Politique de Certification de l'AC "Almerys Customers Services CA NB", signature cachet

PL
Politique

Référentiel :	Sous-Référentiel :	Référence :	Statut :
Service de Confiance	PKI	PKA013 OID 1.3.6.1.4.1.48620.41.1.5.2.1	validé
Validé par :	**Fonction :**	**Date :**	**Signature :**
KPA	Responsable Sécurité Service Confiance	08/08/2019	
Approuvé par :	**Fonction :**	**Date• :**	**Signature :**
MMI	Autorité de Gouvernance IGC	08/08/2019	
Diffusion auprès de :	ComEx, service juridique		
En accès pour :	Public. Mise à disposition sur site web (http://pki.almerys.com)		
Localisation :	-		

Sommaire

Date de péremption		N/A	Responsable de l'actualisation	Autorité de Gouvernance IGC
Version	**Date**	**Modifications**		**Auteur**
1.9	18/04/2018	Modification pour conformité eIDAS		MMI
2.0	23/07/2018	Modification suite a audit		OLE
2.1	08/08/2019	Modification suite a audit		MMI

• Date d'entrée en vigueur

Sommaire détaillé

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive d'Almerys.

La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par Almerys ou ses ayants droit, sont strictement interdites.

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

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

1. INTRODUCTION

1.1 PRESENTATION GENERALE

Dans le cadre de ses offres de services de dématérialisation et de confiance, Almerys met à disposition de ses Entités clientes (entreprises, administrations, etc.) une Autorité de Certification spécifique, *Customers Services CA*.

Dans ce cadre, **le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification (AC) « Almerys Customer Services CA NB».** Cette AC est habilitée à délivrer des Certificats de signature personne morale qui authentifient ou identifient les entités clientes vis-à-vis d'Almerys et vis-à-vis des différents utilisateurs des services de dématérialisation et de confiance.

L'objectif de la PC est de définir les exigences concernant les certificats de signature
- de personne morale (OID 1.3.6.1.4.1.48620.41.1.5.2.1.1.1) ETSI EN 319411-1 LCP
- cachet d'horodatage (OID 1.3.6.1.4.1.48620.41.1.5.2.1.2.1) ETSI EN 319411-1 LCP

Dans toutes les phases de leur cycle de vie. L'Entité cliente, propriétaire d'un tel certificat, pourra :
- signer numériquement des messages, des documents ou formulaires électroniques, assurant ainsi leur origine, leur intégrité, et leur non-répudiation.
- Générer des contremarques de temps intervenant dans l'horodatage fiable des signatures électroniques, des documents, et des transactions.

La mise en œuvre de ce certificat est assurée par un service automatisé (ensemble de serveurs informatiques) dûment autorisé à utiliser la clé privée de signature cachet.

Cette Politique de Certification est conforme à la norme
- ETSI EN 319411-1
- ETSI EN 319 401

Les certificats produits respectent la norme X.509v3 et leur utilisation est dédiée au mécanisme de signature électronique automatisée (type cachet).

La structure de la présente PC s'appuie sur les références suivantes :
- le RFC 3647 de l'IETF « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework »
- les Politique de Certification Type du Référentiel Général de Sécurité (RGS) émis par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

La section suivante permet d'illustrer l'intérêt de ces Certificats dans le cas du Service de signature électronique proposé par Almerys.

1.1.1. Service de signature électronique Almerys

Almerys propose une solution de signature cachet électronique multicanal qui permet de dématérialiser les échanges de documents et d'informations, et de créer de la valeur probante dans les phases d'engagement, entre les différentes parties concernées, et d'enregistrement d'informations.

Le schéma suivant permet d'illustrer ces principes dans le cas particulier d'un processus de contractualisation multicanal proposée par une entreprise cliente du Service de signature électronique à ses utilisateurs :

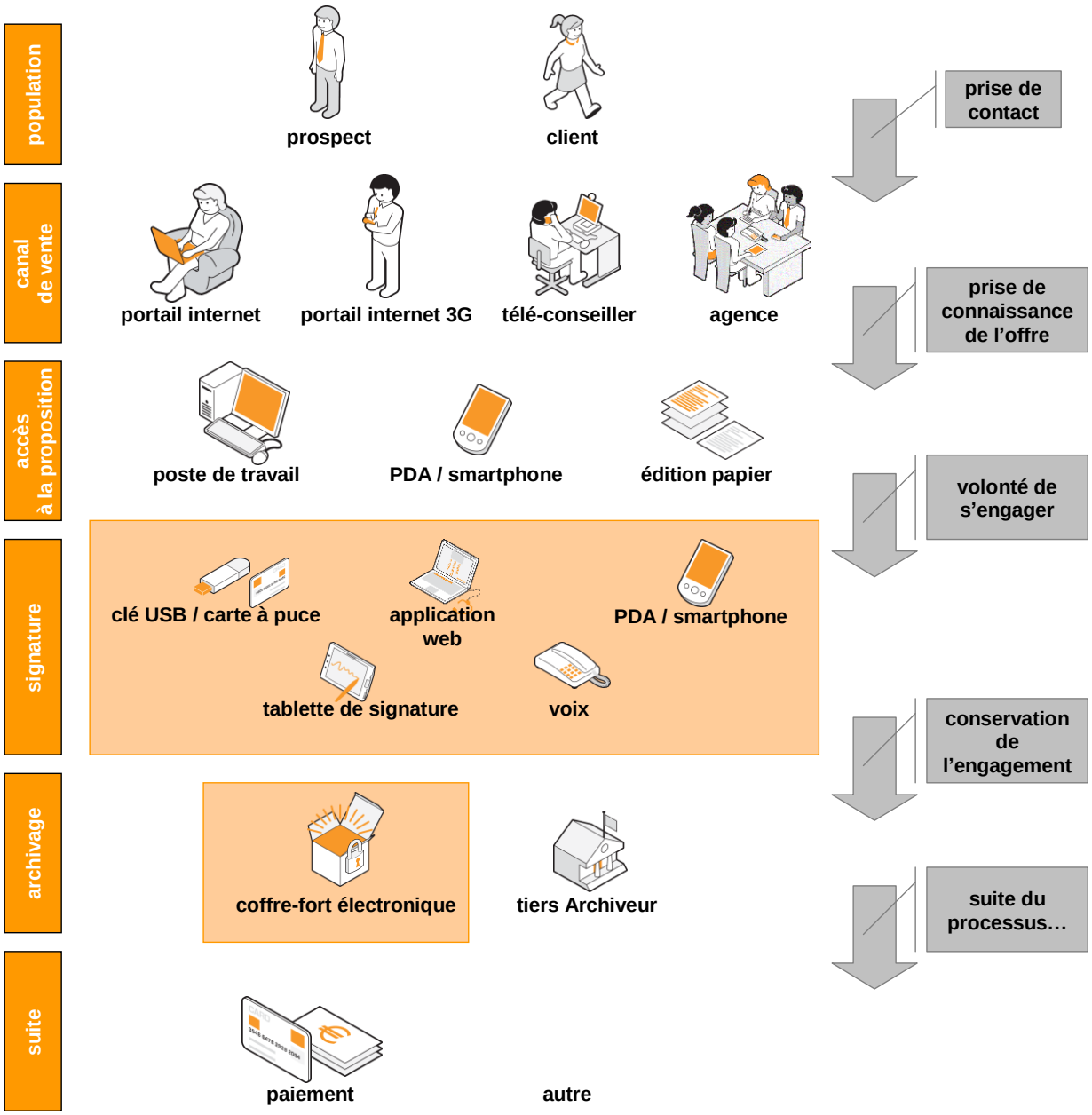
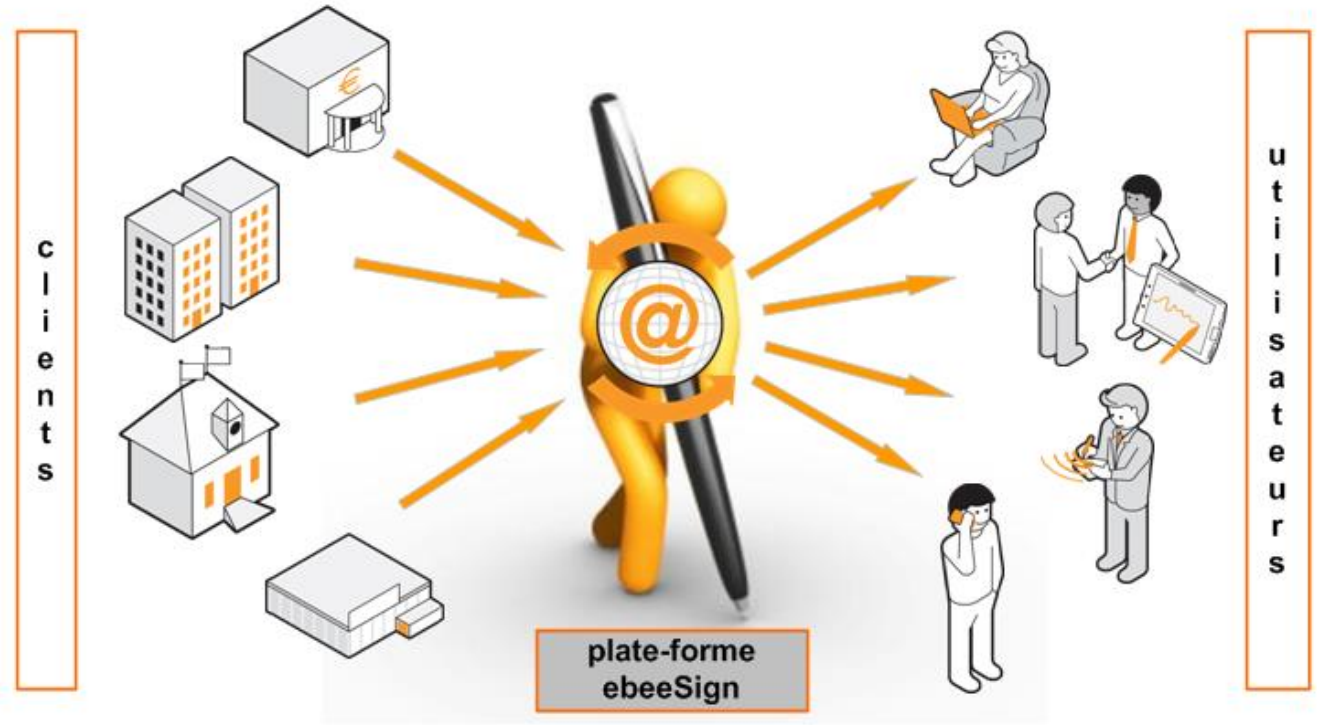


Illustration du principe de contractualisation multicanal

Les services de signature cachet électronique sont appelés par des *Offreurs de Services* (entreprises, institutions, administrations, associations, etc.) afin de mettre à disposition des *Bénéficiaires de Services* (clients, prospects, professionnels, grand public, etc.) les fonctionnalités de signature électronique.

Les *Offreurs de Services* sont les *Clients* de la plate-forme de signature électronique et les *Bénéficiaires de Services* en sont les *Utilisateurs*, tel qu'illustré dans la figure suivante :



Les Clients et les Utilisateurs du Service de signature électronique Almerys

Dans le cadre de ce Service, le Client dispose d'un certificat de signature cachet :

- identifié par l'OID 1.2.250.1.16.12.5.41.1.5.2.1.1 pour les certificats cachet signature
- Identifié par l'OID 1.2.250.1.16.12.5.41.1.5.2.1.2 pour les certificats cachet horodatage
- Identifié par l'OID 1.3.6.1.4.1.48620.41.1.5.2.1.1.1 pour les certificats cachet signature
- Identifié par l'OID 1.3.6.1.4.1.48620.41.1.5.2.1.2.1 pour les certificats cachet horodatage

et objet de la présente PC) qui sera utilisé par les composants du service de signature cachet électronique pour apposer une signature numérique de type cachet de signature ou d'horodatage sur les documents présentés aux Utilisateurs dans le cadre de transactions de contractualisation et de signature.

1.2 IDENTIFICATION DU DOCUMENT

Ce document est la PC de l'AC « **Almerys Customer Services CA NB**» de l'Infrastructure de Gestion de Clés (IGC) d'Almerys pour les certificats de signature de personne morale (cachet).

Son identifiant d'objet (OID) est le suivant : 1.3.6.1.4.1.48620.41.1.5.2.1
Cette référence figure dans les préfixes des OID des Certificats de signature cachet émis par l'AC « **Almerys Customer Services CA NB**» (cf. section 9.12.2).

La référence du document au sein d'Almerys est la suivante : PKA013.

1.3 ENTITES INTERVENANT DANS L'IGC

La décomposition fonctionnelle de l'IGC Almerys qui est retenue dans la présente PC est la suivante :

- **Fonction d'enregistrement** - Cette fonction vérifie les informations d'identification du futur Porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de

l'IGC. Elle a également en charge, lorsque cela est nécessaire, la revérification des informations du Client lors du renouvellement du Certificat de celui-ci.

- **Fonction de génération des certificats** – Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les Certificats à partir des informations transmises par l'Autorité d'Enregistrement et de la clé publique du Client provenant de la fonction de génération des éléments secrets du Client chargée en particulier de générer la bi-clé du Client.

- **Fonction de génération et de stockage des éléments secrets du Client** – Cette fonction génère les éléments secrets du Client et les prépare en vue du stockage sécurisé au niveau des Modules cryptographiques matériels du Service de stockage sécurisé de Bi-clé d'Almerys et de la mise à disposition de la fonction d'activation pour les systèmes dûment reconnus par le Client. Il s'agit en particulier de la bi-clé du Client et des informations d'activation de la clé privée du Client. Cette fonction est déléguée au Service de stockage sécurisé de Bi-clé de l'IGC Almerys (cf. §1.3.4 « Service de stockage sécurisé des Bi-clés des Client »).

- **Fonction de remise au Client** – Cette fonction remet au Client son certificat ainsi que les moyens de contrôle de sa clé privée et de son certificat.

- **Fonction de publication** – Cette fonction met à disposition des différentes parties concernées, les politiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux Clients/porteurs et/ou aux Applications utilisatrices de certificats, hors informations d'état des certificats. La liste complète des Certificats valides des Clients n'est pas fournie publiquement.
  La transmission aux Clients des conditions générales de fourniture et d'utilisation des Certificats Customers Services est à la charge d'Almerys.

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

- **Fonction d'information sur l'état des certificats** – Cette fonction fournit aux Applications utilisatrices de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR) et éventuellement selon un mode requête / réponse temps réel (OCSP).

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 tels que AC, AG, AE, SP, AH, AA, Service support …).

1.3.1. Autorité de certification (AC)

L'***Autorité de Certification (AC)*** « **Almerys Customer Services CA NB**» a en charge la fourniture des prestations de gestion des Certificats de signature cachet des Clients tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation) et est, à ce titre, identifiée dans ces Certificats en tant qu'émetteur.

L'AC « **Almerys Customer Services CA NB**» appartient à la hiérarchie de confiance d'Almerys (ensemble des AC d'Almerys regroupées au sein de son IGC). A ce titre, la gestion de l'AC « **Almerys Customer Services CA NB**» ainsi que de l'AC Racine est assurée par Almerys.

Les prestations de l'AC « **Almerys Customer Services CA NB**» sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

1.3.2. Autorité de Gouvernance (AG)

L'Autorité de Gouvernance (***AG***) est l'autorité responsable de l'ensemble des services de l'IGC Almerys, elle a un pouvoir décisionnaire au sein de l'IGC. Elle définit et fait appliquer les PC et DPC.
Concrètement, il s'agit d'un ou plusieurs représentants d'Almerys ayant un mandat spécifique pour assurer cette fonction.

1.3.3. Autorité d'Enregistrement (AE)

L'***Autorité d'enregistrement (AE)*** est un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC et les Clients, Porteurs de certificats *Customers Services*. Dans le cas du Service de signature électronique, c'est Almerys qui est chargé de la relation avec les Clients, et de leur identification et authentification.

A ce titre, l'AE assure :

- la prise en compte et la vérification des informations, notamment d'informations personnelles, présentées par le Représentant Client, et la constitution de son dossier d'enregistrement ;
- l'établissement et la transmission de la demande de Certificat à la fonction adéquate de l'AC « **Almerys Customer Services CA NB**» ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et protection en confidentialité et en intégrité des données personnelles du Client qui lui sont confiées, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

C'est l'AE qui détermine le niveau d'assurance attendu dans le processus d'identification de ses Clients. Elle établit en conséquence les procédures nécessaires pour assurer ce niveau d'assurance et s'assure de leur mise en œuvre opérationnelle.

L'AE s'engage également au maintien opérationnel des moyens qui sont mis à sa disposition pour transmettre les demandes de Certificats Customers Services, et au respect des règles communes d'authentification et de contrôle des flux établies entre l'AE et l'AC « **Almerys Customer Services CA NB**».

1.3.4. Service de stockage sécurisé des Bi-clés des Clients

L'AC « **Almerys Customer Services CA NB**» met en œuvre un service de stockage sécurisé des Bi-clés des Clients.
Ce service est hébergé dans les locaux d'Almerys à accès très restreint et met en œuvre des modules cryptographiques matériels répondant aux exigences du standard FIPS 140-2 level 3 ou EAL4+ critères communs. Chaque Client bénéficie d'un container cryptographique qui est totalement dédiée au stockage de sa ou de ses Bi-clé(s)

Seule l'application de signature électronique, ou d'horodatage peut communiquer avec le Module cryptographique matériel pour une demande de signature cachet. A aucun moment la clé privée de signature du Client ne peut être exportée du Module.

La création du Bi-clé Client a lieu lors d'une Cérémonie de Clés de signature, et après validation de la demande du Représentant Client.
L'activation du Bi-clé de signature d'un Client par l'application de signature n'est possible qu'après enregistrement sécurisé de l'application au niveau du Module cryptographique.

.

1.3.5. Client et Représentant Client (RC)

Le Client est l'entité cliente ayant décidé de souscrire au Service Almerys, qu'il utilise pour ses propres besoins ou qu'il met à disposition des Utilisateurs. Le Client, Porteur du Certificat, est représenté par une personne physique mandatée à le représenter : le Représentant Client (RC).

Le RC est une personne physique qui est responsable de l'utilisation du Certificat de signature de personne morale (Certificat de type cachet) pour le service identifié dans le Certificat et de la clé privée correspondant à ce Certificat, pour le compte de l'entité également identifiée dans ce Certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RC respecte les conditions qui lui incombent définies dans la présente PC.

Il est à noter que le certificat étant attaché à un service et non au RC, ce dernier peut être amené à changer en cours de validité du Certificat : départ du RC de l'entité cliente, changement d'affectation et de responsabilités au sein de l'entité, etc.
Le Client doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur. L'AC peut être amenée à révoquer un certificat de signature de personne morale pour lequel il n'y a plus de RC explicitement identifié.
Dans le cas de certificats d'horodatage almerys, le RC est une personne d'Almerys.

1.3.6. Applications utilisatrices des certificats

La présente PC traitant de Certificats de signature cachet, une application utilisatrice de certificat est un processus qui met en place la vérification d'une signature cachet. C'est donc une application informatique qui utilise un dispositif de vérification de signature afin d'assurer l'Intégrité et la Non-répudiation du document ou du message signé.

Les applications peuvent être notamment :

- le service de vérification de signature cachet Almerys qui permet à partir d'une information ou d'un document signé à l'aide d'un certificat Customers Services, de vérifier et d'afficher un statut sur l'état du certificat utilisé et de la signature ;
- l'application Acrobat Reader™ d'Adobe™ qui permet d'afficher un document au format PDF signé par un certificat Customers Services ainsi que le cartouche d'information sur les signatures associées au document. Cette application doit être correctement configurée pour accepter les certificats Customers Services.
- Le service d'horodatage d'Almerys qui met en œuvre des certificats cachets sur les unités d'horodatage.

1.3.7. Autres participants

Sans objet.

1.4 USAGE DES CERTIFICATS

1.4.1. Domaines d'utilisation applicable

1.4.1.1. Bi-clés et Certificats des Clients

Le seul domaine d'utilisation applicable de la présente PC pour les Bi-clés et les Certificats Customers Services des Clients est le Service Almerys, qui propose des fonctionnalités de signature cachet établies au sein des processus automatisés du Service.
Les certificats sont émis pour un usage de cachet (signature de personne morale) pour :

- Les services de signature cachet ;
- Le service d'horodatage.

1.4.1.2. Bi-clés et Certificats d'AC et de composantes

Les Bi-clés et Certificats de l'AC « **Almerys Customer Services CA NB**» ne peuvent être utilisés que pour la signature de Certificats Customers Services et de LCR.

1.4.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par ses Clients et les Applications utilisatrices de certificats.

A cette fin, elle communique à tous les Clients et Applications utilisatrices de certificats potentiels les termes et conditions relatives à l'utilisation du Certificat.

1.5 GESTION DE LA PC

1.5.1. Entité gérant la PC

L'entité en charge de l'administration et de la gestion de la politique de certification est l'AG. L'AG est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.
A cette fin, elle met en œuvre et coordonne une organisation dédiée, qui statue à échéance régulière, sur la nécessité d'apporter des modifications à la PC.

1.5.2. Point de contact

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

Gouvernance IGC be-ys
Email : gouvernance.igc@be-ys.com
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

Afin de déterminer la conformité de la DPC avec la présente PC, l'AG s'appuie sur les ressources d'Almerys spécialisées dans l'audit et l'évaluation de la sécurité des services et des produits.
Un document interne précise, au sein de l'organisation Almerys, l'entité qui assure cette responsabilité.

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

L'approbation de conformité de la DPC par rapport à cette PC fait l'objet d'une procédure interne.

L'AG est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place.

1.6 ACRONYMES ET DEFINITIONS

1.6.1. Acronymes

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

AC	Autorité de Certification [Certification Authority (CA)]
AE	Autorité d'Enregistrement [Registration Authority (RA)]
AH	Autorité d'Horodatage [Time-stamping Authority (TA)]
AG	Autorité de Gouvernance [Governance Authority (GA)]
ANSSI	Agence nationale de la sécurité des systèmes d'information
CC	Critères Communs [Common Criteria (CC)]
CEN	Comité Européen de Normalisation
CSP	Cryptographic Service Provider
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
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
RC	Représentant Client

RSA	Rivest Shamir Adelman
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

1.6.2. Définitions

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

Applications utilisatrices :
Services applicatifs exploitant les Certificats émis par l'AC « **Almerys Customer Services CA NB**», par exemple, pour des besoins d'authentification ou de vérification de signature du Client du certificat.

Authentification [Authentication] :
Action de s'assurer de l'identité d'une personne physique ou morale ou de l'origine d'une communication.

Autorité de Certification (AC) [Certificate Authority (CA)] :
Entité qui délivre et est responsable des Certificats électroniques émis et signés en son nom conformément aux règles définies dans la PC et dans la DPC associée.
Dans le cadre de la présente PC, il s'agit de l'AC « **Almerys Customer Services CA NB**» d'Almerys.

Remarque :
L'AC peut assurer elle-même l'exploitation ou la faire gérer par un Opérateur de Services de Certification (OSC ou OC) disposant de locaux sécurisés, du personnel et de l'infrastructure technique qui lui permettront de réaliser l'ensemble des tâches de gestion des certificats pour le compte de l'AC.

Autorité de Certification Racine (ACR) :
Entité qui dispose d'une IGC lui permettant d'enregistrer, de générer, d'émettre et de révoquer des Certificats d'AC (dont l'AC « **Almerys Customer Services CA NB**»), conformément à la PC et à la DPC définies par son AG.
L'ACR d'Almerys est auto-certifiée, c'est-à-dire que son certificat est auto-signé.
L'ACR d'Almerys est l'AC « Almerys Root CA ».

Autorité d'Enregistrement (AE) [Registration Authority (RA)] :
Entité disposant d'un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC et les Porteurs de certificats conformément au paragraphe 1.3.3 de la présente PC.
L'AE a pour rôle de vérifier l'identité du futur Porteur de certificat.

Autorité de Gouvernance (AG) [Governance Authority (GA)] :
Entité responsable de l'ensemble des fonctions de l'IGC Almerys avec pouvoir décisionnaire.

Bi-clé [Key Pair] :
Couple clé publique / clé privée.

Cérémonie des Clés ou **Key Ceremony (KC)** :
Réunion spéciale des personnes autorisées pour générer le Certificat d'une AC ou d'un Client (KC Client). 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'une 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 AC. 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.
Dans le cadre de la présente PC, le Certificat désigne un Certificat électronique de signature de personne morale (signature cachet), pour lequel la protection matérielle de la Bi-clé de signature est assurée par le service de stockage sécurisé de Bi-clé de l'AC.

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

Client :
Entité cliente ayant décidé de souscrire au Service Almerys, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des Utilisateurs. Les Certificats émis par l'AC « **Almerys Customer Services CA NB**» conformément aux exigences de la présente PC sont produits pour le Client.

Voir également Porteur de certificat.

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)] :
Document qui 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 PC qu'elle s'est engagée à respecter.

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.

Infrastructure de Gestion de Clés (IGC) [Public Key Infrastructure (PKI)] :
Ensemble de composants, 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 AC, d'un OC, d'une AE centralisée et/ou locale, de MC, d'une entité d'archivage, d'une entité de publication.

Intégrité [Integrity] :
Propriété d'exactitude, de complétude et d'inaltérabilité dans le temps des *informations* et des *fonctions* de l'information traitée.

Liste des certificats d'AC Révoqués (LAR) :
Liste de certificats d'AC ayant fait l'objet d'une révocation avant la fin de leur période de validité.

Liste de Révocations de Certifcats (LRC) [Certificate Revocation List (CRL)] :
Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.

Mandataire de Certification (MC) :
Personne physique désignée par et placée sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des Porteurs de cette entité.
Dans le cadre de la présente PC, ce rôle n'est pas mis en œuvre.

Module cryptographique matériel : Matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques.

Online Certificate Status Protocol (OSCP) :
Protocole permettant à une personne de vérifier en temps réel la validité d'un certificat, en particulier s'il a été révoqué.
Dans le cadre de la présente PC, ce protocole n'est pas implémenté.

Non-répudiation [Non-repudiation] :
Impossibilité pour un Porteur, un Utilisateur ou une Application utilisatrice 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*).

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 Applications utilisatrices de certificats.

Porteur de certificat [Subscriber] :
Client qui doit respecter les conditions qui lui incombent définies dans la présente PC.
L'identification et l'authentification du Client sont à la charge d'Almerys (rôle d'AE).

Produit de sécurité :
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.

Promoteur d'application :
Fournisseur d'une offre de service sécurisé (échanges dématérialisés).

Représentant Client :
Personne physique qui a un lien contractuel / hiérarchique / réglementaire avec l'entité cliente, Porteur de certificat, et qui est responsable de l'utilisation du certificat de signature de personne morale (Certificat de type cachet) pour le service identifié dans le Certificat et de la clé privée correspondant à ce Certificat, pour le compte de l'entité cliente également identifiée dans ce Certificat.

Responsable d'Autorité d'Enregistrement (RAE) :

Personne physique en charge de l'AE.

Service Almerys :
Un des services de la gamme d'offres de services de dématérialisation et de confiance d'Almerys, déployé en tout ou partie.

Signature électronique ou Signature :
« *Usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* », conformément au Code civil.

Uniform Resource Locator (URL) :
Adresse d'un site internet.

Utilisateur :
Personne physique, utilisatrice d'un service mis à disposition par un Client

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

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Pour la mise à disposition des informations devant être publiées à destination des Clients et des Applications utilisatrices de certificats, l'AC « **Almerys Customer Services CA NB**» met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats.

La mise à disposition des informations sur l'état des certificats se base sur un mécanisme de LCR (Liste de Certificats Révoqués) accessible via un lien HTTP. Les adresses de publication sont fournies dans la section 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ».

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

L'AC « **Almerys Customer Services CA NB**» diffuse les informations suivantes :

- la présente PC, qui contient en particulier les profils de certificat et de LCR, les délais et fréquences de publication, le glossaire qui contient les acronymes et les définitions applicables, les adresses principales de diffusion) ;
- les certificats en cours de validité des AC de la hiérarchie de rattachement de l'AC Customers Services, les différentes PC correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'ACR ;
- la liste des certificats de signature des Clients et des AC révoqués ;
- les conditions générales d'utilisation des Certificats.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Pour la PC, la publication est effective dès que nécessaire afin d'assurer, à tout moment, la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. La PC valide est publiée avant la première émission d'un certificat final.

Pour les certificats d'AC, ils sont publiés préalablement à toute émission de certificats et/ou de LCR correspondants sous délai de 72 heures.

Pour les informations d'état des certificats, les Listes de Certificats Révoqués sont mises à jour dans un délai maximum de 24 heures. Une fois la mise à jour effectuée, la LCR est publiée dans un délai maximum de 60 minutes.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées est du niveau de confidentialité « diffusion libre » pour les Applications utilisatrices de certificats.

La fonction de publication et la fonction d'information sur l'état des certificats assurent à tout moment l'intégrité des informations qu'elles publient.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'AC « **Almerys Customer Services CA NB**», et aux personnes dûment autorisées après authentification par login /mot de passe.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1. Type de noms

Les noms utilisés dans les Certificats émis par l'AC « **Almerys Customer Services CA NB**» sont conformes aux spécifications de la norme X.500.
Dans chaque Certificat X.509v3, l'AC émettrice (issuer) et le Client (subject) sont identifiés par un « Distinguish Name » DN dont le format est précisé dans la section 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ».

3.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les Clients, Porteurs de certificat, sont explicites :

- l'attribut CN du champ du subject DN du Client identifie le service du Client pour lequel le certificat va être utilisé;
- l'attribut O du champ subject DN contient la raison sociale du Client ;
- le premier attribut OU contient le numéro d'enregistrement SIREN/SIRET en France (ou en dehors de la France, de son équivalent reconnu par les autorités compétentes du pays du client) assurant l'unicité de la référence Client.

Le format exact du subject DN des Certificats de signature est précisé dans la section 7 décrivant le profil des certificats et des LCR.

3.1.3. Anonymisation ou pseudonymisation des Clients

Les certificats des Clients ne peuvent pas être anonymes. L'utilisation d'un pseudonyme est interdite.

3.1.4. Règles d'interprétation des différentes formes de nom

Les règles d'interprétation des différentes formes de nom sont explicitées dans la section 7 décrivant le profil des Certificats et des LCR.

3.1.5. Unicité des noms

Afin d'assurer la continuité d'une identification unique du Client au sein du domaine de l'AC « **Almerys Customer Services CA NB**» et pour éviter toute ambiguïté, le DN du champ « subject » de chaque Certificat de Client permet d'identifier de façon unique le Client correspondant au sein du domaine de l'AC grâce à la référence unique inscrite dans les attributs CN et « OU = <ICD> <SIREN> [1]» du champ subject DN.
Durant toute la durée de vie de l'AC, un DN attribué à un client ne peut être attribué à un autre client. Des précisions sont fournies, dans la DPC associée à cette PC, répondant à cette exigence en respectant les spécifications sur le DN définies dans les profils de Certificats (cf. section 7).

A noter que l'unicité d'un Certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au Certificat et non pas au Client et ne permet donc pas d'assurer une continuité de l'identification dans les Certificats successifs d'un Client donné.

[1] Ou équivalent en dehors de la France

3.1.6. Identification, authentification et rôle des marques déposées

Les informations d'identification du Client et du RC sont présentées par le RC lors de son enregistrement auprès de l'AE (i.e. Almerys).
En cas de litige sur l'interprétation de ces paramètres, une résolution amiable des conflits est privilégiée.

3.2 VALIDATION INITIALE DE L'IDENTITE

L'enregistrement d'un Client se fait directement auprès de l'AE, i.e. Almerys.
Les modalités pratiques de validation de l'identité du Client sont déterminées par Almerys et se base sur la validation de l'identité du RC, habilité à représenter le Client.

3.2.1. Méthode pour prouver la possession de la clé privée

La clé privée du Client est générée lors d'une Cérémonie des Clés Client (KC Client) à laquelle assiste le RC, toute personne dûment mandatée par le Client, ou éventuellement huissier. Le script de déroulement de la KC Client permet de s'assurer que la clé privée est créée dans un environnement maîtrisé. La requête de certificat générée par le module cryptographique est signée par la clé privée qui est stockée de manière sécurisée dans le Module cryptographique, prouvant ainsi la possession de la clé privée.

3.2.2. Validation de l'identité d'un organisme

Cf. chapitre 3.2.3.

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un Client

L'AE demande une preuve de l'habilitation du RC à demander un certificat pour l'entité morale qu'il représente, sauf si le RC est le représentant légal de l'entité cliente.

L'enregistrement du RC, personne physique représentant le Client, nécessite l'identification de cette entité cliente et, l'identification de la personne physique et la preuve du rattachement de la personne physique à l'entité. Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- tout document attestant de la qualité du signataire de la demande de certificat,
- un document officiel d'identité en cours de validité du représentant de l'entité cliente comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le RC,
- les conditions générales d'utilisation des certificats Customers Services signées.

Les modalités complètes de validation de l'identité du RC et de l'entité cliente sont fournies dans la DPC.

3.2.4. Informations non vérifiées du Client

Sans objet dans le cadre de la présente PC.

3.2.5. Validation de l'autorité du demandeur

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

3.2.6. Critères d'interopérabilité

Les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient est de la responsabilité de l'AG de l'ACR « AMERYS ROOT CA ».

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

Le renouvellement du Bi-clé de signature d'un Client entraîne automatiquement la génération et la fourniture d'un nouveau Certificat de signature et d'une nouvelle bi-clé. L'ancien certificat est révoqué.

La vérification de l'identité dans le cadre d'un renouvellement de clés est la même que lors de l'enregistrement initial. Un nouveau Certificat ne peut pas être fourni au Client sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

3.3.1. Identification et validation pour un renouvellement courant

Lors des renouvellements, l'AE doit identifier le Client selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

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

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

3.4.1. Demande faite via les moyens informatiques

3.4.1.1. Par le Client du Service

Le demandeur est le RC qui a effectué la demande initiale de Certificat, il doit valider la révocation en utilisant le formulaire mis à sa disposition, et en contactant l'AE d'Almerys. L'AE doit vérifier l'identité du RC habilité à demander une révocation de Certificat en s'appuyant sur la procédure en vigueur.

Pour une révocation d'urgence

Utiliser le service d'enregistrement des demandes de révocation disponible en ligne 24H/24 7j/7, à l'adresse http://pki.almerys.com/revoquer.html, l'authentification des demandes de révocation s'effectue via un code OTP.

3.4.1.2. Par le responsable du Service

Si un Client ne souhaite plus faire appel au Service proposé par Almerys et met fin à la relation contractuelle établie entre lui et Almerys, le responsable du Service est habilité à demander la révocation des Certificats

Customers Services émis au nom de ce Client ou s'assurer qu'aucune requête de signature ne sera plus acceptée par le Service pour l'un quelconque de ces Certificats.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1. Origine d'une demande de certificat

Un certificat ne peut être demandé que par un RC dûment mandaté, ou le représentant légal de l'entité cliente.

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

Le RC établit le dossier de demande de Certificat à partir du formulaire mis à sa disposition par l'AE. Il joint également les pièces justificatives demandées (cf. chapitre 3.2.3.1).
Des précisions sont fournies dans la DPC associée à la présente PC.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

L'AE doit valider l'identité du RC et du Client en s'assurant de la cohérence des justificatifs présentés, ainsi que de la cohérence de la demande de Certificat papier signée par le RC.

4.2.2. Acceptation ou rejet de la demande

A réception de la demande papier de Certificat, l'AE vérifie que les éléments fournis sont complets et intègres, et en cas de succès transmet la demande de Certificat proprement dite à l'AG qui valide la planification d'une Cérémonie des Clés Client (KC Client) pour générer le Bi-clé et du Certificat du Client.
C'est le service de stockage sécurisé de Bi-clés qui est chargé de la mise en œuvre de la KC Client.

4.2.3. Durée d'établissement du certificat

La durée d'établissement des Certificats est déterminée avec le RC, elle correspond au temps de mise en œuvre de la KC Client avant la mise à disposition du Certificat auprès du Client.

4.3 DELIVRANCE DU CERTIFICAT

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

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche le processus de génération du Bi-Clé et du Certificat du Client lors de la KC Client. Le RC, un autre représentant dûment mandaté par le Client, ou un huissier assiste à la KC Client et s'assure du bon déroulement de la KC Client.

La durée du Certificat est de 3 ans. Le chapitre 7.1.1 détaille le format utilisé par l'AC pour les certificats Customers Services.

A l'issue de la KC Client, le Bi-Clé et le Certificat Client sont stockés dans le ou les Modules cryptographiques matériels du service de stockage sécurisé des Bi-clés et l'AC remet au Client son Certificat.
La section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques » précise les caractéristiques des modules utilisés pour générer et stocker la Bi-clé de signature du Client.

4.3.2. Notification par l'AC de la délivrance du certificat

L'AC « **Almerys Customer Services CA NB**» renvoie à l'AE et au Client du Service un statut sur l'opération de génération du Bi-clé et du Certificat Client. La DPC associée à la présente PC précise les différentes informations qui sont mises à disposition.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1. Démarche d'acceptation du certificat

L'acceptation du Client a lieu :

- lors de la KC Client (en cas de présence du RC ou du représentant légal):
  - une fois le Certificat créé, le profil et les propriétés du Certificat sont validés par le RC, son représentant en séance. Cette validation est enregistrée dans le script de déroulement de la KC Client ;
  - le Certificat et la signature du script de la KC per le RC à l'issue de la KC ce qui vaut acceptation finale du certificat et valide le bon déroulement de la KC Client.
- suite à la notification du RC par email de la génération du certificat avec une description du champs « subject » , la date d'emission et date de fin (en cas d'absence du RC ou du représentant légal le jour de la KC).
  - une fois le Certificat créé, un email de notification est envoyé au RC,.
  - La non contestation du client dans les deux semaines, ainsi que la première utilisation du certificat vaut acceptation finale du certificat et valide le bon déroulement de la KC Client.

4.4.2. Publication du certificat

Les certificats *Customers Services* ne sont pas publiés de manière centralisée et publique.

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

L'AC « **Almerys Customer Services CA NB**» informe l'AE de la délivrance du certificat. Cf. section 4.3.2 « Notification par l'AC de la délivrance du certificat ».

4.5 USAGES DE LA BI-CLE ET DU CERTIFICAT

4.5.1. Utilisation de la clé privée et du certificat par le Client

L'utilisation de la clé privée du Client et du Certificat associé est strictement limitée au Service Almerys (cf. section 1.4 « Usage des certificats »).

L'usage autorisé de la Bi-clé du Client et du Certificat associé est précisé dans le Certificat lui-même, via les extensions concernant les usages des clés (cf. section 7.2 pour le détail du profil du Certificat Customers Services).

Les Clients doivent respecter strictement les usages autorisés des Bi-clés et des Certificats. Dans le cas contraire, leur responsabilité serait engagée.

D'une manière générale, tout usage non autorisé explicitement est interdit.

4.5.2. Utilisation de la clé publique et du certificat par les Applications utilisatrices du certificat

Cf. chapitre précédent et sections 1.4 « Usage des certificats » et 1.3.6 « Applications utilisatrices des certificats »
Les Applications utilisatrices de certificats doivent respecter strictement les usages autorisés des Certificats. Dans le cas contraire, leur responsabilité peut être engagée.

4.5.3. Utilisation de la clé privée et du certificat de l'AC racine

La clé privée de l'AC Racine est utilisée :

- Pour signer les certificats des AC intermédiaires
- Pour signer les CARLs

Le certificat de l'AC Racine est utilisé

- Pour vérifier les certificats des AC intermédiaires
- Pour vérifier l'intégrité et l'origine d'une CARL

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

La clé privée de l'AC est utilisée :

- Pour signer les certificats des porteurs
- Pour signer les certificats des répondeurs OCSP
- Pour signer les CRLs

Le certificat de l'AC est utilisé

- Pour vérifier les certificats émis et les signatures générés par les clés privées des porteurs
- Pour vérifier l'intégrité et l'origine d'une CRL
- Pour vérifier l'intégrité et l'origine d'un certificat d'OCSP

4.5.5. Utilisation de la clé privée et du certificat de l'OCSP

La clé privée d'un répondeur OCSP est utilisée pour signer les réponses OCSP, tout autre usage est interdit.
Le certificat d'un répondeur OCSP est utilisée par les utilisateurs pour vérifier l'origine et l'intégrité d'une réponse OCSP.

4.6 RENOUVELLEMENT D'UN CERTIFICAT

Le renouvellement d'un Certificat – i.e. la délivrance d'un nouveau Certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations restant identiques au Certificat précédent (y compris la clé publique du porteur) , cf. [RFC3647] – n'est pas autorisé dans le cadre de la présente PC.

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

Tout changement de Bi-clé doit faire l'objet au préalable d'une révocation du Certificat existant (cf. 4.9 « Révocation et suspension des certificats »), si celui-ci n'a pas encore expiré et n'a pas déjà été révoqué avant la demande de nouveau Certificat.

4.7.1. Causes possibles de changement d'une bi-clé

Les Bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Par ailleurs, une Bi-clé et un Certificat peuvent être renouvelés par anticipation, suite à la révocation du Certificat du Client (cf. section 4.9.1 « Causes possibles d'une révocation »).

Les causes possibles de changement d'une Bi-clé et de Certificat sont donc les suivantes :

- Certificat valide, arrivant prochainement à expiration,
- Certificat expiré,
- Certificat révoqué.

Remarque : à échéance de l'expiration d'un Certificat encore valide d'un Client, l'AC peut fournir un statut à l'AE, qui peut alors choisir de prévenir le RC

- pour préparer l'établissement d'une demande de délivrance d'un nouveau Certificat pour le Client concerné,
- ou ne rien faire.

4.7.2. Origine d'une demande d'un nouveau certificat

Cf section 4.1.1 « Origine d'une demande de certificat ».

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

Cf chapitre 4.2 « Traitement d'une demande de certificat ».

L'identification et la validation d'une demande de fourniture d'un nouveau Certificat sont précisées au 3.3 « Identification et validation d'une demande de renouvellement des clés ».

Pour les actions de l'AC, cf. 4.3 « Délivrance du certificat ».

4.7.4. Notification de l'établissement du nouveau certificat

Cf. section 4.3.2 « Notification par l'AC de la délivrance du certificat ».

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. section 4.4.1 « Démarche d'acceptation du certificat ».

4.7.6. Publication du nouveau certificat

Cf. section 4.4.2 « Publication du certificat ».

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

Cf. section 4.4.3 « Notification par l'AC aux autres entités de la délivrance du certificat ».

4.8 MODIFICATION DU CERTIFICAT

La modification d'un Certificat – i.e. des modifications d'informations du Certificat sans changement de la clé publique, et autres qu'uniquement la modification des dates de validité, cf. [RFC3647] – n'est pas autorisée dans le cadre de la présente PC.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

L'AC « **Almerys Customer Services CA NB**» ne met pas en œuvre de processus de suspension de ses Certificats.

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats de Client

Les circonstances suivantes peuvent être à l'origine de la révocation du Certificat de signature du Client :

- le Certificat est devenu obsolète suite à un changement des données du Client figurant dans le Certificat,
- les informations du Client figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le Certificat,
- les modalités applicables d'utilisation du Certificat n'ont pas été respectées par le Client,
- le Client, l'AE ou l'AC n'ont pas respecté leurs obligations découlant de la PC de l'AC « **Almerys Customer Services CA NB**»,
- une erreur (intentionnelle ou non) a été détectée dans le dossier de demande de Certificat,
- la clé privée du Client est suspectée de compromission, est compromise, est perdue ou est volée,
- le Client ou une entité autorisée demande la révocation du Certificat (notamment dans le cas d'une destruction ou altération de la clé privée du Client),
- le Certificat de signature de l'AC « **Almerys Customer Services CA NB**» est révoqué (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante),
- événements (décès du représentant légal de l'entité cliente, cessation d'activité du Client, etc.) initialisés par le processus de gestion des identités et des droits d'accès,
- fin de relation contractuelle / hiérarchique / réglementaire entre l'AC « **Almerys Customer Services CA NB**» et le Client du Service – et donc avec ses Utilisateurs – avant la fin de validité des certificats.
- Le remplacement d'un RC n'a pas été mis en œuvre par le Client

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC « **Almerys Customer Services CA NB**» ou l'AE en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau Certificat notamment), le Certificat concerné doit être révoqué.

4.9.1.2. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat de l'AC « **Almerys Customer Services CA NB**» pour la génération de Certificats et de LCR) :

- suspiscion de compromission, compromission, perte ou vol de la clé privée de la composante ;

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

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats cachet

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

- L'AC « **Almerys Customer Services CA NB**», émettrice du Certificat ou l'une de ses composantes (AE),
- Le RC ou toute autre personne dûment habilitée par le client. En cas de changement du RC le client s'engage à en informer almerys et fournir le pouvoir associé.
- Le Client via son représentant légal.

4.9.2.2. Certificat d'une composante de l'IGC

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

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat cachet

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre 3.4 « Identification et validation d'une demande de révocation ».

Les informations suivantes doivent au moins figurer dans la demande de révocation de Certificat :

- l'identité du Client utilisée dans le Certificat (Raison sociale, SIREN[2], etc.) ;
- l'identification de l'entité qui demande la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le Certificat à révoquer (n° de série, ...) ;
- la cause de révocation. Cette cause de révocation n'est pas inscrite dans la LCR mais peut être enregistrée dans la base de données du Service.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations de l'AC « **Almerys Customer Services CA NB**» révoque le Certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée au minimum via le mécanisme de Liste de Certificats Révoqués (LCR) mis en œuvre par l'AC « **Almerys Customer Services CA NB**». D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC (cf. chapitre 4.9.9 « Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats »).

Le processus de révocation d'un Certificat de signature de Client est décrit dans la DPC.

[2] Ou équivalent

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du Certificat. De plus, si le RC n'est pas le demandeur, il doit également être informé de la révocation effective du Certificat Client.

L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du Certificat.

Les causes de révocation des Certificats ne sont pas publiées.

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

La DPC de l'AC « **Almerys Customer Services CA NB**» précise les procédures à mettre en œuvre en cas de révocation d'un Certificat d'une composante de l'IGC.

En cas de révocation d'un des Certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des Clients concernés que leur Certificat n'est plus valide.

4.9.4. Délai accordé pour formuler la demande de révocation

Dès qu'une entité autorisée (cf 4.9.2 « Origine d'une demande de révocation ») a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

Almerys réalise le traitement effectif d'un certificat dans un délai de 60 minutes à partir de la validation de la demande. L'horloge sur laquelle Almerys s'appuie pour calculer ce délai est synchronisée avec le temps UTC au moins une fois toutes les 24 heures.

4.9.5.1. Révocation d'un certificat cachet

Par nature une demande de révocation doit être traitée en urgence.
Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme aux engagements contractuels établis entre Almerys et le Client.
Par défaut, l'AE s'engage à réaliser la révocation dans les 72 heures.

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

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

La révocation du Certificat est effective lorsque le numéro de série du Certificat est introduit dans la liste de révocation de l'AC qui a émis le Certificat, et que cette liste est accessible au téléchargement. La révocation d'un Certificat de signature de l'AC (signature de certificats et de LAR) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.6. Exigences de vérification de la révocation par les applications utilisatrices de certificats

L'application utilisatrice d'un Certificat de Client est tenue de vérifier, avant son utilisation, l'état des Certificats de l'ensemble de la chaîne de certification correspondante, y compris le Certificat du Client lui-même.

4.9.7. Fréquence d'établissement des LCR

La fréquence d'établissement des LCR est au maximum de 24 heures (durée maximale pendant laquelle aucune révocation naturelle n'a eu lieu). La durée de validité est de 72 heures.
Concernant les CRL émises par l'AC Racine, elles sont générées

- au moins une fois par an avec une durée de vie inférieure à un an ;
- systématiquement après toute révocation d'un certificat d'AC.

4.9.8. Délai maximum de publication d'une LCR

Suite à sa génération, une LCR doit être publiée dans le délai maximum de 60 Minutes.

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

Almerys a mis en place un dispositif OCSP. L'adresse du système est précisée dans le profil des certificats émis. L'accès au service OCSP est disponible uniquement pour les professionnelles via des VPN sur le SI almerys, l'OCSP n'est pas accessible via internet.
Les résultats retournés par l'OCSP et les LCR sont consistants modulo les délais de publication des CRLs.

4.9.10. Exigences de vérification en ligne de la révocation des certificats par les applications utilisatrices de certificats

Cf. section 4.9.6 « Exigences de vérification de la révocation par les applications utilisatrices de certificats » ci-dessus.

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

Pour les Certificats des Clients, les personnels autorisés à effectuer une demande de révocation sont tenus de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les Certificats d'AC, outre les exigences du chapitre 4.9.3.2, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC.

4.9.13. Causes possibles d'une suspension

Sans objet.

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 fournit aux Applications utilisatrices de certificats 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 des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état des Certificats de l'ACR.

La fonction d'information sur l'état des certificats met à la disposition des applications utilisatrices de certificats un mécanisme de consultation libre de LCR/LAR. Ces LCR/LAR sont des LCR/LAR respectant le format X.509v2 [RFC5280], publiées en mode HTTP directement accessibles via l'Internet.

Le chapitre 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR » fournit les informations de format sur les LCR, ainsi que les URL de publication des LCR/LAR.

4.10.2. Disponibilité de la fonction

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

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme aux engagements contractuels établis entre Almerys et le Client.

4.10.3. Dispositifs optionnels

Sans objet.

4.11 FIN DE LA RELATION ENTRE LE CLIENT ET L'AC

En cas de fin de relation contractuelle entre l'AC et le Client – porteur de certificat – avant la fin de validité du certificat, ce dernier est révoqué.

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Le séquestre de clé et le recouvrement sont interdits dans le cadre de la présente Politique de Certification.

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

Le Responsable de l'AC « **Almerys Customer Services CA NB**» 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 construction des sites

En fonction de la sensibilité des composants de l'IGC interne d'Almerys, les sites sont définis au niveau 1 de la politique de sécurité Almerys : impact vital (majeur pour l'entreprise).
A ce titre, la mise en sécurité du site du bâtiment respecte les mesures de sécurité physique 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 permettent également de respecter les engagements pris dans la PC ou dans les engagements contractuels avec les Clients du Service, en matière de disponibilité des services.

5.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'AC « **Almerys Customer Services CA NB**», les accès aux locaux sont contrôlés conformément au niveau de zonage des locaux de niveau 1 : « accès très restreint ».

Pour les fonctions de génération des Certificats, de génération des éléments secrets du Client, et de gestion des révocations, ainsi que toutes les fonctions identifiées comme critique dans l'analyse de risques, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. De plus, le contrôle en entrée et en sortie est permanent en heures non ouvrées (HNO).
Chaque entrée et sortie dans la zone sécurisée faire l'objet d'une surveillance indépendante. Tout personnel non-autorisé doit obligatoirement être accompagné d'une personne autorisée. Chaque entrée et sortie fait l'objet d'une traçabilité.
Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC définissent 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) est en dehors de ce périmètre de sécurité.
L'ouverture de la porte est commandée par un système de contrôle d'accès.
Les AC Racines sont opérées dans un espace physiquement isolé des autres opérations. L'accès à cet espace doit permettre son accès qu'aux personnes autorisées à accéder aux clés de l'AC Racine.

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 Customer Services CA NB**» 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 Customer Services CA NB** permettent de protéger son infrastructure contre les dégâts des eaux.

5.1.5. Prévention et protection incendie

L'AC **Almerys Customer Services CA NB** met en place des moyens de protection et de lutte contre les incendies.

5.1.6. Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) utilisés au sein de l'AC « **Almerys Customer Services CA NB**» sont traités et conservés conformément aux besoins de sécurité pour les actifs sensibles (en confidentialité, intégrité et disponibilité).
En particulier, les supports font l'objet de mesures contre les dommages, le vol, les accès non autorisés et l'obsolescence. Ces mesures s'appliquent durant toute la période de rétention du contenu de ces supports.

5.1.7. Mise hors service des supports

En fin de vie, les supports seront, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.
Les procédures et moyens de destruction et de réinitialisation sont conformes à la Politique de Sécurité d'Almerys.
Les sauvegardes sont testées régulièrement.

5.1.8. Sauvegardes hors site

En complément de sauvegardes sur sites, les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des services après incident la plus rapide possible.

5.2 MESURES DE SECURITE PROCEDURALES

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé de l'AC « **Almerys Customer Services CA NB**».
Les procédures et politiques de sécurité sont communiquées aux employés suivant le besoin d'en connaître.
Des procédures sont établies et appliquées pour toutes les opérations des personnels en rôle de confiance pouvant impacter la fourniture du service.

5.2.1. Rôles de confiance

Les rôles de confiance définis ci-dessous sont ceux requis pour les composantes de l'IGC, indépendamment des rôles de confiance définis dans le cadre de la cérémonie des clés.

- 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 Customer Services CA NB**». 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 Customer**

Services CA NB». 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 Customer Services CA NB**».
- Opérateur d'enregistrement – Personne responsable pour vérifier les informations nécessaires à la délivrance d'un certificat et approuver les demandes de certificat.
- Opérateur de révocation – Personne responsable pour toutes les opérations de changement d'un statut de certificat.

5.2.2. Nombre de personnes requises par tâches

La DPC de l'AC « **Almerys Customer Services CA NB**» précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.), en particulier, les personnes requises pour la cérémonie des clés.

5.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC fait 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,
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.
- Ces contrôles sont décrits dans la DPC de l'AC « **Almerys Customer Services CA NB**» et sont conformes à la Politique de Sécurité d'Almerys.

Les rôles d'opérateurs, d'administrateurs et de contrôleurs sont directement gérés par Almerys. Les administrateurs sont en charge de la gestion des comptes. Ils effectuent les modifications et/ou suppressions des accès sans délais.
Les opérations réalisées par les personnels en rôle de confiance sont tracées.

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 décrites dans la DPC de l'AC « **Almerys Customer Services CA NB**» et sont conformes à la Politique de Sécurité d'Almerys.
Pour les différents rôles de confiance, il est recommandé qu'une même personne ne détienne pas plusieurs rôles et les cumuls suivants sont interdits :

- officier de sécurité et ingénieur système / opérateur,
- ingénieur système et opérateur.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé de l'AC « **Almerys Customer Services CA NB**».

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité.

Le responsable de l'AC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de l'IGC, 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 ainsi que des mesures de protection des données personnelles.

L'AC « **Almerys Customer Services CA NB**» informe toute personne intervenant dans des rôles de confiance de l'IGC :

- de ses responsabilités relatives aux services de l'IGC,
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.
- Cette nomination est réalisée de façon formelle par le responsable de la sécurité de l'AC et est accepté par écrit par la personne nommée dans un rôle de confiance.

Les qualifications, compétences et habilitations requises pour la cérémonie des clés sont définies dans une procédure spécifique.
Les responsabilités des personnels dans les rôles de confiance sont attribuées de façon à séparer les rôles et responsabilité, éviter les conflits d'intérêt et réduire les opportunités de modification ou de mauvaise utilisation, volontaire ou involontaire, des systèmes de l'IGC.
Les accès et habilitation sont attribués et configurés suivant la politique du moindre privilège.

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 est 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 la composante de l'IGC dans laquelle il opère.
Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, les procédures, l'organisation, etc. en fonction de la nature de ces évolutions.
De plus, la formation continue inclut une formation annuelle aux nouvelles menaces et aux procédures de sécurité appliquées.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

La présente PC ne prévoit pas d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la DPC de l'AC « **Almerys Customer Services CA NB**».

5.3.6. Sanctions en cas d'actions non autorisées

Des sanctions appropriées sont appliquées aux personnelles qui ne respecteraient pas les procédures et politiques de sécurité applicables. Des précisions peuvent être apportées dans la DPC de l'AC « **Almerys Customer Services CA NB**».

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

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

5.3.8. Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille, plus spécifiquement de la Politique de Sécurité l'impactant.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'événements consiste à enregistrer des événements 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.

5.4.1. Type d'événements à enregistrer

Chaque entité opérant une composante de l'IGC journalise au minimum les événements suivants, automatiquement dès le démarrage d'un système et sous forme électronique :

- création / modification / suppression des données d'authentification correspondantes (mots de passe, certificats, etc.),
- démarrage et arrêt des systèmes informatiques et des applications,
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation,
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.
- Changement de la politique de sécurité
- Arrêt système inopiné, crash, détection d'erreurs matérielles
- Activité des routeurs et des pare-feu

D'autres événements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques,
- les actions de maintenance et de changements de la configuration des systèmes,
- les changements apportés au personnel,

- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des événements spécifiques aux différentes fonctions de l'IGC sont également journalisés, notamment :

- réception d'une demande de Certificat (initiale et renouvellement),
- validation / rejet d'une demande de certificat,
- évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...),
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.),
- génération des Bi-clés de signature des Clients,
- génération des Certificats des Clients,
- transmission des Certificats aux Clients,
- réception d'une demande de révocation,
- validation / rejet d'une demande de révocation,
- génération puis publication des LCR
- évènements liés à la dissémination des certificats

Chaque enregistrement d'un événement dans un journal contient lorsque cela est applicable 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'évènement (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 figure explicitement dans l'un des champs du journal d'événements.

De plus, en fonction du type de l'événement, chaque enregistrement contient également les champs suivants :

- dans la mesure du possible : demandeur et destinataire 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,
- toute information caractérisant l'événement (par exemple, pour la génération d'un Certificat, le numéro de série de ce Certificat).

Les opérations de journalisation sont effectuées au cours du processus.
En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement.

5.4.2. Fréquence de traitement des journaux d'événements

Les journaux d'événements de l'IGC sont analysés en moyenne 2 à 3 fois chaque semaine. De plus, les journaux d'événements font l'objet d'analyses automatiques permettant d'identifier des activités anormales et alerter les personnels de l'occurrence potentielle d'événements critiques de sécurité.

5.4.3. Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins un mois. Les journaux sont conservés et archivées pour la durée nécessaire dans le cadre de la Législation en vigueur, même en cas de cessation d'activité de l'IGC.

5.4.4. Protection des journaux d'événements

L'AC met en œuvre une protection des journaux d'événements adaptée au niveau de sensibilité des informations contenues dans ces journaux. Ce niveau de sensibilité est issu d'une analyse de risque.

5.4.5. Procédure de sauvegarde des journaux d'événements

L'AC met en œuvre un processus de sauvegarde des journaux d'événements adapté au niveau de sensibilité des informations contenues dans ces journaux. Ce niveau de sensibilité est issu d'une analyse de risque.

5.4.6. Système de collecte des journaux d'événements

L'AC met en œuvre un système de journalisation des événements qui intègre une datation conforme aux exigences du paragraphe 6.8.

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

La PC ne prévoit pas d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la DPC de l'AC « **Almerys Customer Services CA NB** ».

5.4.8. Evaluation des vulnérabilités

L'AC met en œuvre une gestion des vulnérabilités de systèmes de l'AC « **Almerys Customer Services CA NB**» en conformité avec la Politique de Sécurité d'Almerys.

Les journaux d'évènements sont contrôlés régulièrement selon des modalités définies dans le paragraphe 5.4.2.

Les journaux sont analysés dès la détection d'une anomalie. Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées. Toute vulnérabilité critique est adressée par Almerys dans une période de 48 heures après sa découverte. Selon le résultat de son analyse, Almerys :

- mettra en place un plan de correction de la vulnérabilité ou ;
- documentera les raisons pour lesquelles aucune correction ne sera appliquée.

5.5 ARCHIVAGE DES DONNEES

5.5.1. Types de données à archiver

Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.
Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

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

- les PC ;
- les DPC ;
- les agréments contractuels avec d'autres AC ;
- les LCR tels qu'émises ou publiées ;
- les récépissés ou notifications (à titre informatif) ;
- les dossiers d'enregistrement des RC.

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 d'enregistrement : 7 ans après expiration du certificat,
- certificats émis par l'AC après expiration : 7 ans après expiration du certificat,
- dernière LCR émis par l'AC après expiration : 7 ans après expiration du certificat,
- journaux d'évènements après leur génération : 7 ans après expiration du certificat.

Almerys a mis en place les mesures nécessaires pour que ces archives soient conservées sur les durées mentionnées même en cas d'arrêt d'activité.

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 ;
- pouvoir être relues et exploitées.

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

5.5.4. Procédure de sauvegarde des archives

La procédure est précisée dans la DPC.
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 datés au moment de leur génération et cette information est archivée avec le certificat correspondant.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6. Système de collecte des archives

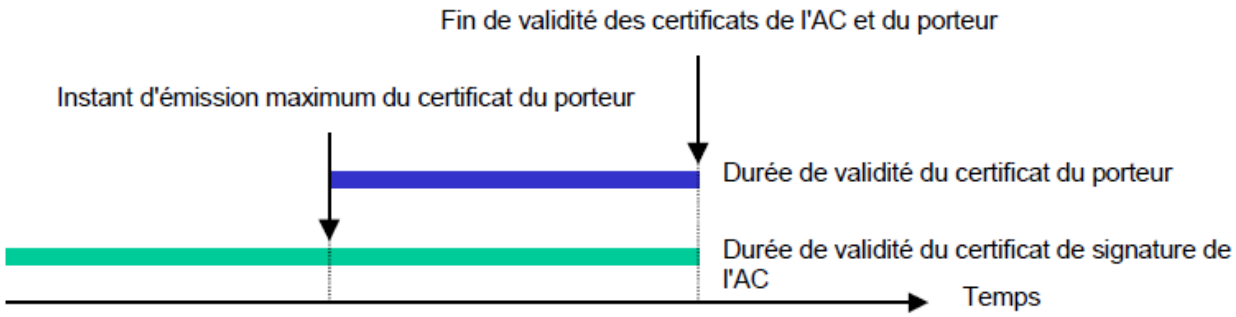
La DPC précise les moyens mis en œuvre pour collecter les archives en toute sécurité.

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).
Les conditions de récupération des archives sont précisées dans la DPC.

5.6 CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.



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

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

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

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 Customer Services CA NB**», 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.

En cas d'incident majeur de sécurité ou de perte d'intégrité ayant un impact important sur ses opérations de service de confiance ou sur les données personnelles, Almerys notifiera les parties concernées, en particulier l'organe de contrôle et la CNIL, dans les 24 heures après l'identification de l'incident, conformément aux exigences du Règlement eIDAS et, le cas échéant, les clients impactés.

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 Customer Services CA NB**» 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 d'une clé d'infrastructure ou de contrôle d'une composante de l'IGC Almerys est traité conformément au chapitre 5.7.2 « Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) ».
En particulier, en cas de compromission d'une clé d'AC, Almerys :

- Informera les clients et les porteurs de certificats impactés, ainsi que les tiers utilisateurs de certificats.
- Indiquera que les certificats émis par l'AC, ainsi que les statuts de révocation publiés, ne sont plus valides
- Révoquera immédiatement tous les certificats d'AC compromis.

En cas de compromission d'un algorithme, Almerys appliquera les mesures ci-dessous à l'exception de la révocation immédiate de tous les certificats compromis. Almerys programmera une révocation programmée en adéquation avec l'état de l'art sur les faiblesses de l'algorithme compromis.

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

Les différentes composantes de l'IGC Almerys disposent des moyens raisonnablement nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. section 5.7.2 « Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) »).
Almerys dispose d'un plan de continuité d'activité à jour afin de réagir efficacement en cas de désastre et de restaurer le système dans les délais précisé dans ce plan. Ce plan comprend en particulier les cas de compromission de clé privée d'AC ou de perte des moyens d'activation de la clé.

5.8 FIN DE VIE DE L'IGC

Une ou plusieurs composantes de l'IGC Almerys peut être amenée à cesser son activité en tout ou partie, ou à la transférer à une autre entité.
Almerys a provisionné les moyens nécessaires en cas de cessation d'activité. Ces moyens sont décrits dans un plan d'arrêt d'activité tenu à jour par Almerys.

La compromission de la Bi-clé de l'AC « **Almerys Customer Services CA NB**» entraîne immédiatement sa cessation d'activité et la révocation de tous les Certificats émis en cours de validité. Pour retrouver le niveau de service, la création d'une nouvelle AC et de nouveaux Certificats sont obligatoires.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC Almerys

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC « **Almerys Customer Services CA NB** » s'engage, entre autres obligations :

1) à mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des Certificats des Clients et des informations relatives aux Certificats) ;
2) à assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.

L'AC « **Almerys Customer Services CA NB**» s'engage à respecter les points suivants :

1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des Clients ou des applications utilisatrices de certificats, l'AC « **Almerys Customer Services CA NB**» doit les en aviser aussitôt que nécessaire et, au moins, sous le délai de mois.
2) L'AC « **Almerys Customer Services CA NB** » doit communiquer aux Clients les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC « **Almerys Customer Services CA NB**» devra communiquer aux Clients les modalités des changements survenus. L'AC « **Almerys Customer Services CA NB** » mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les Clients.
3) L'AC « **Almerys Customer Services CA NB**» doit tenir informés les Clients et autres entités de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus. Almerys s'engage à notifier l'organe de control, ainsi que toutes les autorités pertinentes, en cas de fin de vie de l'IGC ainsi qu'à mettre l'information disponible pour des tiers utilisateurs des certificats

Cessation d'activité affectant l'AC « Almerys Customer Services CA NB»

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de Certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC « **Almerys Customer Services CA NB**», ou une entité tierce qui reprend les activités, lors de l'expiration du dernier Certificat émis par elle.
Dans l'hypothèse d'une cessation d'activité totale, l'AC « **Almerys Customer Services CA NB**» 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, assure la révocation des Certificats et la publication des LCR conformément aux engagements pris dans sa PC.

Lors de l'arrêt du Service, l'AC « **Almerys Customer Services CA NB**» :

1) détruit la clé privée lui ayant permis d'émettre des Certificats ainsi que toutes ces copies;
2) prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) révoque son Certificat ;

4) révoque tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;
5) informe (par exemple par récépissé) tous les Porteurs des certificats révoqués ou à révoquer ;
6) Transfert à un tiers l'obligation de disponibilité des informations publiée, en particulier de de sa clé publique.

6. MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI-CLES

6.1.1. Génération des bi-clés

6.1.1.1. Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé.

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique certifié Fips 140-2 Niveau 3 (cf. également la section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques »).

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre d'une « Cérémonies des Clés » (ou encore Key Ceremony – KC). Cette cérémonie se déroule suivant des scripts, organisationnels et techniques, préalablement définis.
Le script de « Cérémonie des clés » indique :

- L'ensemble des rôles des participants de la cérémonie
- Les fonctions de chacun de ces rôles et les phases auxquelles ils interviennent
- Leurs responsabilités durant la cérémonie et à l'issue de celle-ci
- Les preuves qui seront recueillis durant la cérémonie.

La cérémonie se fait en présence :

- D'un officier de sécurité pour une clé d'AC
- D'un officier de sécurité et d'un huissier pour un certificat d'AC Racine.

La cérémonie fait l'objet d'un PV signé des participants attestant qu'elle s'est déroulée conformément à la procédure prévue et démontrant que l'intégrité et la confidentialité de la génération de la paire de clé a été assurée.
La génération des clés d'AC s'accompagne de la génération de différents secrets et éléments sensibles. Ces secrets sont des données permettant de gérer de manière sécurisée (personne ne peut posséder l'intégralité du secret), et ultérieurement à la Cérémonie des Clés, les opérations sur le HSM cryptographique, notamment, de pouvoir redémarrer, sauvegarder, et restaurer la sauvegarde de la partition HSM.

Suite à leur génération, les secrets sont remis à des Détenteurs de secrets désignés au préalable et habilités à ce rôle de confiance.

Le renouvellement du Certificat et des clés de l'AC suit les mêmes principes que ceux de la première génération des clés d'AC.
L'émission d'un certificat par l'AC Racine est réalisée obligatoirement par deux personnels autorisés ayant un rôle de confiance.

6.1.1.2. Clés Client générées par l'AC

Le Service de stockage sécurisé de Bi-clé de l'AC « **Almerys Customer Services CA NB**» est en charge de la génération des Bi-clés de signature des Clients.

La génération et le stockage de la Bi-clé de signature se fait au sein d'un module cryptographique matériel certifié FIPS 140-2 niveau 3. Ce module est hébergé dans les locaux à accès très restreint Almerys.

La génération des clés de signature Client est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre d'une « Cérémonies des Clés Client » (ou encore Key Ceremony – KC Client). Cette cérémonie se déroule suivant des scripts, organisationnels et techniques, préalablement définis.

La génération des clés de signature Client s'accompagne de la génération de différents secrets et éléments sensibles. Ces secrets sont des données permettant de gérer et de manipuler de manière sécurisée (personne ne peut posséder l'intégralité du secret), et ultérieurement à la Cérémonie des Clés, la clé privée de signature du Client, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signature Client.

Suite à leur génération, les secrets sont remis à des Détenteurs de secrets désignés au préalable et habilités à ce rôle de confiance par le Client.

6.1.1.3. Clés Clients générées par le Client

Le Client n'a pas la charge de la génération des Bi-clés cryptographiques.
Cette génération est à la charge d'Almerys conformément au paragraphe 6.1.1.2, et notamment pour les certificats d'horodatage.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée Client n'est jamais transmise « en clair » au RC, car elle est stockée de manière sécurisée au sein du Service de stockage sécurisé de Bi-clé de l'AC, et ne peut en aucun cas être exportée en clair compte tenu de la configuration des Modules cryptographiques matériels.

Cependant, les différents secrets générés lors de la KC Client permettant d'obtenir une sauvegarde sécurisée (chiffrée et répartie) de la Bi-clé de signature du Client peuvent être remis en totalité au RC.
Il est alors de la responsabilité du RC de choisir les Détenteurs de secrets auxquels vont être attribués les secrets. Ces Détenteurs doivent pouvoir être mobilisés s'il est nécessaire de réinstaller les secrets Client (installation d'un nouveau Module, reprise sur incident).

6.1.3. Transmission de la clé publique à l'AC

La clé publique est transmise à l'AC « **Almerys Customer Services CA NB**» dans la demande de génération de Certificat. La clé est protégée en intégrité et l'origine est authentifiée grâce à l'utilisation d'une enveloppe au format PKCS#10 qui est signée par la clé privée associée à la clé publique.

6.1.4. Transmission de la clé publique de l'AC aux Applications utilisatrices de certificats

Plus d'informations sur le sujet sont fournies dans la PC de l'ACR d'Almerys.

6.1.5. Tailles des clés

Les tailles de clés sont les suivantes :

- Certificat de l'AC « **Almerys Customer Services CA NB**» : 4096 bits (algorithme RSA)
- Certificats des Clients : 2048 bits (algorithme RSA)

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

L'équipement de génération de Bi-clé utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant au Bi-clé. Ces paramètres sont rappelés dans le chapitre 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ». De plus, cet équipement est configuré pour respecter au minimum une configuration FIPS 140-2 niveau 2 minimum qui interdit les algorithmes et paramètres considérés comme faibles, ainsi que l'exportation en clair de la clé privée de Signature du Client.

6.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du Certificat associé est strictement limitée à la signature de Certificats et de LAR.

L'usage de la clé privée du Client et du Certificat associé est strictement limité au Service Almerys (cf. sections 1.4 « Usage des certificats » et 7.2 pour les restrictions dans le format de certificat *Customers Services*).

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

6.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature sont certifiés Fips 140-2 niveau 3.

6.2.1.2. Dispositifs de création de signature des Clients

Les dispositifs de création de signature des Clients pouvant être utilisés sont des modules cryptographiques matériels certifiés FIPS 140-2 niveau 3 pour les certificats de signature avec gestion sécurisée Almerys. Sa configuration opérationnelle minimale est conforme au standard FIPS 140-2 niveau 2.

Le Service de stockage sécurisé des Bi-clés de l'AC est chargé du maintien opérationnel et de la sécurité de ces Modules.

6.2.2. Contrôle de la clé privée de l'AC par plusieurs personnes

Le contrôle de la clé privée de l'AC est assuré pour les actions suivantes :

- pour l'exportation / l'importation hors / dans un module cryptographique : les systèmes sont configurés pour interdire l'exportation en clair de la clé privée, assurant ainsi sa non compromission ;
- pour la génération de la bi-clé (cf. 6.1.1.1) : utilisation d'un module cryptographique matériel sécurisé pour la génération et le stockage de la clé privée, et le partage des secrets assure qu'aucun acteur ne puisse accéder ou interpréter un des secrets ;

- pour l'activation de la clé privée (cf. section 6.2.8) : les flux de requêtes de certificats et de révocation (mise à jour de la LCR) sont maîtrisés pour s'assurer que seuls les services autorisés puissent être enregistrés ; l'action d'autorisation et de configuration de ces flux nécessite la présence d'au minimum 2 Officiers PKI;
- pour la destruction (cf. section 6.2.10) : les procédures de destruction permettent de s'assurer que personne ne pourra utiliser la clé privé.

6.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des Clients ne sont séquestrées.

6.2.4. Copie de secours de la clé privée

Les partitions contenant les clés privées des Clients font l'objet de copies de secours hors des modules cryptographiques sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

La partition contenant clé privée d'AC fait l'objet de copies de secours hors des modules cryptographiques sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.
L'installation et la restauration des clés d'AC dans un module cryptographique requièrent le contrôle simultané de deux personnels en rôle de confiance.

6.2.5. Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivées.
Les clés privées des Clients ne sont pas archivées, ni par l'AC, ni par aucune des composantes de l'IGC.

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

Pour les clés privées d'AC, tout transfert se fait sous forme chiffrée, conformément aux indications de la section 6.2.4 « Copie de secours de la clé privée ».

Pour les clés privées de signature des Clients, tout transfert se fait sous forme chiffrée, conformément aux indications de la section 6.2.4 « Copie de secours de la clé privée ».

6.2.7. Stockage de la clé privée dans un module cryptographique

cf. section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques ».

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clé privée d'AC

cf. 6.2.2 « Contrôle de la clé privée de l'AC par plusieurs personnes ».

6.2.8.2. Clés privées des Clients

L'activation de la clé privée du Client est contrôlée via des données ou des actions d'activation (cf. section 6.4 « Données d'activation ») propres au Client.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clé privée d'AC

La désactivation de la clé privée d'AC dans les modules cryptographiques est automatique dès que l'environnement du module évolue de manière sensible : choc, déconnexion, etc.
Les modalités de désactivation sont propres à la technologie du module ; elles sont détaillées dans la documentation constructeur.

6.2.9.2. Clés privées des Clients

L'activation des clés privées des Clients peut être temporairement suspendue ou définitivement interdite en cas de non-respect des termes contractuels définis entre l'AC et le Client du Service.

La désactivation de la clé privée des Clients dans les Modules cryptographiques matériels est automatique dès que l'environnement du module évolue de manière sensible : choc, déconnexion, etc.
Les modalités de désactivation sont propres à la technologie du module ; elles sont détaillées dans la documentation constructeur.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Clés privées d'AC

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2. Clés privées des Clients

La clé privée de signature d'un Client doit être automatiquement détruite dès lors que le Certificat associé à cette clé a expiré. Cette clé est alors systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

cf. section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques ».

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des Clients sont archivées dans le cadre de l'archivage des Certificats correspondants.

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

Les Bi-clés et les Certificats des Clients couverts par la présente PC ont une durée de vie de 3 ans. D'autre part, les Bi-clés et les Certificats ont la même durée de vie.

6.4 DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

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

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se fait lors de la phase d'initialisation et de personnalisation de ce module.

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du Client

La génération et l'installation des données d'activation du Module cryptographique matériel pour les clés privées de signature se fait lors de la phase d'initialisation et de personnalisation de ce module et lors de la KC Client.
L'enregistrement des modules applicatifs du Service au niveau du Module cryptographique nécessite également l'installation de données d'activation pour que le Service puisse communiquer avec la partition cryptographique Client contenant les secrets de signature.

6.4.2. Protection des données d'activation

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

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

6.4.2.2. Protection des données d'activation correspondant aux clés privées des Clients

Les données d'activation qui sont générées par l'AC pour les partitions cryptographiques des Clients sont protégées en intégrité et en confidentialité jusqu'à la remise au destinataire. Ce dernier a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

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 « **Almerys Customer Services CA NB**». Il répond en particulier aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;

- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- protection du réseau contre toute intrusion d'une personne non autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle doit être cohérente avec la Politique de Sécurité.
Pour atteindre ces objectifs de sécurité, Almerys utilise des systèmes et des produits fiables permettant de mettre en œuvre de façon sécurisé les différents processus de l'IGC. Les systèmes et produits sont choisis et/ou développé en prenant en compte les exigences de sécurité.
Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système sont mis en place.
Ces dispositifs permettent

- de détecter, enregistrer et réagir dans les meilleurs délais à un accès ou une tentative d'accès non autorisée aux ressources de l'IGC ;
- de surveiller l'usage du service et les requêtes ;
- de déclencher des alarmes en cas de détection de potentielles violations des mesures de sécurité ;
- de surveiller l'activation ou la désactivation des fonctions de génération de traces ;
- de surveiller la disponibilité et le trafic réseau

Les dispositifs de surveillance prennent en compte la sensitivité de l'information collectée et analysées. Le suivi des alertes sur les événements critiques de sécurité est assuré par des personnels en rôle de confiance. Ces derniers s'assurent que les incidents sont analysés et sont traités suivant les procédures en places.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.6.1. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre 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.
Des procédures de contrôle des changements sont mises en œuvre et appliquées à chaque modification (planifiée ou urgente) du système d'information ou de sa configuration.

6.6.2. Mesures liées à la gestion de la sécurité

6.6.2.1. Mise à jour des composantes

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.
En particulier, Almerys a spécifié et mis-en place des procédures de gestion des mises-à-jour de sécurité, afin que celle-ci soient appliquées dans les meilleurs délais. En cas d'introduction potentielle de nouvelles vulnérabilités ou de mise en danger de la stabilité du système, Almerys documentera les raisons de non-application d'une mise à jour de sécurité.

6.6.2.2. Analyse des risques

Almerys a réalisé une analyse de risque pour identifier, analyser et évaluer les risques pesant sur l'IGC en prenant en compte les risques techniques et métier. Suite à cette analyse de risque, Almerys a sélectionner et mis en œuvre des mesures de traitement du risque et les procédures opérationnelles associées, de telle façon que le niveau de sécurité soit approprié vis-à-vis du degré de risque.

L'analyse de risque est approuvée par le Responsable de l'IGC qui accepte, par cette approbation, le risque résiduel identifié.

Les mesures de traitement du risque sont décrites dans la DPC d'Almerys ainsi que dans sa PSSI.

Cette analyse de risque est revue régulièrement, a minima annuellement et lors de toute évolution significative d'un système ou d'une composante de l'IGC Almerys.

6.6.2.1. Scan de vulnérabilité

Almerys réalise régulièrement des scans de vulnérabilité sur ses adresses IP publiques et privées. Chaque scan est réalisé par une personne ou une entité qualifié et indépendante.

6.6.2.1. Test d'intrusion

Almerys réalise des tests d'intrusion lors de la mise en place de nouvelles infrastructures ou lors de modification significatives d'une composante. Almerys garde des éléments de preuves de la qualification et de l'indépendance du testeur.

6.7 MESURES DE SECURITE RESEAU

6.7.1. Segmentation en zone

Fondé sur les résultats de l'analyse de risque, Almerys a segmenté son réseau en zone séparées (fonctionnellement, logiquement ou physiquement). Des mesures de contrôle similaire sont mis-e-place pour l'ensemble des éléments d'une même zone. Chaque système de l'IGC est exploité dans une zone réseau sécurisée et est installé suivant des procédures et une configuration assurant une exploitation sécurisée.
Les systèmes les plus critiques, tels que les AC Racines, sont opérés dans les zones les plus sécurisées.

Almerys a également mis en place une séparation stricte entre les systèmes de production et les autres systèmes (test, qualification,…)

6.7.2. Interconnexion

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement et logiquement sécurisé.

De plus, les échanges entre composantes au sein de l'IGC Almerys font l'objet de la mise en place de canaux sécurisés logiquement distincts et permettant d'assurer l'authentification de la destination des données et d'assurer l'intégrité et la confidentialité des données échangées.

6.7.3. Connexions

Seuls les personnels en rôle de confiance ont accès aux zones réseaux sécurisées. De plus, les échanges entre composantes au sein de l'IGC Almerys font l'objet de la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés notamment).
Toute connexion d'un compte permettant de créer directement un certificat n'est possible qu'après une authentification multi-facteur. Les réseaux permettant d'opérer et d'administré l'IGC sont séparés. Le réseau d'administration est dédié à cet usage.

Tous les systèmes de l'AC sont configurés de façon à supprimer ou désactivé les comptes, applications, services et ports qui ne sont pas utilisés pour les opérations de l'IGC.

6.7.4. Disponibilité

Afin de répondre aux besoins de disponibilité de ses composantes, Almerys a mis en place des mesures de redondances permettant d'offrir une haute disponibilité des services critiques.

6.8 HORODATAGE / SYSTEME DE DATATION

Les systèmes de datation sont synchronisés par rapport à une source fiable du temps universel (UTC) et un système de synchronisation temporelle (NTP) avec une précision au moins égale à une minute.

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 PROFIL DU CERTIFICAT DE L'AC « ALMERYS CUSTOMER SERVICES CA NB»

Le tableau suivant fournit les valeurs des attributs du Certificat de l'AC « **Almerys Customer Services CA NB**» émis par l'AC racine « ALMERYS ROOT CA ».
Le format de ce certificat ainsi que ses attributs respectent le profil X.509v3 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire
signature		
▶ algorithm		Sha256withRSAEncryption
▶ 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= ALMERYS CUSTOMER SERVICES CA NB OU=ADVANCED SERVICES 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	Non	Stratégie du certificat : Identificateur de stratégie = 1.2.250.1.16.12.5.41.1.5.2.1
▶ basicContraints ➥ cA ➥ pathLenConstraint	Oui	 True None
▶ cRLDistributionPoints	Non	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	non	[1] : accessMethod : id-ad-caIssuers accessLocation : URL=http://pki.almerys.com/almerysrootca.cer
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption, clé de 4096 bits
parameters		NULL

7.1.1. Profil des certificats Customers Services

Le tableau suivant fournit les valeurs par défaut des attributs d'un Certificat Customers Services émis par l'AC « **Almerys Customer Services CA NB**».
Le format de ce Certificat ainsi que ses attributs respecte le profil X.509v3 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

7.1.2. Certificat cachet signature profil eIDAS

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ALMERYS CUSTOMER SERVICES CA NB OU = ADVANCED SERVICES OU = 0002 432701639 O = ALMERYS C = FR
validity		
▶ notBefore		Date de création
▶ notAfter		notBefore + 3 ans
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = <Service signature> OI= <NTR ou VAT><code pays>-<Identifiant NTR ou identifiant TVA> OU = organisation unit O = <raison sociale> C = <code pays>
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		 rsaEncryption RSAParams : NULL
▶ subjectPublicKey		DER encoded RSAPublicKey (2048 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	digitalSignature (0)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie =1.3.6.1.4.1.48620.41.1.5.2.1.1.1
▶ basicContraints ⮑ cA ⮑ pathLenConstraint	Non	false None
▶ extKeyUsage		Extension non utilisée
▶ cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almeryscustomerservicescanb.crl
Private extensions		
▶ authorityInfoAccess	Non	[1] : accessMethod : id-ad-caIssuers accessLocation : URL=http://pki.almerys.com/almeryscustomerservicescanb.cer [2] accessMethod : id-ad-ocsp accessLocation : http://ocsp.almerys.com
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

[1] Variables de l'attribut subject DN :

- <Service> = Service proposé par le Client à ses Utilisateurs, et pour lequel le certificat est utilisable
- <SIREN/SIRET Client> = SIREN/SIRET du Client du Service ou équivalent
- <Informations> = Des champs OU optionnels de description de l'entité cliente ou du Service peuvent être ajoutés
- <Client> = raison sociale du Client du Service

7.1.3. Certificat cachet horodatage

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ALMERYS CUSTOMER SERVICES CA NB OU = ADVANCED SERVICES OU = 0002 432701639 O = ALMERYS C = FR
validity		
▶ notBefore		Date de création
▶ notAfter		notBefore + 3 ans
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = <Service Horodatage XX> OI= <NTR ou VAT><code pays>-< Identifiant NTR ou identifiant TVA> OU = organisation unit O = <raison sociale> C = <code pays>
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		rsaEncryption RSAParams : NULL
▶ subjectPublicKey		RSAPublicKey (2048 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	digitalSignature (0)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.5.2.1.2.1
▶ basicContraints ➥ cA ➥ pathLenConstraint	Non	false None
▶ extKeyUsage	oui	id-kp-timestamping
▶ cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution :

		Nom complet : URL=http://pki.almerys.com/almeryscustomerservicescanb.crl
Private extensions		
▶ authorityInfoAccess	Non	[1] : accessMethod : id-ad-caIssuers accessLocation : http://pki.almerys.com/almeryscustomerservicescanb.cer [2] accessMethod : id-ad-ocsp accessLocation : http://ocsp.almerys.com
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.2 PROFIL DE L'OCSP

tbsCertList		Valeur
version		2 (c'est-à-dire version 3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		CN = ALMERYS CUSTOMER SERVICES CA NB OU=ADVANCED SERVICES OU = 0002 432701639 O = ALMERYS C = FR
validity		
▶notBefore		Date de création
▶notAfter		notBefore + 3 ans Maximum
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		CN = <service OCSP XX>[3] OU = organisation unit[4] OI = <NTRou VAT><code pays>- < Identifiant NTR ou identifiant TVA >[5] O = <Raison socia>[6] C = FR
subjectPublicKeyInfo		

[3] Où <XX> sera remplacé par l'indice du certificat d'OCSP en commençant à « 01 ».
[4] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ».
[5] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ».
[6] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ».

▶algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams : NULL
▶subjectPublicKey		DER encoded RSAPublicKey (2048 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	digitalSignature
▶certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie =1.3.6.1.4.1.48620.41.1.5.2.1.6.1
▶extKeyUsage	Non	OCSPSigning
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.3 PROFIL DE LCR

Le tableau suivant fournit les valeurs par défaut des attributs de la Liste de Certificats Révoqués (LCR) émise par l'AC « **Almerys Customer Services CA NB** ».
Le format de cette LCR ainsi que ses attributs respectent le profil X.509v2 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

tbsCertList		**Valeur**
version		1 (c'est-à-dire version2)
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= ALMERYS CUSTOMER SERVICES CA NB OU=ADVANCED SERVICES OU=0002 432701639 O= ALMERYS C=FR
thisUpdate		Date de création (référentiel temporel de l'AC)
nextUpdate		nextUpdate + 72 heures
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	160 bits du haché SHA-1 de la clé publique de l'issuer
▶ issuerAltName	-	Extension non utilisée
▶ cRLNumber	Non	Numéro de séquence de la LCR (incrémental simple).
▶ deltaCRLIndicator	-	Extension non utilisée
▶ freshestCRL	-	Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11), clé de 4096 bits
parameters		NULL

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre concerne que les audits et évaluations de la responsabilité de l'AC ou de l'AE afin de s'assurer du bon fonctionnement de son IGC.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Suite à toute modification significative d'une composante de l'IGC, l'AG procède à une analyse de sécurité et fait évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.
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'AG choisit et assigne une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité 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, et 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'AG, 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'AG qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du Certificat de la composante, la révocation de l'ensemble des Certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AG et doit respecter ses politiques de sécurité internes ;
- en cas de résultat « à confirmer », l'AG remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. 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 modalités de communication concernant les résultats des audits de conformité sont précisées dans la DPC.

8.7 AUTRES ELEMENTS DE CONFORMITE

Les pratiques de l'AC sont non-discriminatoires. Dans la mesure du possible, l'AC mettra en œuvre toutes les dispositions nécessaires pour rendre accessible son service aux personnes en situation de handicap.

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

Les informations suivantes sont fournies dans les différents documents contractuels établis entre les parties : (i.e. Almerys, les Clients du service, et éventuellement les fournisseurs assurant en tout ou partie certaines fonctions de l'AC « **Almerys Customer Services CA NB**» ou de l'AE) :

- les conditions de facturation du Service proposé par Almerys,
- les responsabilités,
- les responsabilités financières,
- le montant des indemnités.

L'accès à la fonction sur l'état des certificats n'est pas soumis à tarification.

9.2 RESPONSABILITE FINANCIERE

Cf 9.1 « Tarifs ».

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1. Périmètre des informations confidentielles

La classification des informations se décompose en :

- secret (niveau 4 de la Politique de Sécurité) ;
- confidentiel (niveau 3 de la Politique de Sécurité) ;
- interne (niveau 2 de la Politique de Sécurité).

Les informations considérées comme « secret » sont au moins les suivantes :

- les clés privées des AC de l'IGC Almerys, des composantes et des Porteurs de certificats ;
- tous les secrets de l'IGC, notamment les informations liées à la gestion des modules cryptographiques (HSM) ;
- les données d'activation associées aux clés privées d'AC et de Clients.

Les informations considérées comme « confidentiel » sont au moins les suivantes :

- la DPC de l'AC ;
- les journaux d'événements des composantes de l'IGC ;
- les causes de révocations, sauf accord explicite de publication du Client ;
- les dossiers d'enregistrement des Clients.

9.3.2. Informations hors du périmètre des informations confidentielles

Par défaut, en complément des informations déjà explicitement listées dans les paragraphes 9.3.1 et 9.4, une information est considérée comme confidentielle à l'exception des informations publiées dont la liste est fournie dans la section 2.2 « Informations devant être publiées », et n'est diffusée qu'avec le consentement explicite de l'AG de l'IGC Almerys aux personnes ayant le besoin d'en connaître.

9.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des Clients à des tiers dans le cadre de procédures légales.

9.4 PROTECTION DES DONNEES A CARACTERE PERSONNEL

9.4.1. Politique de protection des données à caractère personnel

Toute collecte et tout traitement de données à caractère personnel par l'AE et l'AC « **Almerys Customer Services CA NB** » sont réalisés dans le strict respect de la réglementation en vigueur, et en particulier le règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit « Règlement Général sur la Protection des Données (RGPD) [RGPD].

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des Certificats des Clients (qui sont considérées comme confidentielles sauf accord explicite du Client) ;
- les informations d'enregistrement du Client.

Elles sont traitées dans le strict respect de la réglementation en vigueur relative au [RGPD].

9.4.3. Responsabilité en termes de protection des données à caractère personnel

Le Client est responsable du respect de la réglementation en vigueur dite [RGPD].
Le traitement des données à caractère personnel est sous la responsabilité du président du directoire groupe be-ys. Pour la conformité [RGPD], almerys a mis en place une organisation centrée sur le le Délégué à la Protection des Données DPO.

9.4.4. Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations à caractère personnel remises par les Clients à l'AE ne sont ni divulguées ni transférées à un tiers, sauf dans les cas suivants : consentement préalable de la personne concernée, décision judiciaire ou autre autorisation légale.

9.4.5. Conditions de divulgation d'informations à caractère personnel aux autorités judiciaires ou administratives

Toute diffusion et communication des données à caractère personnel vers des tiers autorisés doivent être en conformité aux lois spécifiques y afférant.

9.4.6. Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

Tous les droits de propriété intellectuelle détenus par l'IGC Almerys sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de non-respect. Par exemple, conformément au droit applicable les bases de données réalisées par les composantes de l'IGC sont protégées.

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

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'IGC 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 présente PC 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 audits de sécurité et aux contrôles de conformité demandés par les parties prenantes dûment identifiées et habilitées,
- respecter les accords ou contrats qui les lient entre elles ou avec les Clients,
- 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. Autorité de Certification

L'AC « **Almerys Customer Services CA NB**» a pour obligation de :

- pouvoir démontrer aux Applications utilisatrices de ses Certificats qu'elle a émis un Certificat pour un Client donné et que ce Client a accepté le Certificat, conformément aux exigences du chapitre 4.4 « Acceptation du certificat » ci-dessus ;
- protéger les clés privées de signature des Clients conformément aux exigences de la présente PC ;
- garantir et maintenir la cohérence de la DPC avec la PC.

9.6.2. Autorité de gouvernance

L'AG est responsable de la conformité de la PC de l'AC « **Almerys Customer Services CA NB**CA », avec les exigences émises dans la PC de l'ACR. L'AG assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la PC de l'ACR, par l'AC « **Almerys Customer Services CA NB**» ou l'une des composantes de l'IGC. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées aux opérations et/ou activités de l'AC « **Almerys Customer Services CA NB**» et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC de l'ACR.

De plus, l'AG reconnaît engager sa responsabilité en cas de faute ou de négligence de l'AC « **Almerys Customer Services CA NB** » ou de l'une des composantes de l'IGC, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données à caractère personnel des Clients à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des Certificats de l'AC « **Almerys Customer Services CA NB**».

Par ailleurs, l'AG reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des Certificats délivrés par l'AC « **Almerys Customer Services CA NB**» ou l'une des composantes de l'IGC. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services.

9.6.3. Autorité d'enregistrement

Outre ses responsabilités décrites dans l'introduction de la section 9.6, et dans les sections 1.3.3 et 4, l'AE doit :

- conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées
- et prendre toutes les mesures raisonnables pour s'assurer que les Clients qui la requêtent 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 éventuellement utilisés.

9.6.4. Client, Représentant Client

Le Client doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur.
Le RC, qui représente le Client, doit :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat,
- assister à la KC Client,
- gérer de manière sécurisée les secrets et éléments sensibles qui lui sont remis à l'issue de la KC Client, et désigner les Détenteurs de secrets Client,
- autoriser l'AC « **Almerys Customer Services CA NB**» à héberger sa clé privée de signature dans les conditions décrites dans la présente PC,
- accepter les conditions d'utilisation de sa clé privée et du certificat correspondant,
- informer l'AE de toute modification concernant les informations contenues dans son Certificat,
- faire, sans délai, une demande de révocation de son Certificat auprès de l'AE en cas de suspicion de compromission de sa clé privée (ou de ses données d'activation).

La relation entre le Client et l'AC ou ses composantes est formalisée par un engagement par le contrat de prestation du Service entre le Client et Almerys.

9.6.5. Applications utilisatrices de certificats

Les applications utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un Certificat a été émis ;
- contrôler que le Certificat émis par l'AC « **Almerys Customer Services CA NB**» est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- vérifier la signature électronique de l'AC « **Almerys Customer Services CA NB** » émettrice du Certificat en parcourant la chaîne de certification jusqu'à l'ACR « Almerys Root CA » ;

- vérifier et respecter les obligations des Applications utilisatrices de certificats exprimées dans la présente PC ;
- contrôler la validité des Certificats (dates de validité, statut de révocation).

9.6.6. Autres participants

Sans objet.

9.7 LIMITE DE GARANTIE

Cf 9.1 « Tarifs ».

9.8 LIMITE DE RESPONSABILITE

Sous réserve des dispositions d'ordre public applicables, l'AC « ALMERYS CUSTOMER SERVICES CA NB» d'Almerys ne pourra pas être tenue responsable d'une utilisation non autorisée ou non conforme des Certificats, des données d'activation, des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.
L'AC « ALMERYS CUSTOMER SERVICES CA NB» d'Almerys décline en particulier sa responsabilité pour tout dommage résultant :

- d'un emploi des Bi-clés pour un usage autre que ceux prévus avec le Client ;
- de l'usage de Certificats expirés ;
- d'un cas de force majeure tel que défini par l'article 1218 du Code civil

L'AC « ALMERYS CUSTOMER SERVICES CA NB» d'Almerys décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les Certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.

En aucun cas, l'AC « ALMERYS CUSTOMER SERVICES CA NB» n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre les Clients et les Porteurs, notamment quant au contenu des documents soumis à signature cachet via le Service de signature électronique, ou le service d'horodatage d'Almerys.

Pour la tarification Cf 9.1 « Tarifs ».

9.9 INDEMNITES

Cf 9.1 « Tarifs ».

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1. Durée de validité

La PC de l'AC « **Almerys Customer Services CA NB**» reste en application au moins jusqu'à la fin de vie du dernier Certificat émis au titre de cette PC.

9.10.2. Fin anticipée de validité

La publication d'une nouvelle version de la PC de l'AC Racine Almerys peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.

Suite à publication interne au sein de l'IGC d'une nouvelle version de la PC de l'AC Racine Almerys ou de la présente PC, l'AC « **Almerys Customer Services CA NB**» dispose d'un délai de 1 an pour se mettre en conformité.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des Certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

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

Suite à l'arrêt de l'AC « **Almerys Customer Services CA NB** » et donc à la fin de validité de cette politique, étant donné que le dernier Certificat aura été émis avec une date de fin de validité T_{FIN_VAL}, les exigences des sections suivantes :

- 2 « RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES »
- 3.4 « Identification et validation d'une demande de révocation »
- 4.5 « Usages de la bi-clé et du certificat »
- 4.8 « Modification du certificat »
- 4.9 « Révocation et suspension des certificats »
- 4.10 « Fonction d'information sur l'état des certificats »

doivent rester applicables pendant cette même durée T_{FIN_VAL}.

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AG devra au plus tard un mois avant le début de l'opération, faire valider ce changement, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC « **Almerys Customer Services CA NB**» et de ses différentes composantes.

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.Circonstances selon lesquelles l'OID doit être changé

L'OID du type de Certificat émis par l'AC « **Almerys Customer Services CA NB**» étant inscrit dans les Certificats qu'elle émet, toute évolution de la PC ayant un impact majeur sur les Certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des Clients, qui ne peuvent donc pas s'appliquer aux Certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les Applications utilisatrices puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Pour toute demande d'information ou réclamation relative au service Certificats de signature cachet, il convient de contacter le service Autorité de Certification par mail à l'adresse suivante :
gouvernance.igc@almerys.com.

En cas de litige sur l'interprétation du contenu ou l'exécution de la présente PC, une résolution amiable des conflits est privilégiée.

9.14 JURIDICTIONS COMPETENTES

Le droit applicable à tout litige relatif à l'interprétation et l'exécution de la présente PC est le droit français.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués en Annexe 1. Almerys se conforme à la législation et aux réglementations en vigueur et conserve les éléments de preuve de cette conformité. En particulier, chaque fois que cela est possible, Almerys

- met en place des moyens pour faciliter l'accès de ses services aux personnes en situation de handicap.
- Almerys traite les données personnelles en conformité avec la Réglementation en vigueur

10. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 REGLEMENTATION

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
[RGPD]	règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[LCEN]	Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés
[SIG_LOI]	Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
[SIG_DEC]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique

10.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS_A_3]	RGS - Fonction de sécurité « Signature électronique » - Version 2.3
[RGS_A_13]	RGS - Politiques de Certification Types - Variables de Temps - Version 2.3
[RGS_A_14]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3
[ETSI_NQCP]	ETSI TS 102 042 V2.1.1 (2009-05) Policy Requirements for Certification Authorities issuing public key certificates
[ETSI_319401]	General Policy Requirements forTrust Service Providers
[ETSI_319411-1]	Policy and security requirements for Trust Service Providers issuing certificates;
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - 11/2003
[PROG_ACCRED]	COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance
[CC]	Norme ISO/IEC 15408 : Critères communs version 2.1
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Recommendation X.509, version 3
[PC²]	Procédures et politiques de certification de clés, CISSI, version 2.2 de Janvier 2001.

Renvoi	Document
[RFC822]	Standard for the format of Arpa internet text messages, August 13, 1982, Revised by David H. Crocker
[RFC5280]	Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280 May 2008
[ROLES_IGC]	Rôles des exploitants d'une infrastructure de gestion de clés, CISSI, version 1.2 de janvier 2001
[DCSSI_ALGO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.0 du 3 mai 2004 N°1064 SGDN/DCSSI/SDS/AsTeC du 3 mai 2004
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)
[CWA14167-4]	CWA 14167-4 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSO-PP)
[CWA14169]	CWA 14169 (2003-08) Secure Signature Creation Device, version « EAL 4 +»