Objet	**Déclaration des Pratiques de Certification (version publique)** **OID : 1.3.6.1.4.1.48620.41.33.1 v2.6**

Niveau de diffusion	Liste de diffusion si Restreint ou Confidentiel
Public	

Version *	Date	Modifications	Rédacteur
V1.9	26/04/2018	Modification suite audit	MMI
V1.10	21/05/2019	Version revue	JGR
V2.01	15/06/2020	MAJ avec les nouvelles ACs	MMI
V2.02	12/11/2020	MAJ Mineur	MMI
V2.2	28/05/2021	MAJ Mineur	MMI
V2.3	01/06/2022	Changement logo, correction orthographique	PDA
V2.4	17/04/2025	Prise en compte de l'identification par MIE ou vidéo identification Mise en place de la nouvelle charte graphique	SPA
V2.5	24/06/2025	Gestion du cas théorique d'impossibilité de révocation	LBI
V2.6	30/03/2026	Mise en cohérence avec la PC 2.10	GBA

* <Version>.<Edition> Changement de version = évolution majeure Changement d'édition = évolution mineure

Durée de validité	Nombre de versions à conserver
1 ans	Minimum 2 (actuelle + précédente)

	Fonction	Date & Signature
Vérificateur 1	*Directeur de Sécurité* *Guillaume Bailleul*	Signature manuscrite – version officielle conservée
Vérificateur 2	*Responsable de l'AC* *Sébastien PASSELERGUE*	Signature manuscrite – version officielle conservée
Approbateur	*Directeur Général* *Younès El Gui*	Signature manuscrite – version officielle conservée

Glossaire / Abréviations

Terme / Acronyme Fr	Terme / Acronyme EN	Définition
AC	CA	Autorité de Certification *[Certification Authority]*
AE	RA	Autorité d'Enregistrement *[Registration Authority]*
AED		Autorité d'Enregistrement Déléguée
AH	TA	Autorité d'Horodatage *[Time-stamping Authority]*
AG	GA	Autorité de Gouvernance *[Governance Authority]*
ANSSI		Agence nationale de la sécurité des systèmes d'information
CC	CC	Critères Communs *[Common Criteria]*
CEN		Comité Européen de Normalisation
CSP		Cryptographic Service Provider
DN		Distinguished Name
DPC	CPS	Déclaration des Pratiques de Certification *[Certification Practice Statement]*
EAL		Evaluation Assurance Level
ETSI		European Telecommunications Standards Institute
HSM		Hardware Security Module
IGC	PKI	Infrastructure de Gestion de Clés *[Public Key Infrastructure]*
KC		Cérémonie des clés *[Key Ceremony]*
LAR		Liste des certificats d'AC Révoqués *[Authority Revocation List]*
LCR	CRL	Liste des Certificats Révoqués *[Certificate Revocation List]*
MC		Mandataire de Certification
OC	CO	Opérateur de Certification *[Certification Operator]*
OCSP		Online Certificate Status Protocol
OID		Object Identifier
PC	CP	Politique de Certification *[Certification Policy]*
PKCS		Public Key Cryptography Standards
PKI		Public Key Infrastructure
PKIX		Public Key Infrastructure – X.509
PP	PP	Profil de Protection *[Protection Profile]*
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

Sommaire

1 INTRODUCTION

1.1 Présentation générale

BE INVEST INTERNATIONAL SA, ci-après le Prestataire, 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 beys 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 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 SIGNATURE AND AUTHENTICATION CA NC) ;
- 1.3.6.1.4.1.48620.41.1.7.3.2 (PC SIGNATURE AND AUTHENTICATION CA NC 2) ;
- 1.3.6.1.4.1.48620.41.1.5.2.1 (PC CUSTOMER SERVICES CA NB) ;
- 1.3.6.1.4.1.48620.41.1.4.2.1. (PC USER SIGNING CA NB).

Son identifiant d'objet (OID) est le suivant : 1.3.6.1.4.1.48620.41.33.1 v2.6.

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).dpcpublic(33).v(1).

1.3 Entités 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'AED a pour fonction de gérer les relations entre l'A C et les Porteurs de Certificat notamment en matière de délivrance des Certificats conformément aux Procédures d'AED.

L'AED 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 au Prestataire, 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'AED 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'AED 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'AC.

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

L'AED 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'AED s'engage à désigner les personnes physiques jouant le rôle d'opérateur d'AED et à informer l'AC en cas de modification des opérateurs.

L'AED s'engage à se soumettre à toute action de contrôle, par un membre de l'AC 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'AC.

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 les informations d'identification du futur Porteur de Certificat, selon l'un des procédés suivants :
    - Lors d'un face à face avec l'AE ou AED, ou via un Mandataire de Certification.
    - A distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfont aux exigences énoncées à l'article 8 du règlement No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 en ce qui concerne le niveau de garantie élevé à l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne.
- 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'AE ;
- 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.

1.3.3 Client et Représentant Client

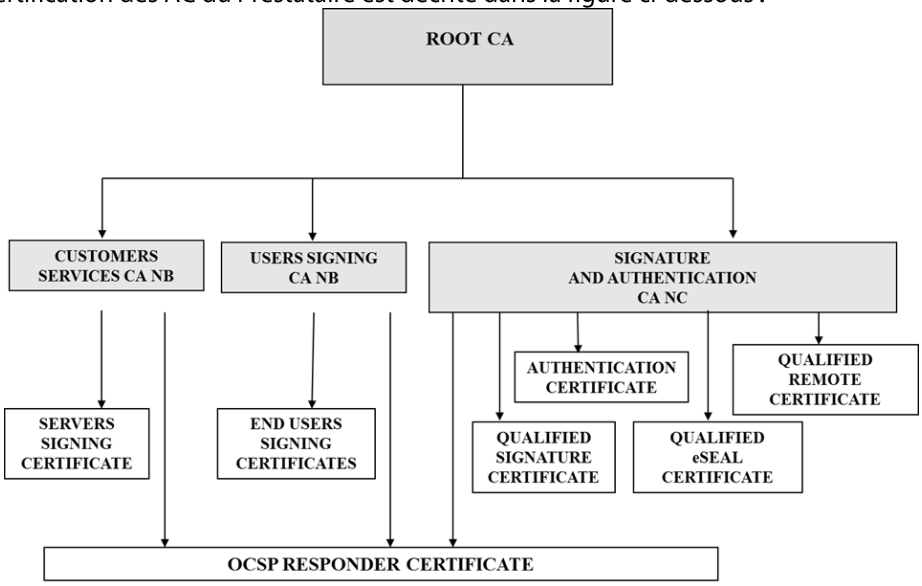
Pour les certificats de cachet d'organisation et les certificats d'unité d'horodatage, le Client est l'entité ayant souscrit au service du Prestataire pour ses propres besoins ou pour mise à disposition de ses utilisateurs.
Le Client est représenté, pour les opérations relatives au certificat, par une personne physique mandatée : le Représentant Client (RC).
Le RC est responsable, pour le compte de l'entité cliente, de la demande, de l'acceptation, de l'usage et, le cas échéant, de la révocation du certificat concerné, ainsi que du respect des obligations qui lui incombent au titre de la présente DPC.
Le RC peut être le représentant légal de l'entité ou une personne physique dûment désignée par ce dernier. Cette désignation repose sur un mandat écrit et signé, par lequel le représentant légal délègue explicitement tout ou partie des responsabilités liées à la gestion du certificat.

Le Client informe le Prestataire, préalablement sauf cas exceptionnel et dans ce cas sans délai, de tout changement affectant le RC ou son habilitation. En l'absence de RC explicitement identifié et habilité, le Prestataire peut refuser toute opération sur le certificat concerné ou procéder à sa révocation conformément aux procédures en vigueur.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

La chaîne de certification des AC du Prestataire 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 : le terme AC dans ce document sera utilisé pour désigner une AC subordonnée ;

Catégories d'AC	Noms des ACs
AC CUSTOMERS SERVICES CA NB	ALMERYS CUSTOMERS SERVICES CA NB BE-YS CUSTOMERS SERVICES CA NB
AC USERS SIGNING CA NB	ALMERYS USERS SIGNING CA NB BE-YS USERS SIGNING CA NB
AC SIGNATURE AND AUTHENTICATION CA NC	ALMERYS SIGNATURE AND AUTHENTICATION CA NC BE-YS SIGNATURE AND AUTHENTICATION CA NC BE-YS SIGNATURE AND AUTHENTICATION CA NC 2

- Les certificats utilisateurs finaux de chaque AC sont décrits dans le paragraphe ci-après.

1.4.1.1 Bi-clés et Certificats des Clients

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

- 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 qualifiés de cachet électronique, conforme au Règlement eIDAS et à la 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 ; ou
- Des certificats de signature déportée conforme à la norme EN 319 411-2 QCP-n, utilisé par Service de signature électronique, grâce auquel l'Utilisateur peut signer les formulaires ou documents présentés par le Client, générant ainsi une signature avancée fondée sur un certificat qualifié.

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

- 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 « USER SIGNING CA NB » sont :

- 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 du Prestataire.

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

Les Bi-clés et Certificats des AC 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

Se référer au même paragraphe présent dans chaque Politique de Certification.

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 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

Se référer au même paragraphe présent dans chaque Politique de Certification.

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

Afin de déterminer la conformité de la présente DPC avec les PC, l'AG s'appuie sur les ressources internes ou externes spécialisées dans l'audit et l'évaluation de la sécurité des services et des produits.
Pour les exigences portant sur une AE déléguée « Client be-ys », l'AG est en charge de commanditer un audit annuel pour mesurer cette conformité.

1.5.4 Procédure 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 Définitions

Terme	Définition
Applications utilisatrices	Services applicatifs exploitant les Certificats émis par l'AC, par exemple, pour des besoins de signature électronique ou de vérification de signature ou de cachet
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 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, conformément à la PC et à la DPC définies par son AG. L'ACR be-invest est auto-certifiée, c'est-à-dire que son certificat est auto-signé. L'ACR be-invest 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 **Erreur ! Source du renvoi introuvable.** de la présente PC. L'AE a pour rôle de vérifier l'identité du futur Porteur de certificat
Autorité d'Enregistrement Délégué (AED) ***[Delegate Registration Authority (DRA)]***	Autorité d'enregistrement sous contrat avec l'AC, pour effectuer les tâches d'une AE
Autorité de Gouvernance (AG) ***[Governance Authority (GA)]***	Entité responsable de l'ensemble des fonctions de l'IGC be-invest 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. Certificats de cachet pour les organisations et d'unité d'horodatage Dans le cadre de la présente PC, le Certificat désigne un Certificat électronique de signature de personne morale (signature cachet),

Terme	Définition
	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 be-invest, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des Utilisateurs. Certificats de cachet pour les organisations et d'unité d'horodatage Les Certificats Cachet émis par l'AC 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 Certificats (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)	Le Mandataire de Certification est désigné par et placé 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 (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis)

Terme	Définition
Module cryptographique matériel *[Hardware Cryptographic Module (HSM)]*	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 ou une application 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]*	Un Porteur de certificats est une personne physique ou un Client (cf. § *Erreur ! Source du renvoi introuvable.*)
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 du Prestataire	Un des services de la gamme d'offres de services de dématérialisation et de confiance be-invest, déployé en tout ou partie
Signature électronique ou Signature	« Données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer », conformément au Règlement eIDAS
Uniform Resource Locator (URL)	Adresse d'un site internet

Terme	Définition
Utilisateur	Voir « Application utilisatrice »

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

2.1 Entités chargées de la mise à disposition des informations

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

- 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, le site pki.almerys.com est redondé avec un autre site de publication au Luxembourg : pki.be-ys.com.

2.2 Informations devant être publiées

Conformément à la PC, les informations publiées par l'AC sont les suivantes :

- Les Politiques de Certifications des AC ;
- 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 AC et de l'AC racine ;
- La présente DPC.

La page web de présentation PKI disponible à l'URL http://pki.almerys.com/almerys.html et l'URL https://pki.be-ys.com/be-ys.html 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 Délais et fréquences 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 certificats 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 est accessible 24h/24 et 7j/7.

Le Prestataire 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 Contrôle d'accès aux informations publiées

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.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Type 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 au niveau du paragraphe ***3.1.2***, la DPC précise les éléments suivants :

Pour les AC almerys

- 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 AC sont identifiés comme suit :

Attributs	Valeurs
CN	Nom de l'AC
OU	0002 432701639
O	Almerys
C	FR

Pour les AC du Prestataire

- La raison sociale du Prestataire, tel que figurant au registre de commerce pour le certificat de l'AC (be-ys) et la raison sociale de l'entité du porteur pour les certificats finaux (attribut OrganizationName) ;
- Le numéro de TVA communautaire du Prestataire pour le certificat d'AC, et le code SIREN (numéro d'immatriculation au registre commerce) du Client pour les certificats finaux.

Le certificat des AC sont identifiés comme suit :

Attributs	Valeurs
CN	Nom de l'AC
OU	VATLU-LU29222134
O	BE INVEST International S.A.
C	LU

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 nom

Voir le paragraphe 7 de la PC.
Les noms utilisés pour les certificats des AC 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 au niveau du paragraphe 3.1.5, le Prestataire applique les pratiques ci-dessous.

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 contenant un identifiant unique.

Un identifiant unique est utilisé pour référencer le porteur dans le référentiel.

De plus tous les certificats émis par les AC 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'identité

L'AE doit être de confiance et authentifiée par l'AC, en particulier, le Prestataire s'assure que les AE 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

La validation de l'identité d'un organisme applique les mêmes règles que celles décrites dans le paragraphe ***3.2.3*** « ***Validation de l'identité d'un individu*** » présent ci-dessous.

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 ;
- Soit par l'AE ou l'AED 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'AE ;
  - Pré-remplie sur la base des informations contenues dans une base de données du Client, si le Porteur est déjà connu du Client, ou du Prestataire.
- Soit 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'AE ou l'AED 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 futur Porteur et l'AE (ou le mandataire) pour les certificats qualifiés.

Moyens recevables pour l'identification initiale
L'identification initiale d'une personne physique peut être réalisée :

- en présence physique devant l'AE, l'AED ou via un Mandataire de Certification, selon les procédures applicables ;
- à distance au moyen d'un moyen d'identification électronique satisfaisant au niveau de garantie requis par la réglementation applicable ;
- à distance au moyen d'une signature électronique qualifiée apposée par la personne à identifier, lorsque cette modalité est autorisée par le Prestataire et mise en œuvre conformément aux procédures internes assurant un niveau d'assurance équivalent.

Dans ce dernier cas, l'AE vérifie la validité du certificat qualifié utilisé, son état non révoqué, la cohérence des données d'identité portées par le certificat avec les informations du dossier, ainsi que la conservation des preuves associées au contrôle effectué.

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.

Le Prestataire 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 Client

Voir le paragraphe ***3.2.3.3*** de la PC 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 le numéro d'identification (typiquement 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 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 la 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 la 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 demande émane du représentant légal ou de son mandataire désigné.

Cas des certificats de cachet et des certificats d'unité d'horodatage

L'AE vérifie que la personne physique agissant au nom de l'organisation est dûment habilitée à effectuer la demande de certificat.

Cette vérification repose sur :

- l'identification de l'organisation cliente ;
- l'identification de la personne physique agissant comme Représentant Client ;
- la vérification de la qualité de représentant légal ou, à défaut, de l'existence d'un mandat écrit et signé conférant au RC les pouvoirs nécessaires pour demander, accepter, utiliser et révoquer le certificat, en tout ou partie.

Toute limitation ou retrait d'habilitation du RC doit être pris en compte avant exécution de toute nouvelle demande, renouvellement, modification ou révocation.

3.2.6 Critères d'interopérabilité

Les AC n'ont aucun accord de reconnaissance avec une AC extérieure au domaine de sécurité auquel elles appartiennent.

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 clés

3.3.1 Identification et validation pour un renouvellement courant

Voir le paragraphe ***3.3.1*** de la PC.

3.3.2 Identification et validation pour un renouvellement des clés après révocation

Voir le paragraphe ***3.3.2*** de la PC.

3.4 Identification et validation d'une demande de révocation

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

Pour les certificats de signature et d'authentification sur support cryptographique, le Porteur ou le demandeur du certificat peut solliciter la révocation :

- soit auprès de l'AE, en agence ou par téléphone ;
- soit via le service téléphonique de révocation d'urgence, selon les modalités publiées par le Prestataire.

Lorsque la demande est reçue à distance, l'AE ou le service habilité procède préalablement à une authentification fiable du demandeur.

Cette authentification fiable peut notamment reposer sur l'utilisation d'un code, secret, donnée de contrôle ou mécanisme équivalent remis ou défini lors de l'enregistrement ou de la remise du certificat, ou sur tout autre moyen jugé suffisamment robuste par le Prestataire au regard des risques.
En cas d'échec de l'authentification fiable, la demande n'est pas exécutée en l'état ; elle est redirigée vers une procédure nécessitant une vérification complémentaire de l'identité ou un traitement par l'AE.
Cas des certificats de cachet pour les organisations et des certificats d'unité d'horodatage
Le demandeur habilité à solliciter la révocation est le Représentant Client identifié dans le dossier ou son successeur régulièrement habilité.
La demande de révocation est réalisée au moyen du formulaire ou du canal mis à disposition par le Prestataire.
L'AE vérifie l'identité du RC ainsi que l'étendue de son habilitation avant d'exécuter la révocation.
En cas de changement de RC non encore enregistré, la révocation ou toute autre opération sensible sur le certificat peut être suspendue jusqu'à régularisation du dossier d'habilitation.

3.4.2 Demande faite par l'Autorité d'Enregistrement

Voir le paragraphe ***3.4.2*** de la PC.
Quel que soit le cas de figure, l'exécution du processus de révocation du certificat consiste pour un opérateur autorisé à :

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

3.4.3 Demande faite par le centre de support

Voir le paragraphe ***3.4.3*** de la PC.

Si le centre de support peut traiter la demande de révocation, les opérations sont similaires à celles réalisées au paragraphe ***3.4.2***.

3.4.4 Demande faite par le responsable du Service

Voir la PC.

3.4.5 Demande faite par l'Autorité de Certification ou l'Autorité de Gouvernance

Voir le paragraphe ***3.4.5*** de la PC.

Les opérations sont similaires à celles réalisées au paragraphe ***3.4.2***.

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 présentés dans le paragraphe 4.1.1 de la PC, 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 du Prestataire ou partenaire du Prestataire, via le portail du service ;
- Par courrier ;
- Lors du face à face avec l'AE.

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

Voir la 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 et présenté dans le paragraphe ***3.2.3.3*** « ***Enregistrement d'un Client*** »).
Il est de la responsabilité du RC de communiquer les informations suivantes dans le formulaire :

- Coordonnées du RC comprenant son prénom, son nom, sa fonction, son adresse électronique et ses coordonnées 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, les 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, cette dernière se connecte sur l'outil d'enrôlement, saisie, et valide les informations puis effectue la demande de génération de certificat auprès de l'AC.

4.2.2 Acceptation ou rejet de la demande

Voir la PC.

4.2.3 Durée d'établissement du certificat

Voir la PC.

4.3 Délivrance 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 en : • La génération des bi-clés dans le QSCD du porteur ; • La génération du certificat par l'AC ; • L'envoi 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 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 (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, sur le script de déroulement de la KC.

Certificats de signature déportée

La procédure de personnalisation des certificats sur le support est décrite dans la documentation interne de l'IGC, elle consiste en :
• La génération des bi-clés du porteur dans le HSM cryptographique ;
• La génération du certificat par l'AC ;
• L'envoi du code d'activation par :
  ○ SMS au porteur pour les certificats à usage unique (durée de validité éphémère) ;
  ○ Moyen d'authentification 1 facteur (Niveau LCP), ou deux facteurs (Niveau Qualifié) pour certificats à usage récurrent.

4.3.2 Notification par l'AC de la délivrance du certificat

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
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.

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

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Voir la PC.

4.4.2 Publication du certificat

Les certificats émis par les AC ne sont pas publiés.

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

Voir la PC.

4.5 Usages de la Bi-clé 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 la PC.

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

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 initiés par les applications autorisées.

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

Voir la 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 la PC.

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

Voir la PC.

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

Voir la PC.

4.6 Renouvellement d'un certificat

Cette pratique n'est pas autorisée. Voir la PC.

4.7 Délivrance d'un nouveau certificat suite à changement de la Bi-clé

4.7.1 Causes possibles de changement d'une bi-clé

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

4.7.2 Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat suit le même processus qu'une demande initiale, conformément au paragraphe ***4.1.1*** « ***Origine d'une demande de certificat*** ».

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

Le traitement d'une demande de nouveau certificat à la suite d'un changement de la Bi-clé applique les mêmes règles que celles décrites dans le paragraphe ***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 paragraphe ***3.3*** « ***Identification et validation d'une demande de renouvellement de clés*** ».
Les actions de l'AC sont les mêmes que celles décrites dans le paragraphe ***4.3*** « ***Délivrance du certificat*** ».

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

4.7.4 Notification de l'établissement du nouveau certificat

La notification de l'établissement du nouveau certificat à la suite d'un changement de la Bi-clé applique les mêmes règles que celles décrites dans le paragraphe ***0*** «

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

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, l'adresse électronique précise qu'il s'agit de la délivrance d'un nouveau certificat.

4.7.5 Démarche d'acceptation du nouveau certificat

Les démarches d'acceptation du nouveau certificat à la suite d'un changement de la Bi-clé appliquent les mêmes règles que celles décrites dans le paragraphe ***4.4.1*** « ***Démarche d'acceptation du certificat*** ».

4.7.6 Publication du nouveau certificat

La publication du nouveau certificat à la suite d'un changement de la Bi-clé applique les mêmes règles que celles décrites dans le paragraphe ***4.4.2*** « ***Publication du certificat*** ».

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

La notification par l'AC aux autres entités de la délivrance du nouveau certificat à la suite d'un changement de la Bi-clé applique les mêmes règles que celles décrites dans le paragraphe ***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 DPC.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de Porteurs

Voir la PC.

4.9.1.2 Certificats 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 dans le paragraphe ***3.4*** « ***Identification et validation d'une demande de révocation*** ».
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 courriel à l'adresse électronique de contact présentée dans les CGU, la demande dûment complétée doit être fournie en pièce jointe du courriel ;
- Par téléphone en joignant soit l'AE, soit le service téléphonique de révocation ;
- 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 be-ys.
En cas de révocation du certificat de l'AC, une information claire sera établie sur le site internet de la PKI : http://pki.almerys.com et http://pki.be-ys.com.

Après la décision prise par l'AG 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 applique systématiquement les procédures de révocation d'un certificat d'AC, en mobilisant les moyens organisationnels et techniques nécessaires pour garantir une exécution dans les délais et sécurisée. L'organisation en place (mobilisation des porteurs de secrets, procédure validée, moyens techniques disponibles) garantit que toute demande de révocation pourra être traitée dans le délai défini dans la politique de certification.

4.9.5.3 Cas de révocation impossible durant le délai prévu

L'organisation mise en place permet de répondre aux demandes de révocation durant le délai défini dans la politique de certification. Il n'y a donc pas de procédure d'exception à mettre en place.

4.9.6 Exigences de vérification de la révocation par les applications utilisatrices 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 30 minutes 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 48 heures.

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

Voir la PC.

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

Les exigences de vérifications sont les mêmes que celles décrites dans le paragraphe ***0*** « ***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 dans le cadre de la présente DPC.

4.9.12 Exigences spécifiques en cas de compromission de la clée 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.
Le Prestataire 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 du Prestataire.

Le Prestataire devra également notifier son organe de contrôle sans délai et aux maximum dans les 24 heures après avoir eu connaissance de la compromission.

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 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.

Certificats de signature déportée
Voir la PC.

4.9.13 Causes possibles d'une suspension

Sans objet dans le cadre de la présente DPC.

4.9.14 Origine d'une demande de suspension

Sans objet dans le cadre de la présente DPC.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet dans le cadre de la présente DPC.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet dans le cadre de la présente DPC.

4.10 Fonction d'information sur l'état 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 du Prestataire.

4.10.3 Dispositifs optionnels

Sans objet dans le cadre de la présente DPC.

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 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.

Certificats de signature déportée
Voir la PC.

4.12 Séquestre de clé 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 dans le cadre de la présente DPC.

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

Sans objet dans le cadre de 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 sécurité physique

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

- Le card management system 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 du Prestataire 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 contruction 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. Tous les accès aux zones

sécurisées sont monitorés, avec une mise sous alarmes de sécurité. Le passage obligatoire d'une zone à l'autre nécessite 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 control.

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 Sauvegardes hors site

En ce qui concerne les sauvegardes informatiques, le Prestataire 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 sécurité procédurales

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 définis 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 tâche. Toutes les tâches 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 à puce et code PIN pour accéder aux composantes de l'IGC. L'authentification forte par carte à puce et code PIN est requise avant tout actions sur les composantes de l'IGC.

5.2.4 Rôles exigeant une séparation des attributions

Voir PC.

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 sécurité vis-à-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

Voir PC.

5.3.3 Exigences en matière de formation initiale

Voir PC.
Un ensemble de ressources documentaires est mis à disposition du personnel.

5.3.4 Exigences et fréquence en matière de formation continue

Le plan de formation du Prestataire 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 rotation 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 Sansctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans le règlement intérieur.

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 le Prestataire aux prestataires externes :

- Le prestataire externe 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 externe 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 externe 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 le Prestataire.

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 Procédures de constitution des données d'audit

Le Prestataire 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 suivi.

5.5 Archivage des données

Les archives des AC sont protégées en intégrité et en confidentialité pendant toute la période de rétention.

5.6 Changement de clés 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.

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 à compromission et sinistre

Des mesures sont mises en œuvre par les AC pour assurer la continuité et la reprise d'activité. Ces mesures incluent :

- 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 le Prestataire décide de transférer son activité d'émission de certificats, il 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, l'AC émettra un communiqué faisant état d'un arrêt temporaire des services d'émission de certificat ;

- L'AC procèdera à l'arrêt des serveurs ;
- L'AC transférera les serveurs vers le nouvel organisme responsable ;
- L'AC 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 Génération et installation de Bi-clés

6.1.1 Génération des Bi-clés

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 AC**».

6.1.1.2 Clés des Porteurs et des Clients

Voir PC.

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 be-ys 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*** « ***Informations devant être publiées*** ».

6.1.5 Tailles des clés

Voir PC.

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 déléguée au HSM cryptographique.

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

6.1.7 Objectifs d'usage 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 Clés porteur générées par l'AC

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 sécurité pour la protection des clés privées 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

Le HSM utilisé par l'AC est un HSM certifié Fips 140 -2 Level 3, ou critères communs EAL4+.

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 du Prestataire.

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

Voir PC.

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

Voir PC.

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.

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

La méthode d'activation de la clé privée d'ACC applique les mêmes règles que celles présentées dans le paragraphe ***6.2.2*** « ***Contrôle de la clé privée 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 et des Clients

Voir PC.

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 désactivation 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 et des Clients

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

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 désactivation des clés privées dans des conditions similaires à celui de l'AC (voir le paragraphe ***6.2.9.1*** présent ci-dessus)

Certificats de signature déportée
Voir Cachet.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

Voir PC.
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 et des Clients

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

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.

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

Le niveau de qualification est soumis aux mêmes règles que celles présentées dans le paragraphe ***6.2.1*** « ***Standards et mesures de sécurité pour les modules cryptographiques*** ».

6.3 Autres aspects de la gestion des Bi-clés

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 paragraphe ***5.5*** « ***Archivage des données*** ».

6.3.2 Durées 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 Données 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, conformément aux règles décrites dans le paragraphe ***6.2.8.1*** « ***Clé privée d'AC*** ».

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
Voir la PC.

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, conformément au paragraphe ***6.2.8*** « ***Méthode d'activation de la clé privée*** ». 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, conformément au paragraphe ***6.2.8*** « ***Méthode d'activation de la clé privée*** ». 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** ».
Les mesures de protection sont fournies dans la procédure « **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 à protéger ses données d'activation et à 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.

6.4.2.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurités des systèmes 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 du Prestataire 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 du Prestataire 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 la PKI.

6.5.1.4 Intégrité des composantes

Des tests de vulnérabilités peuvent être opérés sur les infrastructures de la PKI du Prestataire 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 du Prestataire.

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 du Prestataire 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 du Prestataire.

6.5.2 Niveau de qualification des systèmes informatiques

La DPC ne prévoit pas d'exigences spécifiques à ce sujet.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Voir PC.
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 du Prestataire doit être signalée à l'AG pour validation. Elle doit être documentée.

6.6.2.1 Mise à jour des composantes

Le Prestataire a spécifié et mis en place des procédures de gestion des mises à jour de sécurité.

6.6.2.2 Analyse de risques

Le Prestataire 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

Voir la PC.

6.6.2.4 Test d'intrusion

Voir la PC.

6.7 Mesures de sécurité réseau

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 du Prestataire.

6.8 Horodatage / Système de datation

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

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil du certificat de l'AC

Voir la PC associée à la présente DPC.

7.2 Profil des certificats Porteurs

Voir la PC associée à la présente DPC.

7.3 Profil de LCR

Voir la PC associée à la présente DPC.

7.4 Profil certificat de l'OCSP

Voir la 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 be-ys ».

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

Voir la Politique de Certification de l'AC