les demandes d'accords de reconnaissance avec des AC extérieures au domaine de la PKI Almerys.

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

3.3.1. Identification et validation pour un renouvellement courant des clés

Il n'est pas prévu de renouvellement des clés de l'AC Racine Almerys ni des AC filles dans cette version de la PC.

3.3.2. Identification et validation pour un renouvellement des clés après révocation

idem §3.3.1

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

La demande de révocation doit émaner et être valider de l'AG.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DU CERTIFICAT D'AC

Sauf mention spécifique, ce chapitre ne traite pas du certificat d'AC de l'AC Racine Almerys mais seulement des autres certificats signés par de cette AC : les certificats d'AC Filles.

4.1 DEMANDE DE CERTIFICAT D'AC

4.1.1. Origine d'une demande de certificat d'AC

Le dossier de demande de certificat d'AC doit être établi par l'Autorité de Gouvernance, elle s'effectue lors de la KC AC FILLE en présence de l'AG ou de son représentant.

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

L'établissement de la demande d'un certificat d'AC Fille est sous la responsabilité de l'AG.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT D'AC

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

Le responsable de services de confiance almerys organise à la demande de l'AG, la Cérémonie de clés (KC) correspondante de l'AC Fille. La génération du certificat AC Fille nécessite l'intervention de deux officiers de sécurité de l'AC RACINE en présence de l'AG ou de son représentant.

4.2.2. Acceptation ou rejet de la demande

L'Autorité de Gouvernance Almerys peut souverainement rejeter, suspendre ou ajourner le traitement de la demande de certificat (c'est-à-dire la Cérémonie des Clés) de l'AC Fille si les conditions requises ne sont pas atteintes.

4.2.3. Durée d'établissement du certificat d'AC

La durée de vie du certificat de l'AC Racine Almerys est de 24 ans (cf. §7).

La durée de vie d'un certificat d'AC Fille est définie dans le fichier de profil de certificat correspondant.
Dans tous les cas, une AC Fille ne peut pas avoir de certificat dont la date de fin serait postérieure à la date d'expiration du certificat de l'AC Racine.

4.3 USAGES DU BI-CLE ET DU CERTIFICAT D'AC

4.3.1. Utilisation de la clé privée et du certificat par l'AC

Cas de l'AC Racine Almerys :

L'utilisation de la clé privée de l'AC Racine Almerys et du certificat associé est limitée aux conditions d'usage définies pour l'AC Racine (cf. § 1.4 de la présente PC : génération de certificats d'AC, génération des LAR) et ceci conformément à l'utilisation spécifique décrite dans le contenu du certificat (cf. §7 à propos du paramètre « keyUsage »).

L'utilisation de la clé privée de l'AC Racine et du certificat associé n'est autorisée que pendant la période de validité du certificat associé : cf. § 4.2.3 de la présente PC.
La clé privée de l'AC Racine doit toujours être stockée chiffrée et ne peut être mise en œuvre qu'à l'intérieur d'un HSM (cf. § 6.2 de la présente PC).

Cas des AC Filles :
L'usage de la clé privée et du certificat associé est limité aux conditions d'usage définies pour cette AC Fille (cf. §1.4)de la PC de l'AC concernée : génération de certificats d'entités finales, génération des Liste de révocation et ceci conformément à l'utilisation spécifique décrite dans le contenu du certificat (cf. exemple de profil de certificat d'AC Fille, à propos du paramètre «keyUsage»).
L'utilisation d'une clé privée et/ou du certificat associé n'est autorisée que pendant la période de validité du certificat associé.
Une clé privée d'AC Fille doit toujours être stockée chiffrée et ne peut être mis en œuvre qu'à l'intérieur d'un HSM (cf. PC et DPC applicables à cette AC).

4.3.2. Utilisation de la clé publique et du certificat d'AC par l'utilisateur de certificat

Les utilisateurs (processus) des certificats doivent respecter strictement les usages autorisés des certificats de l'AC Racine Almerys et ses AC Filles. Dans le cas contraire, la responsabilité du propriétaire du processus serait engagée.

4.4 RENOUVELLEMENT D'UN CERTIFICAT D'AC

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

Il n'est pas possible de renouveler un certificat d'AC sans renouvellement (nouvelle génération) du bi-clé correspondant.

4.5 DELIVRANCE D'UN NOUVEAU CERTIFICAT D'AC SUITE A CHANGEMENT DE BI-CLE

Conformément à la [RFC3647], ce paragraphe traite de la délivrance d'un nouveau certificat suite à la génération d'une nouvelle bi-clé.
La délivrance d'un nouveau certificat à une AC Fille suit la même procédure que lors de la première génération CF (§4.1).

4.6 MODIFICATION DU CERTIFICAT D'AC

Conformément à [RFC3647], la notion de « modification de certificat » correspond à des modifications d'informations sans changement de la clé publique (cf. §4.7) et autres que uniquement la modification des dates de validité (cf. §4.6)
La modification du certificat d'AC Fille n'est pas autorisée.

4.7 REVOCATION ET SUSPENSION DES CERTIFICATS D'AC FILLE

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

4.7.1. Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'un certificat d'AC Fille :

- suspicion de compromission, compromission, indisponibilité, 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.

Cette liste n'est pas exhaustive.

4.7.2. Origine d'une demande de révocation

La révocation d'un certificat d'AC (Racine ou Fille) peut être décidée par :

- l'Autorité de Gouvernance,
- le responsable des services de confiance Almerys
- ou sur ordre des autorités judiciaires compétentes suite à une décision de justice.

4.7.3. Procédure de traitement d'une demande de révocation

Les procédures de traitement d'une demande de révocation du certificat d'AC d'une AC Fille sont détaillées dans la DPC de l'AC Racine.

4.7.4. Délai accordé à l'AG d'une AC pour formuler la demande de révocation

La demande de révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat.

4.7.5. Délai de transmission par l'AC Racine d'une demande de révocation

Par nature une demande de révocation doit être traitée en urgence.
Toute demande de révocation d'un certificat d'AC doit être traité dans un délai inférieur à 24h (jours ouvrés); 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.

4.7.6. Exigences de vérification de la révocation par les utilisateurs des certificats d'AC

Les utilisateurs de certificats sont tenus de vérifier l'état d'un certificat signé par l'AC Racine Almerys avant son utilisation.

4.7.7. Fréquence d'établissement de la LAR de l'AC Racine

La fréquence de publication des LCR doit être conforme est de un 6 mois minimum. La durée de validité est de 180 jours

4.7.8. Délai maximal de publication de la LAR de l'AC Racine

Une LCR doit être publiée dans un délai maximal conforme à 2H suivant sa génération.

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

Sans objet.

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

Cf. chapitre 4.9.6 ci-dessus.
Les moyens de vérification sont sous la responsabilité des AC Filles dont les [processus] utilisateurs auraient besoin de vérifier en ligne la révocation – ou non – des certificats d'AC Fille.

4.7.11. Autres moyens disponibles d'information sur les révocations

Pas d'exigence spécifique.

4.7.12. Exigences spécifiques en cas de compromission de la clé privée de l'AC

Pour les certificats d'AC Filles, outre les exigences du § 4.9.3 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information comme indiqué dans la DPC de l'AC Fille en cause.

4.7.13. Causes possibles d'une suspension

Sans objet : la suspension de certificats n'est pas autorisée dans l'AC Racine.

4.7.14. Origine d'une demande de suspension

Sans objet.

4.7.15. Procédure de traitement d'une demande de suspension

Sans objet.

4.7.16. Limites de la période de suspension d'un certificat

Sans objet.

4.8 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS D'AC

Il appartient aux utilisateurs de certificats de vérifier et valider préalablement à son utilisation, le statut d'un certificat et de sa chaîne de certification.

4.8.1. Caractéristiques opérationnelles

Les caractéristiques opérationnelles de cette fonction d'information sont détaillées dans la DPC associée à cette PC.
La fonction d'information sur l'état des certificats signés par l'AC Racine Almerys (certificats d'AC Racine et Filles uniquement) est limitée à la lecture du fichier de LCR.

Cette fonction proposée par l'AC Racine est seulement accessible aux responsables des AC Filles. Ce sont les AC Filles opérationnelles qui doivent fournir aux utilisateurs des certificats émis par ces AC les moyens de vérifier et valider préalablement à son utilisation, le statut d'un certificat et de sa chaîne de certification, c'est-à-dire de vérifier également les signatures et le statut des certificats d'AC de la chaîne. (LCR en ligne sur une page web, par exemple). Le détail de cette implémentation est donné dans la PC de l'AC concernée.

4.8.2. Disponibilité de la fonction

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

4.8.3. Dispositifs optionnels

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

4.9 FIN DE LA RELATION ENTRE L'AC FILLE ET L'AC RACINE

En cas de fin de relation contractuelle entre l'ACR et une AC Fille avant la fin de validité du Certificat, ce dernier est révoqué.
Cette fin de relation doit être compatible avec les engagements pris par l'ACR vis-à-vis des différentes AC Filles pour lesquelles elle a produit des certificats.

4.10 SEQUESTRE DE CLE ET RECOUVREMENT

L'AC Racine Almerys ne séquestre aucune clé privée d'AC Fille. Le séquestre et le recouvrement de la clé privée de l'AC Racine Almerys sont traités dans le chapitre 6.

5. MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

L'Autorité de Gouvernance de l'AC Almerys s'engage à mettre en œuvre et maintenir le niveau de sécurité physique exigé pour les locaux d'exploitation des composantes de l'IGC.

5.1.1. Situation géographique et aménagement du site

Remarque : la plate-forme de l'AC Racine Almerys est la plupart du temps « démontée » et sous séquestre. Sauf indication contraire, les paragraphes ci-dessous concernent les périodes où cette AC est mise en service. Les sites abritant les composants de l'AC Racine Almerys sont définis au niveau 1 : impact vital (majeur pour l'entreprise).

A ce titre, la mise en sécurité du site et du bâtiment doit respecter les mesures de sécurité physiques de niveau 1 pour la protection périphérique, périmétrique et intérieure et notamment les mesures relatives à :

- l'alimentation électrique et climatisation ;
- la vulnérabilité aux dégâts des eaux ;
- la prévention et protection incendie.

Les mesures doivent également permettre de respecter les engagements pris dans la PC, en matière de disponibilité des services, notamment les services de génération de certificats, de gestion des révocations et d'état des certificats.

5.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'AC Racine Almerys, les accès aux locaux des différentes composantes de l'AC Racine Almerys doivent être contrôlés conformément au niveau de zonage des locaux de niveau 1 : accès très restreint.

Pour les fonctions de génération des éléments secrets, de signature des certificats et LCR et de gestion des révocations, l'accès doit être strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. De plus, le contrôle en entrée et en sortie est maintenu en heures non ouvrées (HNO).
Afin d'assurer la disponibilité des systèmes, l'accès aux machines doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC doivent définir un périmètre de sécurité physique où sont installées ces machines. Tout local utilisé en commun entre la composante concernée et une autre composante (de ou hors de l'IGC) doit être en dehors de ce périmètre de sécurité.

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'AC « ALMERYS AC ROOT» telles que fixées par leurs fournisseurs.

5.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection mis en place par l'AC ALMERYS AC ROOT permettent de protéger son infrastructure contre les dégâts des eaux..

5.1.5. Prévention et protection incendie

l'AC ALMERYS AC ROOT met en places des moyens de protection et de lutte contre les incendies.

5.1.6. Conservation des supports

Les supports (papier, disque dur, disquette, CD-ROM, clé USB, etc.) utilisés au sein de l'AC Racine Almerys sont traités et conservés conformément aux procédures retenues pour le niveau 1.

5.1.7. Mise hors service des supports

Lors de la maintenance des matériels et en fin de vie de l'AC Racine, les supports de données devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes..

5.1.8. Sauvegardes hors site

En temps normal, l'AC Racine est éteinte et sa plate-forme démontée. Les composants permettant la remise en conditions opérationnelles de cette AC peuvent être sauvegardés hors site comme indiqué dans la DPC de l'AC Racine.

En complément de sauvegardes sur site, il est recommandé que 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 services après incident la plus rapide possible, et conforme aux exigences de la présente PC en matière de disponibilité, en particulier pour les fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.2 MESURES DE SECURITE PROCEDURALES

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés ([KCR]).

5.2.1. Rôles de confiance

Les rôles de confiance définis ci-dessous sont ceux requis pour l'IGC, indépendamment des rôles de confiance définis dans le cadre de la Cérémonie des Clés :

Chaque entité de l'IGC doit distinguer les rôles fonctionnels de confiance suivants :

- Officier de Sécurité de l'IGC (PKI Security Officer) – L'Officier de Sécurité est chargé de la mise en œuvre de la politique de sécurité de l'AC « ALMERYS AC ROOT». Il gère les contrôles d'accès physiques aux équipements des systèmes de l'entité. Il est habilité à prendre connaissance des documents conservés, et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- Responsable d'application – Le responsable d'application est chargé, au sein de la composante de l'IGC concernée, de la mise en œuvre des différentes PC et DPC de l'AC « ALMERYS AC ROOT». Sa responsabilité couvre l'ensemble des fonctions rendues par les applications 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 l'entité. Il assure l'administration technique des systèmes et des réseaux de l'entité.
- Opérateur – Un opérateur au sein de la composante de l'IGC concernée réalise, dans le cadre de ses attributions, l'exploitation des applications pour les services délivrés par la composante de l'IGC.

- auditeur – Personne désignée par le responsable de la composante de l'IGC et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des services fournis par la composante de l'IGC par rapport aux PC, aux DPC de l'AC « ALMERYS AC ROOT».

Les personnels techniques requis pour la Cérémonie des Clés ou toute autre opération sur la plate-forme de l'AC Racine Almerys seront choisis parmi les personnes de confiance de l'IGC Almerys.

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 seront définis dans la DPC, en particulier les personnes requises pour chaque action de la Cérémonie des Clés.

5.2.3. Identification et authentification pour chaque rôle

Chaque entité intervenant dans la cadre de l'AC Racine Almerys (cf § 1.3) doit faire vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant les systèmes concernés par le rôle,
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes,
- qu'un compte soit ouvert à son nom dans ces systèmes, si nécessaire,
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

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 services offerts.
Les attributions associées à chaque rôle sont décrits dans la DPC de l'AC Racine Almerys.
Les règles particulières s'appliquant aux détenteurs de secrets de l'AC Racine sont détaillées dans le document [KCR].

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

Les mesures de sécurité vis-à-vis du personnel ci-après complètent celles définies dans le cadre de la Cérémonie des Clés.

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC Almerys doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur. Les agents d'autorités administratives sont soumis à leur devoir de réserve. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Chaque entité opérant une composante de l'IGC Almerys doit s'assurer que les attributions de ses personnels, amener à travailler au sein de la composante, correspondent à leurs compétences professionnelles.
Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC Almerys.

L'Autorité de Gouvernance et le responsable de sécurité, doivent informer toute personne intervenant dans des rôles de confiance de l'IGC Almerys :

- de ses responsabilités relatives aux services de l'IGC Almerys,
- des procédures liées à la sécurité du système et au contrôle du personnel.

Les qualifications, compétences et habilitations requises sont précisées dans la DPC.

5.3.2. Procédures de vérification des antécédents

Les personnels amenés à travailler au sein d'une composante de l'IGC, et en fonction du contexte applicable, sont amenés à remettre une attestation sur l'honneur de non-condamnation, un extrait de casier judiciaire, ou un engagement de confidentialité.
Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3. Exigences en matière de formation initiale

Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter au sein de l'entité pour laquelle il opère.
Les membres du personnel doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.3.4. Exigences et fréquence en matière de formation continue

Suite à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc., le personnel concerné doit recevoir, préalablement à l'évolution, une information et une formation adéquate en fonction de la nature de l'évolution.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Pas d'exigence spécifique de l'Autorité de Gouvernance Almerys.

5.3.6. Sanctions en cas d'actions non autorisées

Ce point fait l'objet du traitement RH standard en application dans l'entité concernée. Des références aux règles définies à ce sujet dans le règlement intérieur ainsi que la charte informatique sont notamment possibles.

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 Almerys doit également respecter les exigences du présent chapitre.
Chaque prestataire signe personnellement un engagement de confidentialité l'engageant lui et son employeur.

5.3.8. Documentation fournie au personnel

Chaque membre du personnel doit disposer au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de l'entité.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'événements 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, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

Rappel : l'AC Racine Almerys est éteinte et démontée la majorité du temps, il n'y a d'événements nouveaux à enregistrer que lors de sa remise en service : pour les Cérémonies de Clés des AC Filles ou la révocation de celles-ci, ainsi que lors d'opérations de maintenance de la plate-forme de l'AC Racine.

Dans la cas de l'AC Racine Almerys, les journaux sont :

- Script de la Cérémonie des Clés ([KCR]) effectuée devant témoins : ce document est annoté et visé par un huissier, puis confié à l'Autorité de Gouvernance de l'AC Racine ;
- Liste des Secrets et Détenteurs de Secrets, signée pour chaque élément par son détenteur. Cette liste est gérée par l'Autorité de Gouvernance de l'AC Racine et permet de tracer chaque élément sensible de l'AC Racine ;
- Pour toute autre intervention sur l'AC Racine, un script détaillant les opérations, signé par ses acteurs et par l'AG-ACR, sert de journal en vue d'un audit. Ce script est remis à l'Autorité de Gouvernance de l'AC Racine.

5.4.1. Type d'événements à enregistrer

Toute action sur un dossier lié à un certificat émis par l'AC RACINE doit être enregistrée, et un historique complet du dossier doit être conservé dans la base de données de l'AC RACINE.
De plus, les événements suivants font l'objet d'un enregistrement électronique par l'application IGC :

- acceptation ou refus de connexion à l'application IGC ;
- génération de certificat d'AC racine;
- génération des certificats AC Fille;
- demande de révocation ;
- révocation de certificat AC Fille;
- génération de la LCR ;
- modification des droits des personnels autorisés à intervenir auprès de l'application IGC ;
- modification des paramètres de configuration de l'application IGC.

Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants :

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

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'événements.
De plus, en fonction du type de l'événement, chaque enregistrement devra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'événement.

5.4.2. Fréquence de traitement des journaux d'événements

La fréquence de traitement des journaux d'événements n'est pas prédictible pour une AC offline ; cette fréquence est calquée sur la fréquence d'établissement des processus de l'ACR : Signature Certificat AC Fille, Génération et Signature CRL AC Racine, Maintien Conditions Opérationnelles AC Racine, Révocation AC Fille, etc.

5.4.3. Période de conservation des journaux d'événements

Les enregistrements des journaux doivent être conservés au sein de l'application IGC sans limitation de durée.

5.4.4. Protection des journaux d'événements

Les journaux d'événements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non) : voir le § 5.4.5 ci-dessous.
Le système de datation des événements doit respecter les exigences du chapitre 6.8.

La définition de la sensibilité des journaux d'événements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin supplémentaire de protection en confidentialité, indiqué le cas échéant dans la DPC.

5.4.5. Procédure de sauvegarde des journaux d'événements

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risque de l'ACR Almerys.
Dans le cas de l'AC Racine Almerys, les journaux (sur support papier) sont sauvegardés dans un ou plusieurs meubles de sécurité, à l'usage exclusif de l'Autorité de Gouvernance.

5.4.6. Système de collecte des journaux d'événements

Sans objet pour l'AC Racine Almerys.

5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

Les opérations sur l'AC Racine se déroulent en présence de toutes les parties concernées ; elles sont de facto informées de l'enregistrement éventuel des événements les concernant.

5.4.8. Evaluation des vulnérabilités

L'AC doit mettre en œuvre une gestion des vulnérabilités de l'AC Racine Almerys afin d'être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

5.5 ARCHIVAGE DES DONNEES

5.5.1. Types de données à archiver

Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC (liste des journaux : voir § 5.4 Procédures de constitution des données d'audit).
Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les licences et contrats de maintenance ;

- la PC de l'AC Racine ;
- la DPC de l'AC Racine ;
- les agréments contractuels avec d'autres AC ;
- les certificats d'AC (y compris celui de l'AC Racine) et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les journaux d'événements des différentes entités de l'AC Racine Almerys. Dans la cas de l'AC Racine, ces journaux sont listés au § 5.4.

Ces données à archiver ne comprennent pas les secrets d'AC Racine, qui font l'objet du chapitre 6, notamment les paragraphes 6.2 seq.

5.5.2. Période de conservation des archives

En l'état de la législation et de la réglementation en vigueur (dite « Informatique et Libertés »), toute information de type :

- personnel,
- trafic,
- connexion,
- facturation,

et issue d'un processus automatique de traitement de données, n'est pas archivée pendant plus d'un an.

Les durées d'archivage sont les suivantes :

- PC : durée de vie de l'AC,
- documents organisationnels de cérémonies des clés : durée de vie de l'AC,
- DPC : durée de vie de l'AC,
- dossiers de demande de certificat : au moins 5 ans,
- certificats émis par l'AC après expiration : au moins 5 ans,
- dernière LCR émis par l'AC après expiration : au moins 5 ans,
- journaux d'événements après leur génération : au moins 5 ans.
-

5.5.3. Protection des archives

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

- être protégées en intégrité ;
- être accessibles aux personnes autorisées (protection en confidentialité) ;
- pouvoir être relues et exploitées (protection en disponibilité).

La DPC complète le document [KCR] et précise les moyens mis en œuvre pour protéger les archives.

5.5.4. Procédure de sauvegarde des archives

La DPC complète le document [KCR] et précise les procédures mises en œuvre pour sauvegarder les 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

Les certificats sont horodatés au moment de leur génération et cette information est archivée avec le certificat correspondant (voir [RFC3647], [PROFIL_ACR] §7).
L'horodatage du déroulement du script de la Cérémonie des Clés (valant journal) est effectué par un Huissier.
La DPC ou le script des autres interventions précise le niveau d'exigence souhaité dans l'horodatage des autres données.

5.5.6. Système de collecte des archives

Le système de collecte des archives est précisé dans la DPC de l'AC Racine. Il doit respecter 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, étant noté que seule l'AC 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'AC

Sans objet : il n'est pas prévu de changement de bi-clé de l'AC Racine Almerys.

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

Chaque composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents conformément aux exigences de la Politique de Sécurité d'Almerys.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC « ALMERYS AC ROOT», l'événement déclencheur est la constatation de cet incident. L'AG de l'IGC Almerys en est immédiatement informée. Le cas de l'incident majeur doit être impérativement traité dès la détection et la publication de l'information de révocation du Certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible.

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

Conformément à la Politique de Sécurité d'Almerys, l'AC « ALMERYS AC ROOT» dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité de ses fonctions sensibles, et découlant :

- de la présente PC,
- des engagements en termes de qualité de service des différentes composantes de l'IGC, notamment pour ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des Certificats.

Ce plan est testé au minimum une fois tous les 3 ans.

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

Le cas de compromission (cf. définition au § 4.9.1) d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante (cf. chapitre 5.7.2).

5.7.3.1. Dans le cas de compromission de l'AC Racine :

1. Tous les certificats d'AC Filles émis par l'AC Racine sont révoqués
3. Le certificat d'AC Racine doit être immédiatement révoqué.
4. Il n'y a pas de procédure de reprise : il n'est pas prévu de régénération du certificat d'AC Racine

5. Par application du principe de la PKI, tous les certificats d'AC Filles deviennent invérifiables. Leur PC doit préciser les implications d'une telle situation.
6. L'Autorité de Gouvernance de l'AC Racine Almerys et/ou le responsable des services de confiance Almerys prononcent éventuellement le transfert ou la cessation d'activité de l'IGC : cf. § 5.8. Ou régénération d'un nouveau certificat d'AC Racine puis de nouveaux certificats d'AC Filles.

5.7.3.2. Dans le cas de compromission d'une AC Fille :

A la demande de l'AG, Le certificat correspondant de l'AC Fille doit être immédiatement révoqué suivant la procédure donnée au § 4.9.3.
Le renouvellement du certificat d'AC Fille suit la procédure mentionnée au § 4.6.1.

5.7.4. Capacités de continuité d'activités suite à un sinistre naturel ou autre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. chapitre 5.7.2).

5.8 FIN DE VIE DE L'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité.

- Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'Autorité de Gouvernance en collaboration avec la nouvelle entité.
- La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC
Sans objet : Il n'est pas prévu de transfert de l'activité de l'AC Racine Almerys.

Cessation d'activité affectant l'AC Racine Almerys
Dans l'hypothèse d'une cessation d'activité totale, l'autorité de Certification ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans la présente PC (cf. § 5.7.3.1).

Lors de l'arrêt du service, l'autorité de gouvernance doit s'assurer :
1. de la récupération de toutes les copies de sauvegarde du HSM AC RACINE;
2. révoquer le certificat d'AC de l'AC Racine et si possible, explicitement tous les certificats d'AC Filles que l'AC Racine Almerys a signés et qui seraient encore en cours de validité : une nouvelle Liste des Certificats Révoqués est générée et signée ;
3. publier cette nouvelle LAR;
4. prendre toutes les mesures nécessaires pour détruire ou rendre inopérante la clé privée de l'AC Racine sur le HSM et les copies de sauvegarde;
5. informer les utilisateurs de la révocation effective du certificat de l'AC Racine.

6. MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI-CLES

6.1.1. Génération de bi-clés

La génération du bi-clé de signature de l'AC Racine Almerys est décrite dans la procédure de « Cérémonie des Clés » de l'AC Racine [KCR].
Les clés de signature d'AC RACINE sont générées et mises en œuvre dans un module cryptographique certifié Fips 140-2 Niveau 3
La génération du bi-clé de signature de chaque AC Fille est décrite dans la procédure de « Cérémonie des Clés » correspondante.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée de l'AC Racine Almerys est générée dans la plate-forme de l'AC Racine. Elle est sauvegardée comme décrit dans le document [KCR], mais elle n'est pas transmise à un autre propriétaire.
Le propriétaire du bi-clé de l'AC Racine est et reste exclusivement l'Autorité de Gouvernance de l'AC Racine sauf en cas de « transfert d'activité » (cf. § 5.8).

La clé privée d'une AC Fille est générée lors de la Cérémonie des Clés de celle-ci, et les modalités de sa transmission à son propriétaire décrit dans le document correspondant.

6.1.3. Transmission de la clé publique à l'AC Racine

La clé publique d'une AC Fille est transmise à l'AC Racine dans le cadre de la certification de cette AC Fille : génération de son certificat d'AC (en général, sur la plate-forme de l'AC Racine) et signature la clé secrète de l'AC Racine.
Cette transmission suit la procédure décrite dans le document correspondant.

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

La clé publique de l'AC Racine Almerys peut être diffusée dans un certificat qui est un certificat racine autosigné.

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien de la clé publique de l'AC Racine.

La clé publique de l'AC Racine Almerys, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doivent pouvoir être récupérées aisément par les [services] utilisateurs de certificats.

L'IGC Almerys étant privée, la clé publique et le certificat de l'AC Racine Almerys sont transmis au cas par cas aux services Almerys et aux AC Filles Almerys qui le nécessitent.

6.1.5. Taille des clés

Les clés d'AC doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) définies dans les profils de certificats et de LAR (cf. §7 « profils de certificats, OCSP et des LCR »).

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

L'équipement de génération de bi-clés doit utiliser des paramètres respectant les exigences de sécurité propres à l'algorithme correspondant au bi-clé (cf. §7 « profils de certificats, OCSP et des LCR »).
Pour l'AC Racine Almerys, ces paramètres de génération du bi-clé et du certificat d'AC sont vérifiés sous contrôle d'un Huissier et devant témoins au cours de la Cérémonie des Clés.

6.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC Racine et du certificat associé est strictement limitée à la signature de certificats d'AC Fille et de LCR (cf. chapitre 1.4.1 et §7 « profils de certificats, OCSP et des LCR »).

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

Sauf indication particulière, la clé privée mentionnée dans ce paragraphe 6.2 est celle de l'AC Racine Almerys.

6.2.1. Standards et mesures de la sécurité pour les modules cryptographiques

Le module cryptographique (Hardware Security Module : HSM) utilisé par l'AC Racine, pour la génération et la mise en œuvre de ses clés de signature, est un matériel répondant au minimum a une certification FIPS 140 level 3

6.2.2. Contrôle de la clé privée par plusieurs personnes

Toute intervention sur l'AC RACINE nécessite la présence de l'AG, ou du responsable de sécurité des services de confiance.
Deux officiers PKI sont nécessaires pour toutes les opérations sur l'AC racine.

6.2.3. Séquestre de la clé privée

La clé privée de l'AC Racine Almerys n'est jamais exportée en clair en dehors du module cryptographique HSM. Elle est séquestrée sous forme de copies de secours de HSM cryptographique de même niveau de certification.

L'AC Racine Almerys ne séquestre pas les clés privées des AC Filles qu'elle certifie.

6.2.4. Copies de secours de la clé privée

Lors de la Cérémonie des Clés (cf. [KCR]), deux exemplaires de la clé privée de l'AC Racine Almerys sont mis sur des modules HSMs distincts. Chaque HSM cryptographique est Fips 140 level 3.
La clé privée de l'AC racine n'est jamais stockées en dehors du HSM cryptographique.

6.2.5. Archivage de la clé privée

La clé privée de l'AC Racine Almerys est archivée (sous forme chiffrée dans le HSM cryptographique) pendant toute la durée vie de son certificat, ou jusqu'à l'expiration , ou la cessation d'activité de tous les certificats AC FILLES.

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

La clé privée de l'AC Racine Almerys ne peut être activée dans le HSM qu'en réunissant :

- Le HSM cryptographique (de la clé privée) ;
- 1 parmi les 2 Détenteurs de Secrets (AG, ou responsable de sécurité des services de confiance) ;
- le code PIN d'activation et cartes à puce de deux officier PKI;

6.2.7. Stockage de la clé privée dans un module cryptographique

Rappel : en temps normal, la plate-forme de l'AC Racine Almerys est éteinte et démontée. La clé privée de l'AC n'existe que dans les HSM cryptographique.

6.2.8. Méthode d'activation de la clé privée

L'activation de la clé privée est effective dès lors que les détenteurs de secret sont authentifiés sur le HSM cryptographique.

6.2.9. Méthode de désactivation de la clé privée

Sans objet

6.2.10. Méthode de destruction des clés privées

La destruction de la clé privée de l'AC Racine Almerys contenue dans un HSM est documentée dans la DPC. Elle garantit qu'aucune donnée relative à la clé privée ne reste dans le module HSM.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

Le matériels cryptographiques (HSM) de l'AC Racine Almerys ont été évalués FIPS 140 Niveau 3

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1. Archivage des clés publiques

La clé publique de l'AC Racine Almerys est archivée dans le cadre de l'archivage des certificats correspondants pendant la période de validité du certificat.

L'AC Racine Almerys ne conserve aucune clé publique des AC Filles qu'elle certifie.

6.3.2. Durées de vie des bi-clés et des certificats

La durée vie du certificat AC racine est 24 ans

La durée de vie des certificats des AC filles est 10ans .

6.4 DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

Les « données d'activation » du HSM constituent son « monde de sécurité », permettant d'activer la clé privée utilisée.

La génération et l'installation des données d'activation d'un module cryptographique HSM de l'AC Racine Almerys doivent se faire lors de la phase d'initialisation de ce module.

L'Autorité de Gouvernance de l'AC Racine Almerys s'assure de la confidentialité et la disponibilité de ces données d'activation, lesquelles sont confiées en temps normal à des Détenteurs de Secrets de l'AC.

6.4.2. Protection des données d'activation

Les données d'activation qui sont générées par l'AC Racine Almerys pour le module cryptographique de l'IGC doivent être 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.
Les moyens mis en place sont décrits dans la DPC de l'AC Racine Almerys, ainsi que dans [KCR].

6.4.3. Autres aspects liés aux données d'activation

Pas d'exigence spécifique.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

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

- gestion de sessions d'utilisation (accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés
- mises à jour des logiciels ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- éventuellement, gestion des reprises sur erreur.

Les applications utilisant les fonctions des composantes peuvent requérir des moyens de sécurité complémentaires.
La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle fait l'objet de mesures particulières de sécurité

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risques que l'Autorité de Gouvernance doit mener.

6.6.1. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre une fonction de l'IGC Almerys est documentée.
La configuration du système des composantes de l'IGC Almerys ainsi que toute modification et mise à niveau sont documentées.
Tout développement doit être cohérent avec la Politique de Sécurité d'Almerys et avec les exigences contenues dans la présente PC ainsi que dans la PC de l'ACR.

6.6.2. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC Almerys doit être signalée à l'AG pour validation. Elle doit être documentée.

6.7 MESURES DE SECURITE RESEAU

L'AC Racine Almerys étant hors ligne lorsque remise en service, le paragraphe est sans objet.

6.8 HORODATAGE / SYSTEME DE DATATION

Les journaux d'événements sont horodatés au cours des Cérémonies des Clés et de toute intervention sur tout constituant de l'AC Racine Almerys.

7. PROFILS DE CERTIFICATS, OCSP ET DES LCR

Les informations de profil du certificat de l'AC Racine, ainsi que de la LAR qu'elle émet, sont présentés dans ce chapitre. Les informations relatives au certificat de chaque AC Fille sont fournies dans la PC de cette AC. Néanmoins, le gabarit utilisé par l'AC Racine pour produire les certificats d'AC Filles est fourni au 7.2.

Il n'y a pas de mécanisme d'OCSP implémenté pour l'AC Racine Almerys.

7.1 PROFIL DU CERTIFICAT DE L'AC RACINE « ALMERYS ROOT CA »

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		2
signature		
▶ algorithm		Sha2withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= ALMERYS ROOT CA OU=0002 432701639 O=ALMERYS C=FR
validity		
▶ notBefore		Date de création
▶ notAfter		notBefore + 24 ans
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= ALMERYS ROOT CA OU=0002 432701639 O=ALMERYS C=FR
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		 rsaEncryption RSAParams : NULL
▶ subjectPublicKey		DER encoded RSAPublicKey (4096 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶ authorityKeyIdentifier	Non	Hash de la clé publique de l'issuer
▶ subjectKeyIdentifier	Non	Hash de la clé publique du sujet
▶ keyUsage	Oui	keyCertSign (5), cRLSign (6)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies		Stratégie du certificat :

		Identificateur de stratégie = 1.2.250.1.16.12.5.41.1.1.1
▶ basicContraints ➥ cA ➥ pathLenConstraint	Non	 True None
▶ cRLDistributionPoints	Non	[1]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almerysrootca.crl
Private extensions		
▶ authorityInfoAccess		Extension non utilisée
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha2withRSAEncryption, clé de 4096 bits
parameters		NULL

7.2 GABARIT DE CERTIFICAT D'UNE AC FILLE

7.2.1. AC filles

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		2
signature		
▶ algorithm		Sha2withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= ALMERYS ROOT CA OU=0002 432701639 O=ALMERYS C=FR
validity		
▶ notBefore		Date de création
▶ notAfter		notBefore + 10 ans
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= "Non de l'AC Fille" OU="nom de l'organisation unit almerys " OU=0002 432701639 O= ALMERYS C=FR
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		 rsaEncryption) RSAParams : NULL
▶ subjectPublicKey		DER encoded RSAPublicKey (4096 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶ authorityKeyIdentifier	Non	Hash de la clé publique de l'issuer
▶ subjectKeyIdentifier	Non	Hash de la clé publique du sujet
▶ keyUsage	Oui	keyCertSign (5), cRLSign (6)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies		Stratégie du certificat : Identificateur de stratégie = OID AC FILLE
▶ basicContraints ➥ cA ➥ pathLenConstraint	Non	 True None
▶ cRLDistributionPoints	Non	[1]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almerysrootca.crl
Private extensions		
▶ authorityInfoAccess		[1] : accessMethod : id-ad-caIssuers accessLocation : URL=http://pki.almerys.com/almerysrootca.cer
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		

algorithm		Sha2withRSAEncryption, clé de 4096 bits
parameters		NULL

7.3 PROFIL DE LAR DE L'AC RACINE « ALMERYS ROOT CA »

tbsCertList		**Valeur**
version		1 (c'est-à-dire version2)
signature		
▶ algorithm		Sha2withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= ALMERYS ROOT CA OU=0002 432701639 O=ALMERYS C=FR
thisUpdate		Date de création
nextUpdate		thisUpdate + 180 jours
revokedCertificates		
▶ userCertificate		n° de série du certificat révoqué
▶ revocationDate		date de révocation du certificat
▶ crlEntryExtensions		
↪ reasonCode		unspecified (0) *valeur par défaut*
crlExtensions	Critique :	
▶ authorityKeyIdentifier	Non	hash de la clé publique de l'issuer
▶ issuerAltName	-	Extension non utilisée
▶ cRLNumber	Non	Numéro de séquence de la LAR (incrémental simple).
▶ deltaCRLIndicator	-	Extension non utilisée
▶ freshestCRL	-	Extension non utilisée
signatureAlgorithm		
algorithm		Sha2withRSAEncryption
parameters		NULL

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations sont ceux que doit réaliser, ou faire réaliser, l'Autorité de Gouvernance afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

8.1 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'Autorité de Gouvernance doit procéder à un audit de sécurité de cette composante.
L'AG procède également régulièrement à un contrôle de conformité de l'IGC, en tout ou partie. La fréquence de ce contrôle est fournie dans la DPC associée à la présente PC.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

L'Autorité de Gouvernance, en tant que responsable de l'AC Racine Almerys, choisit et assigne 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 doit pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et doit être dûment autorisée à pratiquer les contrôles visés.

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

Les audits de sécurité portent sur tout ou partie de l'IGC et visent à vérifier le respect des engagements et pratiques définies dans la présente PC et dans sa DPC.

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un audit de sécurité, l'équipe d'audit rend à l'Autorité de Gouvernance, 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'Autorité de Gouvernance qui peuvent être la cessation (temporaire ou définitive) d'activité, l'interdiction d'exercer, 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'Autorité de Gouvernance et doit respecter ses politiques de sécurité internes ;
- en cas de résultat "A confirmer", l'AG 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'AG confirme à la composante contrôlée la conformité aux exigences de la PC et de la DPC.

8.6 COMMUNICATION DES RESULTATS

Les résultats des audits de conformité sont communiqués à l'Autorité de Gouvernance de l'AC Racine Almerys.

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

Sans objet.

9.2 RESPONSABILITE FINANCIERE

La garantie financière liée au risque dans la fourniture de service doit être définie dans le contrat de prestation concerné.

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1. Périmètre des informations confidentielles

La classification des informations reprend celle du Groupe France Telecom et d'Almerys comme suit :

- Secret (niveau 1) ;
- Confidentiel(niveau 2) ;
- Interne (niveau 3) ;
- Libre / Public (niveau 4).

Les informations et documents classés secrets sont au moins les suivants :

- les clés privées de l'AC Racine et des composantes comme les AC Filles ;
- le contenu des cartes à puce et des supports des fichiers chiffrés (« Secrets d'AC »)
- tous les secrets de l'IGC, notamment les informations liées à la gestion des modules cryptographiques (HSM) ;

Les informations et documents classés confidentiels sont au moins les suivants :

- la partie non-publique de la DPC de l'AC Racine Almerys ;
- les journaux d'événements des composantes de l'IGC (leur liste est donnée dans le § 5.4) ;
- les documents issus de la Cérémonie des Clés de l'AC Racine :
  - [KCR],
  - liste des Secrets et Détenteurs de Secrets,
  - registres de suivi utilisés,
  - engagements de confidentialité
  - etc.
- les dossiers de certification des AC Filles ([KCF_Cleyris], par exemple)
- les causes de révocations, sauf accord explicite de publication.

Les informations et documents classés publics sont au moins les suivants :

- le certificat de l'AC Racine Almerys ;
- la PC de l'AC Racine Almerys ;
- le document « variables de temps » [VAR_TEMPS];

9.3.2. Informations hors du périmètre des informations confidentielles

Il s'agit de toute information non concernée par le § 9.3.1.

Les informations en diffusion libre (niveau 4) peuvent être diffusées sans restriction autres que les règles du Groupe et d'Almerys en matière de communication externe.

9.3.3. Responsabilités en terme de protection des informations confidentielles

L'AC Racine Almerys est tenue de respecter la législation, la réglementation en vigueur et les dispositions contractuelles. Cette responsabilité incombe à l'Autorité de Gouvernance.

9.4 PROTECTION DES DONNEES PERSONNELLES

Ce paragraphe est sans objet pour les certificats émis par l'AC Racine Almerys.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

Ces droits sont définis dans le contrat de prestation concerné.

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'AC Racine Almerys sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC Racine Almerys et les documents qui en découlent ;
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'Autorité de Gouvernance (cf. chapitre 8) ;
- respecter les accords ou contrats qui les lient entre elles ou aux porteurs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité .

9.6.1. Autorités de Certification

L'AC a pour obligation de fournir le service de PKI au moyen de l'AC Racine Almerys, tel que défini dans le contrat de prestation concerné.

9.6.2. Service d'enregistrement

Almerys a en charge toute l'organisation et la responsabilité en tant qu'Autorité d'Enregistrement de l'AC Racine.

9.6.3. Porteurs de certificats

Sans objet.

9.6.4. Utilisateurs de certificats

Les applications utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;

- contrôler que le certificat signé par l'AC Racine Almerys est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- vérifier la signature numérique de l'AC Racine Almerys émettrice du certificat;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC ;
- contrôler la validité des certificats (dates de validité, statut de révocation).

9.6.5. Autres participants

Sans objet.

9.7 LIMITE DE GARANTIE

La limite de garantie est définie dans le contrat de prestation concerné.

9.8 LIMITE DE RESPONSABILITE

La limite de garantie est définie dans le contrat de prestation concerné.

9.9 INDEMNITES

Cf. § 9.2

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1. Durée de validité

La PC de l'AC Racine Almerys 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

Suite à publication d'une nouvelle version de la PC de l'AC Racine Almerys (voire de la norme), l'Autorité de Gouvernance dispose d'un délai de 1 an pour se mettre en conformité.

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

Pas d'exigence spécifique.

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

Sans objet.

9.12 AMENDEMENTS A LA PC

9.12.1. Procédures d'amendements

Tout projet de modification de la présente PC doit rester conforme aux exigences de la politique de sécurité de l'IGC Almerys, de la PC de l'ACR et respecter les engagements avec les Clients existants du Service. En cas de

changement important, l'AG de l'IGC Almerys pourra faire appel à une expertise technique pour en contrôler l'impact.

La procédure d'amendement devra intégrer l'information et les délais d'information concernant les amendements. Les détails sont fournis dans la DPC associée à la présente PC.

La présente PC devra faire l'objet d'une revue au moins une fois par an, pouvant entraîner ou non un amendement..

9.12.2. Mécanisme et période d'information sur les amendements

cf. 9.12.1.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

Sans objet pour l'AC Racine Almerys.

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Sans objet.

9.14 JURIDICTIONS COMPETENTES

Application du droit en vigueur.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués en Annexe 1.

9.16 DISPOSITIONS DIVERSES

Sans objet.

9.17 AUTRES DISPOSITIONS

Sans objet.