Déclaration des Pratiques de Certification AC Almerys

P
Procédure

Audit	Sous-Référentiel :	Référence :	Statut :
Sécurité	PKI Almerys	PPKIG046 1.3.6.1.4.1.48620.41.33	En cours de validation
validé par :	**Fonction :**	**Date :**	**Signature :**
KPA	Responsable Juridique	26/04/2018	
Approuvé par :	**Fonction :**	**Date• :**	**Signature :**
MMI	Autorité de Gouvernance	26/04/2018	
Diffusion auprès de :	Gouvernance PKI		
En accès pour :	ComEx		
Localisation :			

Sommaire

Date de péremption		Responsable de l'actualisation	
Version	**Date**	**Modifications**	**Auteur**
v1.6	27/06/2017	Modifications conformité eIDAS	JGO, MMI
v1.7	06/08/2017	Modifications conformité eIDAS	MMI
V1.8	19/11/2017	Modification pour prise en compte les MC	MMI
V1.9	26/04/2018	Modification suite audit	MMI

• Date d'entrée en vigueur

Documents de référence

Référence	Version	Titre du document
	V1.1	Politique de certification de l'AC almerys signature and authentication ca nc

Sommaire détaillé

1. INTRODUCTION

1.1 PRESENTATION GENERALE

Almerys s'est positionnée comme prestataire de service de certification électronique à destination de ses clients et partenaires, en offrant des services supports à la confiance numérique, de manière à leur permettre généralement de sécuriser l'ensemble de leurs échanges.

La présente Déclaration des Pratiques de Certification définit la mise en œuvre des engagements que prend almerys dans ses Politiques de Certification pour la fonction de délivrance de certificat.

Ce document a été établi en vue d'une certification selon le référentiel européen :

- ETSI 101456,
- ETSI TS 102 042,
- ETSI EN 319411-2
- ETSI EN 319411-1

Afin de distinguer clairement les exigences spécifiques à un certain type de certificat, ce type d'exigences sera spécifiquement précisé dans un cartouche identifiant le type d'exigence auxquelles le certificat est applicable.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques

Certificats de cachet pour les organisations et d'unité d'horodatage

Certificats de signature déportée

1.2 IDENTIFICATION DU DOCUMENT

La présente DPC est dénommée « Déclaration des Pratiques de Certification de l'Autorité de Certification pour la fonction de signature et d'authentification de personne physique, signature cachet, et signature cachet d'horodatage. Elle correspond aux Politiques de Certification dont l'OID est :

- 1.3.6.1.4.1.48620.41.1.7.3.1. (PC ALMERYS SIGNATURE AND AUTHENTICATION CA NC)
- 1.3.6.1.4.1.48620.41.1.5.2.1 (PC ALMERYS CUSTOMER SERVICES CA NB)
- 1.3.6.1.4.1.48620.41.1.4.2.1. (PC ALMERYS USER SIGNING CA NB)

La référence interne Almerys de ce document est : PPKIG046.
L'identifiant d'objet (OID) est : 1.3.6.1.4.1.48620.41.2.7.3.1

Le préfix d'OID de ce document répond aux principes de nommage suivant :

- (iso)1.member-body(3).almerys(6.1.4.1.48620).igc(41).dpc(2).signandauth(7).nc(3).v(1)

1.3 ENTITES INTERVENANT DANS L'IGC

Pour avoir le détail, par entité, voir les documents politiques de certifications.

1.3.1. Rôle et obligation de l'Autorité d'Enregistrement Déléguée

L'Autorité d'Enregistrement Déléguée a pour fonction de gérer les relations entre l'Autorité de Certification et les Porteurs de Certificat notamment en matière de délivrance des Certificats conformément aux Procédures d'AED.

L'Autorité d'Enregistrement Déléguée s'engage :

- A procéder aux vérifications de l'identité du porteur de certificat, et de son rattachement à la structure juridique pour les certificats entreprise, cela sur la base des documents originaux collectés et la conformité des informations qu'ils contiennent par rapport aux copies fournies ;
- A constituer le dossier de demande de Certificat et éventuellement à faire signer le formulaire, et CGU si applicable;
- A appliquer les procédures de sécurité appropriées dans le cadre de la génération du Dispositif de création de signature électronique (dans le cas des certificats sur support QSCD) afin de garantir l'intégrité du support avant sa remise au Porteur de Certificat ;
- A émettre des avis de délivrance des Dispositifs sécurisés de création de signature par courrier électronique et/ou SMS ;
- A mettre en place les moyens permettant de garantir une acceptation explicite du Certificat et du Dispositif sécurisé de création de signature lors de sa délivrance au Porteur de Certificat et que seul celui-ci puisse prendre connaissance du code d'activation;
- A conserver, ou à envoyer à ALMERYS, à des fins d'archivage, les pièces des dossiers d'enregistrement et toute information relative aux Certificats électroniques délivrés qui pourrait s'avérer nécessaires pour faire la preuve en justice de la certification électronique. Les pièces du dossier d'enregistrement seront conservées pendant au moins sept ans par l'AC ;
- A conserver et à protéger en confidentialité et en intégrité les données confidentielles et les données à caractère personnel du Porteur de Certificat qui lui sont confiées, y compris lors des échanges de ces données avec les autres fonctions de l'IGC et de façon générale à respecter la réglementation relative aux données à caractère personnel ;
- A révoquer sans délai le Certificat du Porteur en cas de perte de sa qualité de représentant de l'entreprise.

L'ensemble de ses obligations est également valable en cas de renouvellement (avec nouvelle génération de bi clé de signature ou d'authentification) du Certificat de Porteur.

L'Autorité d'Enregistrement Déléguée doit prendre toutes les mesures raisonnables pour s'assurer que les Porteurs de Certificats 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.

L'Autorité d'Enregistrement Déléguée s'engage également au maintien opérationnel des moyens qui sont mis à sa disposition pour transmettre les demandes de Certificats, et au respect des règles communes d'authentification et de contrôle des flux établies entre elle et l'Autorité de Certification.

L'AED s'engage à assurer, au titre d'une obligation de résultat, la disponibilité du service dans les conditions prévues par l'Annexe Plan Qualité de Services.

L'Autorité d'Enregistrement Déléguée s'engage à veiller au respect le plus strict de la Politique de Certification de l'Autorité de Certification et à la prise de connaissance des Conditions générales d'utilisation par les Porteurs de Certificat.

L'Autorité d'Enregistrement Déléguée s'engage à employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires permettant l'exécution de l'objet du Contrat et conformément aux procédures décrites dans la Déclaration des Pratiques de Certification figurant en Annexe.

A ce titre, l'Autorité d'Enregistrement Déléguée s'engage à désigner les personnes physiques jouant le rôle d'opérateur d'AED et à informer l'Autorité de Certification en cas de modification des opérateurs.

L'Autorité d'Enregistrement Déléguée s'engage à se soumettre à toute action de contrôle, par un membre de l'Autorité de Certification dûment mandaté, de l'ensemble des pièces d'un ou plusieurs dossiers de demande de Certificat ainsi qu'à tout audit de contrôle mis en place par l'Autorité de Certification conformément.

1.3.2. Rôle et obligation du Mandataire de Certification

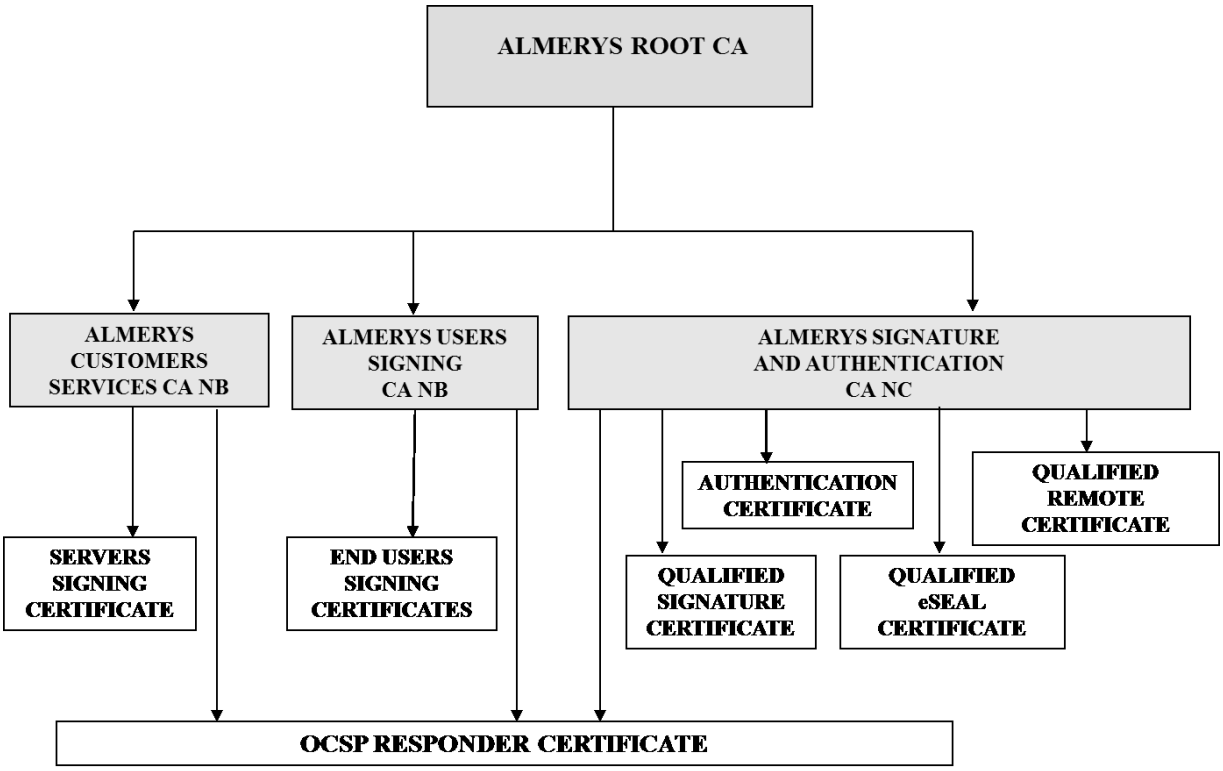
Le rôle du MC consiste à effectuer certaines taches de l'AE, en particulier :

- A réceptionner les formulaires de demande et à collecter la copie des documents permettant de s'assurer de l'identification du futur Porteur de Certificat ;
- A vérifier en face à face les informations d'identification du futur Porteur de Certificat, les originaux des documents collectés et la conformité des informations qu'ils contiennent par rapport aux copies fournies ;
- A constituer le dossier de demande de Certificat et à faire signer le formulaire de demande de Certificat par le futur Porteur de Certificat;
- A informer le futur Porteur de Certificat de ses obligations contractuelles et à faire signer les Conditions Générales d'Utilisation du Certificat;
- A transmettre le dossier de demande de Certificat à l'Autorité d'enregistrement ;
- A mettre en place les moyens permettant de garantir la remise et l'acceptation explicite du Certificat et du Dispositif sécurisé de création de signature lors de sa délivrance au Porteur de Certificat et que seul celui-ci puisse prendre connaissance du code d'activation de la clé privée ;
- A transmettre à l'AE à des fins d'archivage, les dossiers d'enregistrement et toute information relative aux Certificats électroniques délivrés qui pourrait s'avérer nécessaires pour faire la preuve en justice de la certification électronique;
- A demander la révocation sans délai du Certificat du Porteur en cas de perte de sa qualité de représentant de l'entreprise.

1.4 USAGE DES CERTIFICATS

1.4.1. Domaines d'utilisation applicables

La chaine de certification des ACs almerys est décrite dans la figure ci-dessous :



Cette chaine est composée de deux niveaux de certificats d'AC:

- AC RACINE : ALMERYS ROOT CA
- ACs subordonnées : AC ALMERYS CUSTOMERS SERVICES CA NB, AC ALMERYS USERS SIGNING CA NB, AC ALMERYS SIGNATURE AND AUTHENTICATION CA NC, le terme AC dans ce document sera utilisé pour désigner une AC subordonnée.

Les certificats utilisateurs finaux de chaque AC sont décrits dans le paragraphe Ci-dessous.

-

1.4.1.1. Bi-clés et Certificats des Clients

Les certificats émis par l'AC ALMERYS SIGNATURE AND AUTHENTICATION CA NC sont :

- des certificats qualifiés de signature électronique conformes à la directive européenne 1999/93/EC, ou
- des certificats d'authentification certifiés ETSI 102042 NCP+, ou
- des certificats qualifiés de signature électronique conforme au Règlement eIDAS et à la norme ETSI EN 319 411-2 QCP-n-qscd, et permettant de créer des signatures qualifiées ou
- des certificats d'authentification certifiés ETSI EN 319 411-1 NCP+, ou
- des certificats qualifié de cachet électronique, conforme au Règlement eIDAS et à la norme norme ETSI EN 319 411-2 QCP-l, ou
- des certificats d'unité d'horodatage, conforme à la norme EN 319 411-2 QCP-l et pouvant être utilisée par des services d'horodatage qualifiés
- des certificats de signature conforme à la norme EN 319 411-2 QCP-n, utilisé par Service de signature électronique Almerys, grâce auquel l'Utilisateur peut signer les formulaires ou documents présentés par le Client, générant ainsi une signature avancée fondée sur un certificat qualifé

Les certificats émis par l'AC ALMERYS CUSTOMER SERVICES CA NB sont :

- des certificats de signature cachet ETSI 102042 LCP
- des certificats cachet d'horodatage ETSI 102042 LCP
- des certificats de signature cachet ETSI EN 319411-1 LCP
- des certificats cachet d'horodatage ETSI EN 319411-1 LCP

Les certificats émis par l'AC ALMERYS USER SIGNING CA NB sont
- des certificats signature personne physique ETSI 102042 LCP
- des certificats signature personne physique ETSI EN 319411 LCP,

Les certificats concernés sont utilisables dans les applications de dématérialisation sous la responsabilité du Client ou sous la responsabilité d'Almerys.

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

Les Bi-clés et Certificats des ACs ne peuvent être utilisés que pour la signature de Certificats finaux, de Certificats de cachet et d'unité d'horodatage, de certificats de répondeurs OCSP et de LCR.

1.4.2. Domaines d'utilisation interdits

voir PC§1.4.2

1.5 GESTION DE LA DPC

1.5.1. Entité gérant la DPC

L'entité en charge de l'administration et de la gestion de la DPC est l'Autorité de Gouvernance (AG) de l'AC. L'AG est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente DPC.
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 Politique de Certification et à la DPC.

1.5.2. Point de contact

Voir PC§1.5.2

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

Afin de déterminer la conformité de la présente DPC avec les PCs, l'AG s'appuie sur les ressources internes ou externes d'Almerys spécialisées dans l'audit et l'évaluation de la sécurité des services et des produits.

Pour les exigences portant sur une AE déléguée « Client Almerys », l'AG est en charge de commanditer un audit annuel pour mesurer cette conformité.

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

L'audit des modifications de la PC et de la DPC peut être encadré par l'établissement formel d'un audit de la politique de certification sur le périmètre de modification.

L'approbation de la conformité de la DPC à la Politique de certification est prononcée par l'AG sur la base du rapport d'audit présenté par l'auditeur, et la validation du responsable juridique, et du responsable de sécurité confiance numérique.

.

1.6 DEFINITION ET ACRONYMES

Les acronymes utilisés dans la présente DPC sont les suivants :

1.6.1. Abréviations

Voir PC§1.6.1

1.6.2. Définitions

Voir PC§1.6.2

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

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

L'entité en charge de la publication des informations de l'AC est l'Autorité de Certification d'Almerys :

- L'équipe sécurité de l'IGC fournit les documents applicables : la PC, la DPC, les Conditions Générales d'Utilisation, les certificats d'AC ;
- L'équipe sécurité de l'IGC est chargé de la mise en œuvre de la fonction d'information sur l'état des certificats, c'est-à-dire de la mise à jour régulière de la LCR de l'AC ;
- L'équipe sécurité de l'IGC publie les pages d'information et les documents sur le site pki.almerys.com.

2.2 INFORMATION DEVANT ETRE PUBLIEES

Conformément à la Politique de certification, les informations publiées par l'AC sont les suivantes :

- les Politiques de certifications des ACs;
- les Conditions Générales d'Utilisation ;
- les certificats en cours de validité des AC de la hiérarchie de rattachement de l'AC.
- la liste des certificats révoqués (LCR) des ACs et de l'AC racine.
- la présente DPC

La page web de présentation PKI disponible à l'URL pki.almerys.com permet d'accéder aux différentes informations devant être publiées

L'information du statut de révocation au-delà de la durée de validité des certificats est publiée dans la LCR, les numéros de séries des certificats révoqués ne sont jamais supprimés de la LCR.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les délais et fréquences sont établis selon le type d'information à publier :

- Les politiques de certification sont publiées dès validation, dans un délai maximal de 72 heures ouvrées.
    - Dans tous les cas, les PC sont publiées avant toute émission d'un certificat correspondant à cette PC.
- Les certificast d'ACs sont diffusés dans un délai maximum de 72 heures ouvrées à l'issue de la génération.
- En cas de révocation d'un certificat final, la CRL est régénérée par l'AC émettrice. En l'absence de révocation pendant une période de 24 heures, la CRL est mise à jour automatiquement
    - une fois la CRL mise à jour par l'AC, elle est mise à disposition du service de publication dans un délai de 30 minutes Maximum,
    - une fois la CRL à disposition du service de publication, la LCR est publiée dans un délai maximum de 30 minutes.

Le service de certification électronique d'Almerys est accessible 24h/24 et 7j/7.

almerys a mis en œuvre un Plan de Reprise et de continuité d'Activité. Ce PRA/PCA inclut une gestion de la publication voire de la régénération de la CRL en cas de dysfonctionnement.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

Les informations publiées sont mises à disposition en lecture à l'ensemble de la communauté des applications utilisatrices. Les PC, DPC, CGU, certificats d'AC et LCR sont donc mis à disposition en lecture pour tous.

Les ajouts, suppressions et modifications sont limités aux personnes autorisées d'Almerys.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1. Types de noms

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

Chaque entité a un nom distinctif (DN) X.500, porté dans le champ Subject du certificat, non seulement facile à distinguer des autres noms, mais aussi unique pour l'AC considérée.
Il est codé sous la forme d'une chaîne imprimable, en printable-string ou Utf8string pour les caractères spécifiques à la langue française et n'est pas vide.

3.1.2. Nécessité d'utilisation de noms explicites

En plus des règles précisées dans la PC§3.1.2, la DPC précise les éléments suivants :

- La raison sociale d'Almerys, tel que figurant au KBis pour le certificat de l'AC (Almerys) et la raison sociale de l'entité du porteur pour les certificats finaux (attribut OrganizationName) ;
- Le code SIREN d'Almerys pour le certificat d'AC, et le code SIREN du Client pour les certificats finaux (attribut OrganizationalUnit);

Le certificat des ACs sont identifiés comme suit :

- CN = Nom de l'AC
- OU = 0002 432701639
- O = Almerys
- C = FR

3.1.3. Anonymisation ou pseudonymisation des porteurs

Les certificats objets de la présente DPC ne peuvent en aucun cas être anonymes.
Les noms fournis pour l'établissement d'un certificat ne peuvent en aucun cas être des pseudonymes.

3.1.4. Règles d'interprétation des différentes formes de noms

Voir PC§7.
Les noms utilisés pour les certificats des AC d'Almerys sont suffisamment explicites et ne nécessitent pas d'interprétation particulière.

3.1.5. Unicité des noms

L'AC résoudra les problèmes d'homonymie éventuelle et garantit l'unicité des noms utilisés pour les certificats des AC qu'elle gère. En plus des exigences prévues dans la PC§3.1.5, Almerys applique les pratiques suivantes :

La clé d'unicité appliquée pour les certificats porteurs personnes physiques est la suivante :

- Champ CN du certificat, qui comprend les noms, prénom, et le champ SerialNumber un identifiant unique,

Un identifiant unique est utilisé pour référencé le porteur dans le référentiel Almerys,.

De plus tous les certificats émis par les ACs comportent un numéro de série unique qui garantit que chaque certificat est techniquement unique au sein de la PKI.

3.1.6. Identification, authentification et rôle des marques déposées

Les certificats porteurs contiennent des informations propres à leur entité de rattachement (Raison social, …). L'AE s'assurera avec un soin raisonnable de l'identification des marques déposées en validant que la raison sociale présentée est bien celle du porteur.

3.2 VALIDATION INITIALE DE L'IDENTITE

L'autorité d'enregistrement doit être de confiance et authentifiée par l'AC, en particulier, Almerys s'assure que les autorités d'enregistrement mettent en place les mesures de sécurité nécessaires.

3.2.1. Méthode pour prouver la possession de la clé privée

Sans objet, Les clés privées de signature et d'authentification sont générés onboard dans le dispositif de création de signature par l'AE ou dans le service de stockage sécurisé.
Voir PC.

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

Le dossier de demande d'un certificat peut être saisi soit :

- Par le Porteur via un formulaire en ligne sur le portail de service Almerys ;
- Par l'Autorité d'Enregistrement (ou l'Autorité d'Enregistrement Déléguée), ou par le Mandataire de Certification, au guichet d'un des établissements du Client, en présence du Porteur. Dans ce cadre les informations du Porteur peuvent être :
    - saisies entièrement par l'Autorité d'Enregistrement
    - pré-remplie sur la base des informations contenues dans une base de données du Client, si le Porteur est déjà connue du Client, ou Almerys.
- Par l'importation des données par l'AE à partir de sa base d'information fiable comprenant les justificatifs d'identité

Dans tous les cas la saisie ne peut être validée que par l'Autorité d'Enregistrement et après vérification des pièces justificatives.

Les seules informations utilisées pour la génération du certificat sont celles contenues dans le formulaire de demande de certificat, une fois que ce dernier a été validé.

La validation de l'identité du demandeur d'un certificat se fait nécessairement en face à face entre le Porteur et l'Autorité d'Enregistrement pour les certificats qualifiés.

3.2.3.1. Enregistrement d'un Porteur « particulier »

Les informations nécessaires pour procéder à une demande de certificat de ce type sont définies dans la PC.
Le nom et prénom du porteur sont ceux inscrits dans le justificatif d'identité.

Almerys met en place des processus de validation conforme à la Réglementation en matière de traitement des données personnelles et ne conserve que les éléments de preuve strictement nécessaire à la vérification de l'identité du porteur.

3.2.3.2. Enregistrement d'un Porteur « entreprise »

Les informations nécessaires pour un porteur entreprise sont définies dans la PC.

3.2.3.3. Enregistrement d'un Porteur « Cachet serveur Client »

Voir PC & 3.2.3. pour la liste des documents devant être fournis et complétés.

L'AE demande une preuve de l'habilitation du RC à demander un certificat pour l'entité morale qu'il représente.
L'opérateur de l'AE vérifie le contenu des formulaires et des pièces justificatives. En particulier, il vérifie :

- la bonne correspondance entre n° SIREN et raison sociale du Client,
- Les informations du profil de certificat, contenues dans la demande de certificat, sont vérifiées avec le responsable de l'équipe chargée du déploiement du Service, pour s'assurer de leur intégrité par rapport aux contraintes éventuelles du Service,
- L'identité du RC est vérifiée avec le responsable du service client Almerys qui est chargé du suivi du Client dans le cadre du déploiement du Service.

3.2.3.4. Mandataire de Certification

3.2.3.4.1. Enregistrement d'un Mandataire de Certification.

Voir PC.
L'AE vérifie le contenu des formulaires et des pièces justificatives. En particulier, elle vérifie :

- L'identité du mandataire de certification, son entité de rattachement, et l'identité du représentant légal.

3.2.3.4.2. Enregistrement d'un porteur via un Mandataire de Certification

Voir PC.

3.2.4. Informations non vérifiées du porteur

Sans objet dans le cadre de la présente DPC.

3.2.5. Validation de l'autorité du demandeur

L'AE vérifie que le porteur particulier ou entreprise fait bien partie de ses clients, et que :

- pour un porteur « particulier », que le demandeur est bien le futur porteur via son justificatif d'identité,
- pour un porteur « entreprise », que la personne est mandatée par celle-ci via la demande co-signée par le représentant légal

3.2.6. Critères d'interopérabilité

Les ACs n'ont aucun accord de reconnaissance avec une AC extérieure au domaine de sécurité auquel elle appartient.
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 DE CLES

3.3.1. Identification et validation pour un renouvellement courant

Voir PC§3.3.1

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

Voir PC§3.3.2

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

3.4.1. Demande faite par le Porteur, ou le demandeur du certificat

Voir PC

3.4.2. Demande faite par l'Autorité d'Enregistrement

Si l'Autorité d'Enregistrement doit traiter la demande de révocation elle peut soit :

- Identifier le Porteur sur la base des informations personnelles du Porteur contenues dans son dossier;
- Révoquer de son propre chef le certificat concerné sans avoir procéder à l'identification du Porteur.

Dans tous les cas, le processus de révocation du certificat consiste à :

- Se connecter sur les interfaces de gestion
- Révoquer le ou des certificats.

3.4.3. Demande faite par le centre de support

Si le centre de support doit traiter la demande de révocation il peut soit :

- Identifier le Porteur sur la base des informations personnelles du Porteur contenues dans son dossier ;
- Transmettre la demande de révocation à l'Autorité d'Enregistrement correspondante (voir 3.4.2).

Si le centre de support peut traiter la demande de révocation, les opérations consistent à :

- Se connecter sur les interfaces de gestion
- Révoquer le ou les certificats.

3.4.4. Demande faîte par le responsable du Service

Voir PC

3.4.5. Demande faite par l'AC ou l'AG

En cas d'urgence, l'Autorité de Certification ou l'Autorité de Gouvernance peut procéder à la révocation d'un support.
Dans ce cas, les personnes habilitées :

- Se connectent sur les interfaces de l'IGC ;
- Recherchent le certificat concerné ;
- Procèdent à la révocation de ce dernier.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1. Origine d'une demande de certificat

En plus des exigences de la PC§4.1.1, la pratique suivante est définie.
La demande de certificat peut être effectuée :

- Lors de la demande de souscription par le porteur, ou son AE à un service Almerys ou partenaire Almerys, via le portail du service,
- Par courrier
- Lors du face à face avec l'AE

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

Voir PC.

Pour les certificats cachet serveur :
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).
Il est de la responsabilité du RC de communiquer les informations suivantes dans le formulaire :

- coordonnées du RC comprenant ses prénom et nom, sa fonction, ses coordonnées mail et téléphoniques, son adresse professionnelle ;
- Nom du Client / raison sociale ;
- Identifiant SIREN ;
- Nom du service pour lequel le certificat Client va être mis en œuvre ;
- en option, informations complémentaires de description de l'entité cliente ou du Service (ces informations seront inscrites dans des attributs OU du champ sujet du certificat Client).

L'AE est responsable de la vérification de ces informations.

Le dossier de demande de certificat doit être envoyé par courrier à l'AE dont les coordonnées figurent dans les CGU et la PC.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

L'enregistrement et la validation de la demande de certificat s'effectue par l'AE, l'AE se connecte sur l'outil d'enrôlement, saisie, et valide les informations, et effectue la demande de certificat auprès de l'AC..

4.2.2. Acceptation ou rejet de la demande

Voir PC

4.2.3. Durée d'établissement du certificat

Voir PC.

4.3 DELIVRANCE DU CERTIFICAT

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

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
La procédure de personnalisation des certificats sur le support par l'AE est décrite dans la documentation interne de l'IGC, elle consiste a : - La génération d'es bi-clés dans le QSCD du porteur, - La génération du certificat par l'AC - L'envoie du code d'activation du QSCD par SMS au porteur Dans tous les cas le Porteur peut modifier le code d'activation lors de la première utilisation.

Certificats de signature déportée
La procédure de personnalisation des certificats sur le support est décrite dans la documentation interne de l'IGC, elle consiste a : - La génération d'es bi-clés du porteur dans les HSMs cryptographique, - La génération du certificat par l'AC, - L'envoie du code d'activation par SMS au porteur,

Certificats de cachet pour les organisations et d'unité d'horodatage
Le déroulement organisationnel et technique de la KC Client est décrit dans la documentation interne de l'IGC. Les opérations suivantes sont réalisées lors de la KC Client : ➔ Création d'un container Client sur le HSM signature ; ➔ Génération des clés du Client dans le container Client ; ➔ Création d'une requête de certificat au format PKCS#10 ; ➔ Transmission de la demande de certificat à l'AC; ➔ Génération par l'AC du certificat Client conformément à la demande de certificat Client validée par l'AE ; ➔ Vérification formelle du contenu du certificat Client avec le RC, ou de l'huissier; ➔ Installation du certificat dans le container Client ➔ Vérification du bon fonctionnement de signature par le certificat Client ; ➔ Sécurisation et remise des secrets et éléments sensibles aux Détenteurs de secret Almerys (pour les secrets de HSM) et Client (pour la partition et la Bi-clé de signature du Client).

Le bon déroulement de la KC est validé par le RC, ou de l'huissier qui appose sa signature, dans le script de déroulement de la KC.

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

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
L'Autorité d'Enregistrement remet lors du face à face le support cryptographique au Porteur.

Certificats de signature déportée
le porteur est notifié par l'application d'enrôlement par la remise de son moyen d'authentification

Certificats de cachet pour les organisations et d'unité d'horodatage
L'AC renvoie au Client du Service un statut sur l'opération de génération du Bi-clé et du Certificat Client : L'AC remet au Client en mains propres, ou en recommandé avec AR un fac-similé du script de déroulement de la KC;

4.4 ACCEPTATION DU CERTIFICAT

4.4.1. Démarche d'acceptation du certificat

Voir PC

4.4.2. Publication du certificat

Les certificats émis par les ACs ne sont pas publiés.

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

Voir PC

4.5 USAGE DU BI-CLE ET DU CERTIFICAT

4.5.1. Utilisation de la clé privée et du certificat

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Voir PC

Certificats de signature déportée

Les clés privées des porteurs sont protégées dans un HSM cryptographique certifiée FIPS 140 Level 3 ou Critères Communs EAL4+.
Le HSM est accessible depuis les serveurs de signature autorisés via un lien sécurisée.

Le service de gestion sécurisé des clés autorise l'utilisation d'une clé de porteur sous réserve que ce dernier ait été préalablement authentifié par l'application de signature

Ainsi, seul le porteur peut utiliser sa clé privée et son certificat, ceux-ci n'étant jamais exposés directement mais cloisonnés aux cas d'usages de signature initié par les applications autorisées.

Certificats de cachet pour les organisations et d'unité d'horodatage

4.5.1.1. Certificat de Cachet

La clé privée du Client est protégée dans un HSM certifié FIPS 140 LEVEL 3, ou critères Communs EAL4+. Le HSM est accessible depuis les serveurs d'applications autorisés via un lien sécurisée. L'application possède une configuration lui indiquant quel container utiliser pour les demandes de signatures cachet du Client qu'elle envoie au HSM.

4.5.1.2. Certificat d'unité d'horodatage

La clé privée de chaque unité d'horodatage est protégée dans une partition du HSM certifiée FIPS 140 LEVEL 3. Le HSM est accessible depuis les serveurs d'horodatage autorisés via un canal de communication sécurisé.

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

Voir PC.

La présente DPC précise également que toute application utilisatrice d'un certificat émis par l'AC s'engage à vérifier :

- L'ensemble de la chaîne de certification permettant l'émission du certificat;
- Les dates de validité du certificat ;
- Les usages prévus par le certificat.

Ces contraintes sont rappelées dans les CGU des certificats.

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

Voir Politique de Certification.

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

Voir Politique de Certification.

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

Voir Politique de Certification.

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 DPC.

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

4.7.1. Causes possibles de changement de bi-clé

Les causes de changement de bi-clés sont décrites dans la PC.

4.7.2. Origine d'une demande de nouveau certificat

La demande d'un nouveau certificat suit le même processus qu'une demande initiale.
Cf section 4.1.1 « Origine d'une demande de certificat ».
.

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

Cf chapitre 4.2.

L'identification et la validation d'une demande de fourniture d'un nouveau Certificat sont précisées au &3.3.

Pour les actions de l'AC, cf. & 4.3.

Certificats de cachet pour les organisations et d'unité d'horodatage
Il faut cependant adjoindre aux actions décrites en Section 4.3, un traitement complémentaire : Lors de KC Client, le Bi-clé précédent du Client doit être supprimé.

4.7.4. Notification de l'établissement du nouveau certificat

Cf. section 4.3.2.

Certificats de cachet pour les organisations et d'unité d'horodatage
L'exigence supplémentaire suivante est applicable : Lors de l'envoi au RC de la requête de certificat et du certificat Client, le mail précise qu'il s'agit de la

délivrance d'un nouveau certificat.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. section 4.4.1.

4.7.6. Publication du nouveau certificat

Cf. section 4.4.2.

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

Cf. section 4.4.3.

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 DPC.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificat de porteurs

Voir la PC.

4.9.1.2. Certificat d'une composante de l'AC

Voir la PC.

4.9.2. Origine d'une demande de révocation

4.9.2.1. Cas du certificat d'un porteur

Voir la PC.

4.9.2.2. Cas du certificat d'une des composantes de l'AC

Voir la PC.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat porteur

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre 3.4.
La procédure de révocation de certificats d'un porteur est décrite dans la documentation interne de l'IGC.
Les demandes de révocation émanant des Clients peuvent être réalisées :

- par mail à l'adresse mail de contact présentée dans les CGU, la demande dûment complétée est en pièce jointe du mail ;
- Par téléphone à l'AE, ou au support;
- par courrier postale,

Dans tous les cas, la validation de la demande est effectuée par l'AE ou l'AED, ou le MC, ou le support.
Une fois la demande authentifiée et contrôlée, l'AC révoque le Certificat correspondant en changeant son statut, publie une CRL, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

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

La révocation d'une composante de l'AC est opérée par l'AG de la PKI Almerys.
En cas de révocation du certificat de l'AC, une information claire sera établie sur le site internet de la PKI Almerys : http://pki.almerys.com.
Après la décision prise par l'AG Almerys de révoquer le certificat, deux officier PKI procèdent à la révocation du certificat de l'AC et à la signature d'une LAR à jour.
Cette nouvelle LAR, une fois mise en ligne par l'AC, permettra aux applications utilisatrices de s'informer de la révocation effective du certificat de l'AC.

La révocation d'un certificat de l'AC fera alors l'objet d'un PV de révocation qui sera mis au coffre avec les autres éléments de l'AC.

4.9.4. Délai accordé pour formuler la demande de révocation

Voir la PC.

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

4.9.5.1. Révocation d'un certificat de porteur

Voir la PC.

4.9.5.2. Révocation d'un certificat d'une composante de la PKI

Voir la PC.

L'AC fera son meilleur effort pour réaliser l'ensemble des étapes nécessaires à la validation d'une révocation d'un certificat d'AC.

Le nombre minimum de porteurs de secrets est réuni au plus vite pour pouvoir procéder aux opérations techniques de révocation.

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

Les utilisateurs des certificats délivrés par l'AC doivent vérifier l'état des certificats de l'Autorité de Certification et de la chaîne de certification.
La méthode utilisée est à l'appréciation de l'application utilisatrice selon la disponibilité et les contraintes liées à son application.
Par défaut, la liste des autorités révoquées est mise à disposition sous la forme d'un fichier « CRL » par l'AC.
Les adresses de publication sont définies dans le paragraphe 2.2.

4.9.7. Fréquence d'établissement des LAR et 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.
Si une demande de révocation est validée, une nouvelle CRL doit être générée dans les 60 mn au maximum.

Concernant les LARs émises par l'AC Racine, elles sont générées

- au moins une fois tous les six (6) mois au minimum 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 est publiée dès sa génération et dans un délai maximum de 30 minutes.

La durée entre la fin de génération de la LAR et sa publication est inférieure à 32 heures.

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.
Les résultats retournés par l'OCSP et les LCR sont consistants modulo les délais de publication des LCRs.

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

4.9.12.1. Cas du certificat de l'AC

En cas de compromission de la clé privée d'une AC, la révocation du certificat correspondant devra être opérée. Dans ce cas, l'AC informera dans les plus brefs délais les AE concernées et fera procéder à la révocation de l'ensemble des certificats émis par l'AC dont le certificat est à révoquer.
Almerys publiera également sur son site internet une information claire concernant la révocation de ce certificat. Cette publication fera l'objet d'une validation par le service de communication d'Almerys.

4.9.12.2. Cas des certificats des porteurs

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Voir la PC.

Certificats de signature déportée
Voir la PC.

Certificats de cachet pour les organisations et d'unité d'horodatage
Pour les Certificats des Clients, l'AC ou les RC sont tenus de faire la demande de révocation dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée et dans un délai maximum de 24h.

4.9.13. Causes possibles d'une suspension

Sans objet pour la présente DPC.

4.9.14. Origine d'une demande de suspension

Sans objet pour la présente DPC.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet pour la présente DPC.

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

Sans objet pour la présente DPC.

4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.10.1. Caractéristiques opérationnelles

Voir la PC.
Les précisions supplémentaires suivantes sont apportées :

- Les LAR sont publiées au format v2, accessibles sur Internet sous forme d'une liste visible de manière internationale pour tous.
- La LAR est mise à jour et publiée au minimum tous les 6 mois.

- Les LCR sont publiées au format v2, accessibles sur Internet sous forme d'une liste visible de manière internationale pour tous.
- La LCR est mise à jour et publiée a minima toutes les 24 heures.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des Certificats est disponible 24h/24 7j/7.
Les mécanismes mis en œuvre pour assurer la disponibilité de la fonction sont décrits au chapitre Exploitation de la procédure de publication des informations PKI Almerys.

4.10.3. Dispositifs optionnels

Sans objet.

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

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Voir la PC.

Certificats de signature déportée
Voir la PC.

Certificats de cachet pour les organisations et d'unité d'horodatage
En cas de fin de relation contractuelle entre l'AC et le Client dans le cadre du Service, 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 DPC.

4.12.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet pour la présente DPC.

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

Sans objet pour la présente DPC.

5. MESURES DE SECURITE NON TECHNIQUES

Différents contrôles sont mis en place afin d'assurer un haut niveau de confiance dans le fonctionnement de l'AC.

5.1 MESURES DE SECURITE PHYSIQUE

Les mesures de sécurité physique concernent un site géographique, le site Almerys de Clermont-Ferrand qui héberge niveaux salles machines, bunkers, cages de faraday PKI Almerys. On retrouve dans ces bunkers, et cages de faraday le cœur de la PKI Almerys :

- le card management system d'Almerys qui a un rôle d'« AE technique » dans les processus de l'AC et qui traite les cycles de vie des cartes et de certificats envoyés par les Clients. Ce service est hébergé dans la salle machine.
- le Key Management Système de l'AC. Ce service est hébergé dans l'espace « bunker », et cages de faraday
- les HSM cryptographiques

Les accès physiques aux bâtiments et aux Zones Sensibles sont régis par la politique de sécurité.

Le site Almerys de Clermont-Ferrand fait l'objet d'une déclaration de conformité APSAD à la règle APSAD R81 (système de détection d'intrusion).

Les déclinaisons opérationnelles découlant de ces règles et des cahiers des charges PKI sont structurées suivant le schéma suivant :

- Principe de protection de l'emprise,
- Principe de protection du bâtiment,
- Principe de protection de la zone sensible,
- Modalité d'accès – contrôle d'accès,
- Principe de la protection incendie,
- Protection contre l'inondation,
- Alimentation électrique,
- Environnement climatique.

5.1.1. Situation géographique et construction des sites

Plusieurs cloisonnements de sécurité physique sont utilisés en fonction du type de composant de sécurité utilisé par l'AC. Tous ces cloisonnements sont protégés par des zones clairement segmentées :

- Cage de Faraday: ces zones hautement sécurisées sont utilisées pour utiliser le logiciel / matériel utilisé par les services composant, comme les services de génération de certificats et les services d'horodatage.
- Bunker: zones hautement sécurisées utilisées pour opérer les services RA et le répondeur OCSP,
- salle machine : utilisés pour exploiter un serveur de publication Web frontal.

Toutes ces zones sont équipées d'une protection de sécurité physique et logique qui évite l'accès illégitime, y compris les systèmes de détection d'intrusion internes et externes, le système de vidéosurveillance interne et externe, le système de contrôle d'accès avec dual contrôle.

5.1.2. Accès physique

L'accès physique est limité via la mise en œuvre des mécanismes pour contrôler l'accès d'une zone à l'autre ou d'accéder à des zones de sécurité sensible, telles les cages de Faraday et les bunkers, toutes les accès aux zones sécurisées sont monitorés, avec une mise sous des alarmes de sécurité, et nécessitant un passage obligatoire d'une zone à l'autre, et requérant des tokens d'authentification matériels avec trois facteurs, y compris des dispositifs biométriques.
Les zones hautement sécurisées sont protégées contre un accès non autorisé par au moins trois (3) périmètres de protections, permettant l'accès pour une seule personne à la fois et nécessitant un dual contrôle.
L'accès aux zones sécurisées est limité au personnel autorisé figurant sur une liste d'accès, qui fait l'objet d'une revue et d'un contrôle régulier.

5.1.3. Alimentation électrique et climatisation

Les moyens en électricité et en air conditionné (climatisation, refroidissement des machines) sont dûment dimensionnés pour permettre le bon fonctionnement de l'AC et assurer la disponibilité des services essentiels de celle-ci.

5.1.4. Vulnérabilité aux dégâts des eaux

Des mesures de sécurités sont mise en place sur le site pour la protection contre les dégâts des eaux.

5.1.5. Prévention et protection incendie

Les plates-formes hébergeant l'accès sont équipées d'un mécanisme anti-incendie.

5.1.6. Conservation des supports

Les médias de stockage (disquette, CD, …), PV, Key Ceremony, dossier d'enregistrement, sont protégés dans des armoires fortes, contre les agressions extérieures (incendie, humidité, ...).
L'AC met en œuvre des sauvegardes des données sensibles de manière à garantir :

- L'accès à ces données dans le temps ;
- Le rejeu de scénario dans le temps ;
- La protection contre l'obsolescence des supports ;
- La fourniture de preuves les cas échéants.

5.1.7. Mise hors service des supports

Les supports destinés à être recyclés ou à être mis hors service font l'objet d'un recyclage ou d'une destruction. Les disques durs, et Les documents papiers de l'Opérateur de Certification, et en particulier les dossiers confidentiels, sont systématiquement détruits (par broyage) avant d'être envoyés au système de traitement des déchets du site.

5.1.8. Sauvegarde hors site

En ce qui concerne les sauvegardes informatiques, Almerys met en œuvre les procédures de sauvegardes externes des données de la plate-forme PKI afin de permettre la mise en œuvre d'un PRA sur un site distant.
Les sauvegardes sont testées régulièrement.

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1. Rôles de confiance

Les rôles de confiance mis en œuvre par l'AC afin d'assurer la gestion de sécurité de toutes les composantes de l'IGC, ces rôles sont définie pour satisfaire les règles de quorum nécessaires pour l'exécution des taches de l'IGC, et éviter tout abus de privilège.

5.2.2. Nombre de personnes requises par tâches

Lorsque le dual control est requis, au moins deux officiers de sécurité sont nécessaires pour exécuter une tache.
Toutes les taches critiques relative à la gestion des AC intermédiaires, des AC racine, et des clés cryptographiques des autorités requièrent un dual contrôle de deux officiers de sécurités.
La restauration des HSM requière également plusieurs détenteurs de secrets.
D'autre part, l'accès physique les zones sensibles bunker, et cages de faraday nécessite la présence simultanée d'au moins 2 personnes habilitées pour permettre l'accès.

5.2.3. Identification et authentification pour chaque rôle

Tous les membres du personnel de confiance disposent d'un moyen d'authentification fort par carte a puce et code pin pour accéder aux composantes de l'IGC. L'authentification forte par carte a puce et code pin est requise avant tout actions sur les composantes de l'IGC.

5.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul sont respectées.

Concernant les rôles de confiance de l'AC, le cumul suivant est interdit :

- Responsable de sécurité et ingénieur système;
- Auditeur système et tout autre rôle ;
- Ingénieur système et opérateur.

L'AC s'assure de l'adéquation de ces exigences en établissant la liste nominative des personnes concernées dans le document interne de l'IGC.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

5.3.1. Qualifications, compétences et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité, l'engageant à ne pas diffuser les documents sensibles de l'AC à des personnes non habilitées à les recevoir.

Les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée et est familier des procédures de sécurité.

Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités et des procédures liées à la sécurité du système et au contrôle du personnel.

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 conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3. Exigences en matière de formation initiale

Le personnel est préalablement formé ou sensibilisé 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. En particulier, un ensemble de ressources documentaires est mis à disposition du personnel.
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 plan de formation d'Almerys permet d'assurer la planification régulière de formations adaptées aux profils des intervenants. Les collaborateurs peuvent également exprimer leur besoin de formation lors des entretiens individuels semestriels qui permette de remettre à jour les plannings de formation individuels.

5.3.5. Fréquence et séquence de rotations entre différentes attributions

La rotation entre les attributions est effectuée à l'occasion d'un changement de poste ou de fonction de l'une des personnes disposant d'un rôle opérationnel ou d'un rôle de confiance pour l'AC.

La validité des attributions, en fonction des postes réellement occupés par les personnes cibles est revue à l'occasion de chaque audit interne.

5.3.6. Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans :

- Le règlement intérieur,
- La charte informatique d'Almerys
- La politique de sécurité d'Almerys.

5.3.7. Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées notamment celles encadrant le respect des niveaux de confidentialités des documents qui sont délivrés aux prestataires externes.

Les clauses suivantes pourront être ajoutées le cas échéant aux contrats liant Almerys aux prestataires externes :

- Le Prestataire s'oblige à affecter en permanence à l'exécution du présent contrat un personnel qualifié et compétent ou le cas échéant, un personnel ayant le niveau de qualification déterminé.
- Le Prestataire s'engage à actualiser son savoir-faire, à se tenir informé des meilleures pratiques du marché en la matière et à réaliser des sessions de formation permanente de son Personnel à ce savoir-faire évolutif.
- Le Prestataire s'engage à prendre les mesures nécessaires, notamment vis-à-vis de son Personnel, pour que soient maintenues confidentielles les informations de toute nature qui lui sont communiquées par Almerys.

5.3.8. Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de leur prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans l'infrastructure de gestion de clés disposent des procédures correspondantes.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

Almerys effectue des contrôles réguliers des journaux d'évènements, ils sont réalisés par les rôles de confiance « contrôleurs », la nature des contrôles sont tracés dans des fichiers de suivie.

5.5 ARCHIVAGE DES DONNEES

Les archives des ACs sont protégées en intégrité et en confidentialité pendant toutes la période de rétention. .

5.6 CHANGEMENT DE CLES D'AC

La durée de vie des clés des ACs est de 10 ans à compter de leur génération durant la cérémonie des clés.

Le renouvellement des clés sera demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

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 du certificat d'AC doit être supérieure à celle des certificats qu'elle signe.

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

A l'occasion du processus de renouvellement, les demandes de nouveaux certificats seront automatiquement orientées pour signature vers la nouvelle bi-clé d'AC.

Le certificat d'AC précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré. Durant cette période, deux certificats d'AC seront donc valables :

- L'ancien pour valider les certificats émis par ce certificat ;
- Le nouveau pour signer et émettre de nouveaux certificats et valider ces derniers.

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

Des mesures mises en œuvre par les ACs pour assurer la continuité et la reprise d'activité,ces mesures inclues :

- La redondance et le basculement des services
- La sauvegarde et la restauration des services
- La notification et les communications vers les clients
- .

5.8 FIN DE VIE DE L'IGC

5.8.1. Transfert d'activité affectant une composante de l'IGC

Si Almerys décide de transférer son activité d'émission de certificats, elle devra mettre en œuvre les procédures organisationnelles suivantes.

Si le transfert nécessite un arrêt des équipements techniques :

- L'AC s'assurera d'émettre des LCR et des LAR à jour ;
- En concertation avec le service de communication d'Almerys, émettra un communiqué faisant état d'un arrêt temporaire des services d'émission de certificat ;
- Procèdera à l'arrêt des serveurs ;
- Transférera les serveurs vers le nouvel organisme responsable;
- Procèdera au transfert des parts de secrets vers de nouveaux porteurs de secret.

Dans cette situation, l'AC doit maintenir la publication des LCR tant que les équipements de l'IGC n'ont pu être réactivés sur le nouveau site.
Si le transfert est simplement un transfert de responsabilité, seul le transfert des parts de secrets vers de nouveaux porteurs de secrets est à observer.
Dans tous les cas le transfert d'activité nécessite une mise à jour et une nouvelle validation du référentiel documentaire de l'IGC.

5.8.2. Cessation d'activité affectant l'AC

Dans le cas d'une cessation d'activité, l'AC procèdera à la révocation des certificats émis en son nom..

6. MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI CLES

6.1.1. Génération des bi clé

6.1.1.1. Clés d'AC

La génération d'une nouvelle paire de clé pour l'AC est réalisée durant une cérémonie des clés dont le déroulement est détaillé dans le document « Déroulement général de la KC des ACs»,.

6.1.1.2. Clés des porteurs

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les clés des Porteurs sont générées sur des sites des AEs dont les conditions de sécurité sont établies contractuellement entre l'AC et l'AE. La génération des clés se fait sur un support cryptographique matériel qualifié SSCD (Secure Signature Creation Device) ou qualifié QSCD qui bénéficie d'une qualification selon eIDAS. Suite à la remise du support cryptographique au Porteur, ce dernier est amené à signer un procès-verbal de réception de ce support. Le statut de qualification du QSCD fait l'objet d'une surveillance par Almerys afin de prendre les mesures nécessaires en cas de perte ou de non-renouvellement de la qualification.

Certificats de cachet pour les organisations et d'unité d'horodatage
Le Service de stockage sécurisé de Bi-clé de l'AC 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 ou EAL4+ critères communs. Ce module est hébergé dans les locaux à accès très restreint Almerys. La génération des clés de signature cachet 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.. . .

Certificats de signature déportée
Les bi clés de signature des porteurs sont générés dans des HSMs cryptographiques certifié ELA4+ critères communs.

6.1.2. Transmission de la clé privée à son propriétaire

6.1.2.1. Clés d'AC

Les bi-clés sont générées directement dans les dispositifs sécurisés de chacune des AC, la clé privée est utilisée exclusivement dans le HSM cryptographique.

6.1.2.2. Clés porteur générées par l'AC

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Voir la PC

Certificats de cachet pour les organisations et d'unité d'horodatage
les clés privées sont générées et utilisées exclusivement dans les HSMs cryptographiques.

Certificats de signature déportée
Voir certificat de cachet

6.1.3. Transmission de la clé publique à l'AC

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
La clé publique est transmise à l'AC via le middleware carte à puce.

Certificats de cachet pour les organisations et d'unité d'horodatage
La clé publique est transmise à l'AC dans la requête PKCS#10 produite à l'issue de la KC Client et signée par la clé privée du Client. Cette transmission est manuelle : le Maître de Cérémonie de la KC ou le Responsable sécurité de la PKI Almerys transmet la requête à l'un des PKI Security Officer sur une clé USB.

Certificats de signature déportée
La clé publique est transmise à l'AC dans une requête produite automatiquement par le service sécurisé de gestion de clé et signée par la clé privée du Client. La transmission à l'AC est automatique.

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

Les clés publiques de vérification de signature de l'AC sont mises à disposition des utilisateurs de certificats et consultables publiquement tel que défini en section 2.2 « Information devant être publiées ».

6.1.5. Tailles des clés

Les tailles de clés sont les suivantes :

- Certificat de l'AC : 4096 bits (algorithme RSA)
- Certificats des Porteurs et Cachets : 2048 bits (algorithme RSA)

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

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les paramètres utilisés sont conformes au profil défini au paragraphe 7 de la PC.

Certificats de cachet pour les organisations et d'unité d'horodatage
L'opération de génération des clés est délégué au HSM cryptographique.

Certificats de signature déportée
L'opération de génération des clés est délégué au HSM cryptographique.

6.1.7. Objectifs d'usages de la clé

6.1.7.1. Cas de l'AC

L'utilisation de la clé privée pour l'AC et du certificat associé est limitée à la signature de certificats et de LCR. Cet usage est explicitement indiqué dans le champ KeyUsage du certificat de l'AC.
La clé privée de l'AC n'est utilisée que dans un environnement sécurisé, au sein d'un boîtier cryptographique matériel (HSM).

6.1.7.2. Cas des porteurs

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
L'usage de la clé du porteur est strictement limité à la de signature électronique qualifié ou l'authentification forte.

Certificats de cachet pour les organisations et d'unité d'horodatage
L'usage de la clé est strictement limité au service de signature électronique en ligne. La clé est utilisée pour générer des signatures de type cachet qui seront associées aux documents présentés par le Client à l'Utilisateur du Service de signature électronique en ligne. Cet usage est explicitement marqué dans le certificat au niveau du champ KeyUsage. La signature peut être jointe ou intégrée aux documents. Dans le cadre des certificats d'horodatage, il s'agit de certificat de type cachet intégrant un champ spécifique pour préciser qu'il s'agit de certificat d'horodatage. Ces certificats positionnent comme usage de la clé « Digital Signature ».

Certificats de signature déportée
L'usage de la clé est strictement limité au service de signature électronique en ligne. La clé est utilisée pour générer des signatures qui seront associées aux documents présentés par le Client à l'Utilisateur du Service de signature électronique en ligne. Cet usage est explicitement marqué dans le certificat au niveau du champ KeyUsage. La signature peut être jointe ou intégrée aux documents.

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. Module cryptographique de l'AC

Le HSM utilisé par l'AC est un HSM certifié Fips 140 -2 Level 3.

6.2.1.2. Dispositifs cryptographiques des porteurs

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les dispositifs carte à puce remis aux Porteurs sont qualifiés SSCD ou QSCD (qualification eIDAS) sous une ou plusieurs références publiés par l'organe de contrôle, ou la commission européenne.

Certificats de cachet pour les organisations et d'unité d'horodatage
Le dispositif de création de signature des Clients est un Module cryptographique matériel certifié FIPS 140-2 niveau 3, ou EAL4+ critères communs. Sa configuration opérationnelle minimale est conforme au standard FIPS 140-2 niveau 3, ou EAL4+ Critères communs.

Certificats de signature déportée
Voir cachet

6.2.2. Contrôle de la clé privée par plusieurs personnes

La liste des porteurs de secrets du HSM est établie et tenue à jour suivant le respect des principes définis dans les Rôles et habilitations de la PKI Almerys.

6.2.3. Séquestre de la clé privée

Les clés privées ne font pas l'objet de séquestre.

6.2.4. Copie de secours de la clé privée

6.2.4.1. Cas de l'AC

La clé privée de l'AC fait l'objet de copie de secours sous la forme d'un backup de la partition chiffré et matérialisé par un token HARDWARE.

6.2.4.2. Cas des certificats finaux

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les clés privées des certificats des porteurs finaux ne font pas l'objet de copie de secours.

Certificats de cachet pour les organisations et d'unité d'horodatage
La clé privée du Client fait l'objet de copie de secours sous la forme d'un backup chiffré par la clé du HSM.

Certificats de signature déportée
La clé privée du Porteur pour les certificats non destinés pour bun usage unique fait l'objet de copie de secours sous la forme d'un backup chiffré par la clé du HSM.

6.2.5. Archivage de la clé privée

6.2.5.1. Cas de l'AC

Les clés privées des AC ne font pas l'objet d'un archivage.

6.2.5.2. Cas des certificats finaux

Les clés privées des Porteurs 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

Tout transfert de la clé privée d'une AC se fait sous forme chiffrée.
Les procédures de gestion du module cryptographique de l'AC sont détaillées dans la procédure constructeur HSM.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les clés privées des porteurs ne peuvent pas être extraites du QSCD.

Certificats de cachet pour les organisations et d'unité d'horodatage
Tout transfert de la clé privée du Client se fait sous forme chiffrée.

Certificats de signature déportée
Tout transfert de la clé privée du Porteur se fait sous forme chiffrée.

6.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées des AC sont stockées dans un HSM.
Les procédures de gestion du module cryptographique de l'AC sont détaillées dans la procédure du constructeur HSM.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Sans objet

Certificats de cachet pour les organisations et d'unité d'horodatage
Les clés privées des Clients sont stockées dans un HSM. Les procédures de gestion du module cryptographique des Clients sont détaillées dans la procédure du constructeur HSM.

Certificats de signature déportée
Les clés privées des Porteurs sont stockées dans un HSM. Les procédures de gestion du module cryptographique des Clients sont détaillées dans la procédure du constructeur HSM.

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 »
Les données d'activation sont générées au moment de la KC, elles sont détenues par les détenteurs de secrets.

6.2.8.2. Clés privées des porteurs

L'activation de la clé privée de l'Utilisateur est contrôlée via des données ou des actions d'activation (cf. section 6.4 « Données d'activation ») propres au porteur ou au client. L'activation est réalisée de façon sécurisée.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clé privée d'AC

Le module cryptographique résiste aux attaques physiques, par desactivation des clés privées d'AC. Le module est apte à détecter les attaques physiques suivantes : ouverture du dispositif, retrait ou forçage du boîtier.
Les procédures de gestion du module cryptographique de l'AC sont détaillées dans la procédure constructeur HSM.

6.2.9.2. Clés privées des porteurs

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Apres trois tentatives infructueuses de saisie du code d'activation, la carte du porteur est bloqué, la clé privée n'est utilisable par le porteur sans déblocage de la carte.

Certificats de cachet pour les organisations et d'unité d'horodatage
Les clés privées des Clients sont désactivables à partir du module cryptographique. Le module cryptographique résiste aux attaques physiques, par desactivation des clés privées. Le module est apte à détecter les attaques physiques suivantes : ouverture du dispositif, retrait ou forçage du boîtier. Les procédures de gestion du module cryptographique sont détaillées dans la procédure du constructeur de du HSM.

Certificats de signature déportée
Voir Cachet

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.

Les procédures de gestion du module cryptographique de l'AC sont détaillées dans la procédure du constructeur de gestion du HSM.

6.2.10.2. Clés privées des porteurs

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
La destruction de la clé privée est effectuée par destruction physique de la carte du porteur.

Certificats de signature déportée
En fin de vie de la clé privée du Porteur, normale ou anticipée (révocation), la clé est systématiquement détruite de façon automatique. Les procédures de gestion du module cryptographique de l'AC sont détaillées dans la procédure du constructeur du HSM.

6.2.10.1. Clés privées des Clients

Certificats de cachet pour les organisations et d'unité d'horodatage
En fin de vie de la clé privée du Client, normale ou anticipée (révocation), la clé est systématiquement détruite. Les procédures de gestion du module cryptographique de l'AC sont détaillées dans la procédure du constructeur du HSM.

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de création de signature

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 des certificats de l'AC sont archivées conformément à la politique d'archivage définie dans le chapitre 5.5.

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

Les clés de signature et les certificats de l'AC ont une durée de vie de 10 ans.
Les clés privées et les certificats des porteurs finaux ont une durée de vie maximale de 3 ans.

6.4 DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

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

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se fait lors de la Key Ceremony. Voir 6.2.8.1

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

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
La génération et l'installation des données d'activation se fait au moment de la personnalisation du support cryptographique, par l'Autorité d'Enregistrement, et avant remise de ce support au Porteur. La personnalisation du support consiste à générer pour ce support : - Un code PIN qui sera remis au Porteur. un code pin erroné peut être saisi 3 fois avant blocage de l'accès à la clé privée du support.

Certificats de signature déportée
La génération des clés privées de signature se fait et leur association avec un moyen d'authentification se fait lors de la phase préalable à la demande de certificat. Voir section 6.2.8.1 « Méthode d'activation de la Clés privées des Clients ». L'enregistrement des clients applicatifs du Service au niveau du Module nécessite également l'installation de données d'activation pour que les clients puissent communiquer avec la partition cryptographique Client contenant les secrets de signature. .

Certificats de cachet pour les organisations et d'unité d'horodatage
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.Voir section6.2.8.1 « Méthode d'activation de la Clés privées des Clients ». L'enregistrement des clients applicatifs du Service au niveau du Module nécessite également l'installation de données d'activation pour que les clients puissent 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 de la clé privée de l'AC sont remises aux porteurs de secrets du HSM lors de la cérémonie de clés du module HSM.
Les règles à respecter sont définies dans la « Charte Sécurité des Personnels de la PKI Almerys ».
Les mesures de protection sont fournies dans la « procédure de gestion des éléments sensibles ».

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

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Lors de la remise du support au Porteur, ce dernier signe un Procès-verbal de réception de son dispositif de signature. Il s'engage à travers ce procès-verbal à conserver de manière sécurisée et confidentielle les données d'activation (code PIN). Il est notamment invité à ne pas communiquer ces codes.

Certificats de signature déportée
Les données d'activation des clés privées de la signature déportée sont communiquées aux porteurs via un canal hors bande notamment par SMS, le porteur s'engage a protéger ses données d'activation et a ne pas communiquer ces codes.

Certificats de cachet pour les organisations et d'unité d'horodatage
En complément des mesures de sécurisation réseau et d'établissement du lien sécurisé entre l'application cliente et le HSM, l'application de signature possède une donnée d'activation de la clés privée de signature. Ces données sont protégées en confidentialité sur le serveur sur lequel est installée l'application pour que seule l'application puisse y accéder

6.4.1. Autres aspects liés aux données d'activation

Sans objet.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

6.5.1.1. Identification et authentification

L'ensemble des administrateurs intervenant sur le système serveur de l'IGC se connecte sur ces équipements par authentification forte par carte à puce.

.

6.5.1.2. Contrôle d'accès

La gestion des droits d'accès physique aux salles d'hébergement est opérée par l'équipe sécurité Almerys pour le site de Clermont-Ferrand.
Les comptes d'accès aux équipements sont administrés par les équipes d'exploitation pour le site de Clermont-Ferrand.

6.5.1.3. Administration et exploitation

Le cœur de la PKI Almerys est construit autour de l'applicatif PKI.

L'équipe qui exploite ce cœur PKI dispose d'un ensemble documentaire qui lui donne les règles d'administration et d'exploitation de de la PKI.

6.5.1.4. Intégrité des composantes

Des tests de vulnérabilités peuvent être opérés sur les infrastructures de la PKI Almerys de manière à garantir la bonne application des règles de sécurité.

6.5.1.5. Sécurité des flux

Les mesures de sécurité des flux sont décrites dans le Dossier d'architecture technique PKI Almerys.

6.5.1.6. Journalisation et audit

Des tableaux de bords sont mis en œuvre pour obtenir des informations :

- Sur les opérations réalisées sur les certificats (émission, révocation, renouvellement, …) ;
- Sur les incidents survenus sur les équipements de l'IGC.

6.5.1.7. Supervision et contrôle

Les équipes d'exploitation infrastructure Almerys sont en charge de superviser les équipements de l'IGC.
.

6.5.1.8. Sensibilisation

Les documents suivants permettent de sensibiliser les différents acteurs de l'IGC :

- Charte sécurité des personnels de l'IGC,
- Procédures de classification de l'information,
- Procédures de protection de l'information,
- Politique de sécurité de la PKI Almerys,.

6.5.2. Niveau de qualification des systèmes informatiques

N/A.

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.
Tout développement doit être cohérent avec la Politique de Sécurité d'Almerys et avec les exigences contenues dans la PC associée à la présente DPC.

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. Les Procédures de gestion du changement sont décrites dans la procédure de gestion des changements.

6.6.2. Mesures liées à la gestion de la sécurité

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

6.6.2.1. Mise à jour des composantes

Almerys a spécifié et mis en place des procédures de gestion des mises à jour de sécurité

6.6.2.2. Analyse de risque

Almerys a sélectionné 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.

6.6.2.3. Scan de vulnérabilité

Almerys réalise régulièrement des scans de vulnérabilité sur ses adresses IP publiques.

6.6.2.4. 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

Pour des raisons de confidentialité, l'architecture réseau détaillée ainsi que les matrices de flux internes et externes à la plate-forme sont disponibles dans le document Dossier d'architecture technique de la PKI Almerys.

6.8 HORODATAGE / SYSTEME DE DATATION

Les mécanismes de synchronisation mis en œuvre sur la plate-forme PKI d'Almerys sont décrits dans le document d'architecture technique de la PKI Almerys.

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 PROFIL DU CERTIFICAT DE L'AC

Voir PC associée à la présente DPC.

7.2 PROFILS DES CERTIFICATS PORTEUR

Voir PC associée à la présente DPC.

7.3 PROFIL DES LISTES DE CERTIFICATS REVOQUES

Voir PC associée à la présente DPC.

7.4 PROFIL DES CERTIFICATS DE REPONDEUR OCSP

Voir PC associée à la présente DPC.

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les procédures d'audit interne sont décrites dans le document « Procédure d'audit interne des AC Almerys ».

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

Voir la Politique de Certification de l'AC.