bews
corporation luxembourg

POLITIQUE DE CERTIFICATION DE L'AC CA NC 2

Objet	**POLITIQUE DE CERTIFICATION DE L'AC CA NC 2** **OID : 1.3.6.1.4.1.48620.41.1.7.3.2**

Niveau de diffusion	Liste de diffusion si Restreint ou Confidentiel
Public	

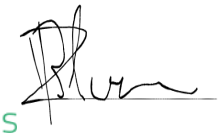
Version *	Date	Modifications	Rédacteur
2.01	15/06/2020	Modification format certificat	MMI
2.1	29/03/2021	Modification format certificat	MMI
2.2	28/05/2021	Maj mineur	MMI
2.3	12/08/2021	Modification suite audit eIDAS	MMI
2.4	25/05/2022	Demande de révocation d'urgence par service téléphonique, service OCSP disponible publiquement, modification mineure sur missions AED	PDA
2.5	22/11/2022	Ajout taille de RSA 3072 bits à partir du 1er janvier 2023 pour les gabarits de certificats pour la signature électronique sur support cryptographique, pour la signature électronique déportée et pour la signature cachet	PDA
2.6	01/02/2023	Validation initiale d'identité, rajout comme preuve d'identité, les éléments apportés par un PVID. Demande de certificat : cas de la demande signé par un certificat émis par une AC qualifiée Mise à jour des cumuls	PDA/SPA
2.7	14/04/2025	Ajout de la possibilité pour les AED d'utiliser un MIE au niveau élevé ou une vidéo-identification et correction de l'OID de stratégie en 7.1 Mise en place de la nouvelle charte graphique	SPA/GBA
2.8	16/05/2025	Demande de révocation faite par le porteur, ajout authenfication « fiable » Correctifs mineurs post audit 2025 Précision sur le rôle de Représentant Client	LBI
2.9	24/11/2025	Ajout de la possibilité d'utiliser une signature qualifiée lors de l'identification.	GBA
2.10	30/03/2026	Suppression du profil signature déportée Clarification conformité NIS 2 Suppression référence 2048 bits	GBA
2.11	22/06/2026	Reformulation des moyens de vérification d'identité Retrait des références à la signature déportée	GBA

Version *	Date	Modifications	Rédacteur
		Reformulation des dates de fin de validité dans les profils de certificats	
2.12	16/09/2026	Alignement des méthodes de vérification d'identité sur l'article 24, paragraphe 1 bis, du règlement (UE) n° 910/2014 modifié (§ 1.3.4.3, 3.2, 3.2.3 et 9.6.3) Retrait de la vérification d'identité au moyen d'un service d'identification en ligne de niveau de garantie substantiel (PVID) Précision de l'établissement exerçant la fonction d'autorité d'enregistrement Précision des critères de détermination de la durée de validité des certificats et des dates de fin de validité dans les profils Mise à jour des références réglementaires Reprise du modèle documentaire BE INVEST : en-tête, pied de page et mise en page Précision de l'entité assurant l'exploitation de l'IGC en sous-traitance	RBL

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

	Fonction	Date & Signature
Vérificateur	*Responsable de l'AC* *Rémi Blancher*	Signé électroniquement par Rémi BLANCHER Le 16/09/2026 à 11:07 CEST bevys trusted solutions 
Approbateur	*Administrateur délégué — BE INVEST INTERNATIONAL S.A.* *Younes El Gui*	Signé électroniquement par younes elgui Le 16/09/2026 à 11:12 CEST bevys trusted solutions

Public

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Glossaire / Abréviations

Terme / Acronyme Fr	Terme / Acronyme EN	Définition
AC	CA	Autorité de Certification *[Certification Authority]*
AE	RA	Autorité d'Enregistrement *[Registration Authority]*
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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Sommaire

1 Introduction 12

1.1 Présentation générale 12

1.1.1 Service de signature électronique BE INVEST INTERNATIONAL S.A. 13

1.2 Identification du document 15

1.3 Entités intervenant dans l'IGC 16

1.3.1 Autorité de certification (AC) 16

1.3.2 Autorité de Gouvernance (AG) 16

1.3.3 Service de stockage sécurisé des Bi-clés des Clients 16

1.3.4 Autorité d'Enregistrement (AE) 17

1.3.5 Autorités d'Enregistrement Déléguée (AED) 18

1.3.6 Client et Représentant Client 18

1.3.7 Le Porteur de Certificat 19

1.3.8 Applications utilisatrices des certificats 19

1.3.9 Autres participants 20

1.4 Usage des certificats 21

1.4.1 Domaines d'utilisation applicable 21

1.4.2 Domaines d'utilisation interdits 21

1.5 Gestion de la PC 22

1.5.1 Entité gérant la PC 22

1.5.2 Point de contact 22

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC 22

1.5.4 Procédure d'approbation de la conformité de la DPC 22

1.6 Définitions 22

2 Responsabilités concernant la mise à disposition des informations devant être publiées 26

2.1 Entités chargées de la mise à disposition des informations 26

2.2 Informations devant être publiées 26

2.3 Délais et fréquences de publication 26

2.4 Contrôle d'accès aux informations publiées 26

3 Identification et authentification 28

3.1 Nommage 28

3.1.1 Type de noms 28

3.1.2 Nécessité d'utilisation de noms explicites 28

3.1.3 Anonymisation ou pseudonymisation des Clients Type de noms 28

3.1.4 Règles d'interprétation des différentes formes de nom 29

3.1.5 Unicité des noms 29

3.1.6 Identification, authentification et rôle des marques déposées 29

3.2 Validation initiale de l'identité 29

3.2.1 Méthode pour prouver la possession de la clé privée 31

3.2.2 Validation de l'identité d'un organisme 31

3.2.3 Validation de l'identité d'un individu 31

3.2.4 Informations non vérifiées du Porteur 34

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

3.2.5 Validation de l'autorité du demandeur 34
3.2.6 Critères d'intéropérabilité 34

3.3 Identification et validation d'une demande de renouvellement des clés 34
3.3.1 Identification et validation pour un renouvellement courant 35
3.3.2 Identification et validation pour un renouvellement des clés après révocation 35

3.4 Identification et validation d'une demande de révocation 35
3.4.1 Demande faite par le Porteur, ou le demandeur du certificat 35
3.4.2 Demande faite par l'Autorité d'Enregistrement 36
3.4.3 Demande faite par le centre de support 36
3.4.4 Par le responsable du Service 36
3.4.5 Demande faite par l'Autorité de Certification ou l'Autorité de Gouvernance 36

4 Exigences opérationnelles sur le cycle de vie des certificats 37

4.1 Demande de certificat 37
4.1.1 Origine d'une demande de certificat 37
4.1.2 Processus et responsabilité pour l'établissement d'une demande de certificat 37

4.2 Traitement d'une demande de certificat 37
4.2.1 Exécution des processus d'identification et de validation de la demande 37
4.2.2 Acceptation ou rejet de la demande 37
4.2.3 Durée d'établissement du certificat 38

4.3 Délivrance du certificat 38
4.3.1 Actions de l'AC concernant la délivrance du certificat 38
4.3.2 Notification par l'AC de la délivrance du certificat 38

4.4 Acceptation du certificat 40
4.4.1 Démarche d'acceptation du certificat 40
4.4.2 Publication du certificat 40
4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat 40

4.5 Usages de la Bi-clés et du certificat 40
4.5.1 Utilisation de la clé privée et du certificat par le Client 40
4.5.2 Utilisation de la clé publique et du certificat par les Applications utilisatrices du certificat 41
4.5.3 Utilisation de la clé privée et du certificat de l'AC Racine 41
4.5.4 Utilisation de la clé privée et du certificat de l'AC 41
4.5.5 Publication du certificat 42

4.6 Renouvellement d'un certificat 42

4.7 Délivrance d'un nouveau certificat suite à changement de la Bi-clé 42
4.7.1 Causes possibles de changement d'une bi-clé 42
4.7.2 Origine d'une demande d'un nouveau certificat 42
4.7.3 Procédure de traitement d'une demande d'un nouveau certificat 42
4.7.4 Notification de l'établissement du nouveau certificat 42
4.7.5 Démarche d'acceptation du nouveau certificat 43
4.7.6 Publication du nouveau certificat 44
4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat 44

4.8 Modification du certificat 44

4.9 Révocation et suspension des certificats 44
4.9.1 Causes possibles d'une révocation 44

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange
© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

4.9.2 Origine d'une demande de révocation 45
4.9.3 Procédure de traitement d'une demande de révocation 45
4.9.4 Délai accordé pour formuler la demande de révocation 46
4.9.5 Délai de traitement par l'AC d'une demande de révocation 46
4.9.6 Exigences de vérification de la révocation par les applications utilisatrices de certificats 48
4.9.7 Fréquence d'établissement des LCR 48
4.9.8 Délai maximum de publication d'une LCR 48
4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats 48
4.9.10 Exigences de vérification en ligne de la révocation des certificats par les applications utilisatrices de certificats 48
4.9.11 Autres moyens disponibles d'information sur les révocations 49
4.9.12 Exigences spécifiques en cas de compromission de la clée privée 49
4.9.13 Causes possibles d'une suspension 49
4.9.14 Origine d'une demande de suspension 49
4.9.15 Procédure de traitement d'une demande de suspension 49
4.9.16 Limites de la période de suspension d'un certificat 49

4.10 Fonction d'information sur l'état des certificats 50
4.10.1 Caractéristiques opérationnelles 50
4.10.2 Disponibilité de la fonction 50
4.10.3 Dispositifs optionnels 50

4.11 Fin de la relation entre le Porteur et l'AC 50

4.12 Séquestre de clé et recouvrement 50
4.12.1 Politique et pratiques de recouvrement par séquestre des clés 50
4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session 50

5 Mesures de sécurité non techniques 51

5.1 Mesures de sécurité physique 51
5.1.1 Situation géographique et contruction des sites 51
5.1.2 Accès physique 51
5.1.3 Alimentation électriqe et climatisation 51
5.1.4 Vulnérabilité aux dégâts des eaux 52
5.1.5 Prévention et protection incendie 52
5.1.6 Conservation des supports 52
5.1.7 Mise hors service des supports 52
5.1.8 Sauvegardes hors site 52

5.2 Mesures de sécurité procédurales 52
5.2.1 Rôles de confiance 52
5.2.2 Nombre de personnes requises par tâches 53
5.2.3 Identification et authentification pour chaque rôle 53
5.2.4 Rôles exigeant une séparation des attributions 53

5.3 Validation initiale de l'identité d'une personne physique représentant une personne morale 54
5.3.1 Qualifications, compétences et habilitations requises 54
5.3.2 Procédures de vérification des antécédents 54
5.3.3 Exigences en matière de formation initiale 54
5.3.4 Exigences et fréquence en matière de formation continue 54
5.3.5 Fréquence et séquence de rotation entre différentes attributions 55
5.3.6 Sansctions en cas d'actions non autorisées 55
5.3.7 Exigences vis-à-vis du personnel des prestataires externes 55
5.3.8 Documentation fournie au personnel 56

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.4 Procédures de constitution des données d'audit 56
5.4.1 Type d'événements à enregistrer 56
5.4.2 Fréquence de traitement des journaux d'événements 57
5.4.3 Période de conservation des journaux d'événements 57
5.4.4 Protection des journaux d'événements 57
5.4.5 Procédure de sauvegarde des journaux d'événements 57
5.4.6 Système de collecte des journaux d'événements 58
5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement 58
5.4.8 Evaluation des vulnérabilités 58

5.5 Archivage des données 58
5.5.1 Types de données à archiver 58
5.5.2 Période de conservation des archives 58
5.5.3 Protection des archives 59
5.5.4 Procédure de sauvegarde des archives 59
5.5.5 Exigences d'horodatage des données 59
5.5.6 Système de collecte des archives 59
5.5.7 Procédures de récupération et de vérification des archives 59

5.6 Changement de clé d'AC 59

5.7 Reprise suite à compromission et sinistre 60
5.7.1 Procédures de remontée et de traitement des incidents et des compromissions 60
5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données) 60
5.7.3 Procédures de reprise en cas de corruption de la clé privée d'une composante 60
5.7.4 Capacités de continuité d'activités suite à un sinistre 61

5.8 Fin de vie de l'IGC 62
5.8.1 Transfert d'activité ou cesstion d'activité affectant une composante de l'IGC du Prestataire 62
5.8.2 Cessation d'activité affectant l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » 63

6 Mesures de sécurité techniques 64

6.1 Génération et installation de Bi-clés 64
6.1.1 Génération des Bi-clés 64
6.1.2 Transmission de la clé privée à son propriétaire 65
6.1.3 Transmission de la clé publique à l'AC 66
6.1.4 Transmission de la clé publique de l'AC aux Applications utilisatrices de certificats 66
6.1.5 Tailles des clés 66
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité 66
6.1.7 Objectifs d'usage de la clé 66

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 66
6.2.1 Standards et mesures de sécurité pour les modules cryptographiques 66
6.2.2 Contrôle de la clé privée de l'AC par plusieurs personnes 67
6.2.3 Séquestre de la clé privée 67
6.2.4 Copie de secours de la clé privée 67
6.2.5 Archivage de la clé privée 68
6.2.6 Transfert de la clé privée vers / depuis le module cryptographique 68
6.2.7 Stockage de la clé privée dans un module cryptographique 68
6.2.8 Méthode d'activation de la clé privée 68
6.2.9 Méthode de désactivation de la clé privée 69
6.2.10 Méthode de destruction des clés privées 69
6.2.11 Niveau d'évaluation sécurité du module cryptographique 70

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

6.3 Autres aspects de la gestion des Bi-clés 70
6.3.1 Archivage des clés publiques 70
6.3.2 Durées de vie des Bi-clés et des certificats 70
6.4 Données d'activation 70
6.4.1 Génération et installation des données d'activation 70
6.4.2 Protection des données d'activation 71
6.5 Mesures de sécurités des systèmes informatiques 71
6.5.1 Politique de sécurité des réseaux et des systèmes d'information 71
6.5.2 Exigences de sécurité technique spécifiques aux systèmes informatiques 71
6.5.3 Niveau de qualification des systèmes informatiques 72
6.6 Mesures de sécurté des systèmes durant leur cycle de vie 72
6.6.1 Mesures de sécurité liées au développement des systèmes 72
6.6.2 Mesures liées à la gestion de la sécurité 72
6.7 Mesures de sécurité réseau 73
6.7.1 Segmentation en zone 73
6.7.2 Interconnexions 73
6.7.3 Connexions 73
6.7.4 Disponibilité 74
6.8 Horodatage / Système de datation 74
7 Profils des certificats, OCSP et des LCR 75
7.1 Profil du certificat de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » 75
7.2 Profil des certificats Porteurs 76
7.2.1 Profils eIDAS support cryptographique 76
7.2.2 Profils eIDAS Cachet 79
7.2.3 Profils eIDAS Horodatage 81
7.3 Profil de LCR 83
7.4 Profil certificat de l'OCSP 85
8 Audit de conformité et autres évaluations 87
8.1 Fréquences et/ou circonstances des évaluations 87
8.2 Identités / Qualifications des évaluateurs 87
8.3 Relations entre évaluateurs et entités évaluées 87
8.4 Sujets couverts par les évaluations 87
8.5 Actions prises suite aux conclusions des évaluations 87
8.6 Communication des résultats 87
8.7 Autres éléments de conformité 88
9 Autres problématiques métiers et légales 89
9.1 Tarifs 89
9.2 Responsabilité financière 89
9.3 Confidentialité des données professionnelles 89

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

9.3.1 Périmètre des informations confidentielles 89
9.3.2 Informations hors du périmètre des informations confidentielles 89
9.3.3 Responsabilités en termes de protection des informations confidentielles 91

9.4 Protection des données à caractère personnel 91
9.4.1 Politique de protection des données à caractère personnel 91
9.4.2 Informations à caractère personnel 91
9.4.3 Responsabilité en termes de protection des données à caractère personnel 91
9.4.4 Notification et consentement d'utilisation des données à caractère personnel 91
9.4.5 Conditions de divulgation d'informations à caractère personnel aux autorités judiciaires ou administratives 91
9.4.6 Autres circonstances de divulgation d'informations personnelles 91

9.5 Droits sur la propriété intellectuelle et industrielle 91

9.6 Interprétations contractuelles et garanties 92
9.6.1 Autorité de Certification 92
9.6.2 Autorité de gouvernance 92
9.6.3 Autorité d'enregistrement (AED) 94
9.6.4 Porteurs 94
9.6.5 Client, Représentant Client 95
9.6.6 Applications utilisatrices de certificats 95
9.6.7 Autres participants 95

9.7 Limite de garantie 95

9.8 Limite de responsabilité 95

9.9 Indemnités 96

9.10 Durée et fin anticipée de validité de la PC 96
9.10.1 Durée de validité 96
9.10.2 Fin anticipée de validité 96
9.10.3 Effets de la fin de validité et clauses restant applicables 96

9.11 Notifications individuelles et communications entre les participants 97

9.12 Amendements à la PC 97
9.12.1 Procédures d'amendements 97
9.12.2 Circonstances selon lesquelles l'OID doit être changé 97

9.13 Dispositions concernant la résolution de conflits 97

9.14 Juridictions compétentes 97

9.15 Conformité aux législations et réglementations 98

10 Annexe 1 : Documents cités en référence 99

10.1 Conformité aux législations et réglementations 99

10.2 Conformité aux législations et réglementations 99

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange
© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions légales relatives aux droits de propriété intellectuelle. Ces droits sont la propriété exclusive BE INVEST INTERNATIONAL S.A..

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

1 INTRODUCTION

1.1 Présentation générale

Dans le cadre de ses offres de services de dématérialisation et de confiance, BE INVEST INTERNATIONAL S.A., ci-après le Prestataire, met à disposition de ses Entités clientes (entreprises, administrations, etc.) une Autorité de Certification spécifique, « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».Dans ce cadre, **le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification (AC)** « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 »**.** Cette AC est destinée à délivrer des Certificats :

- De signature électronique qualifié conforme au Règlement Européen eIDAS (ETSI EN 319411-2 niveau QCP-n-qscd) ;
- D'authentification conformément à l'ETSI 319411-1 NCP+ ;
- De cachet qualifié au sens du Règlement Européen eIDAS (ETSI EN 319411-2 2 niveau QCP-l) ;
- De cachet qualifié destiné à être utilisé dans des unités d'horodatage en vue de fournir un service d'horodatage qualifié au sens de eIDAS (Certificat de cachet conforme à l'ETSI EN 319411-2 niveau 2 niveau QCP-l) ;
- De certificat qualifié destiné à la création de signature avancée en mode déporté à l'aide d'un certificat qualifié (Certificat conforme à l'ETSI EN 319411-2 niveau QCP-n-qscd).

Ces certificats peuvent être délivrés à des Clients propres au Prestataire (dans ce cas le PrestataireBE INVEST INTERNATIONAL S.A. est sa propre Autorité d'Enregistrement) ou bien via les Autorités d'Enregistrement des Clients du Prestataire.

L'objectif de la PC est de définir les exigences concernant plusieurs typologies de certificats :

- Des certificats de signature et authentification sur support cryptographiques ;
- Des certificats de cachet et d'unité d'horodatage ;

Afin de distinguer clairement les exigences spécifiques aux différents types de certificat, celles-ci seront précisées dans un cartouche propre à chaque certificat suivant les codes de références ci-dessous :

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

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

Nous définissons à présent, pour chaque typologie de certificat, les différents OID associés :

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
La présente PC définit les exigences concernant les certificats de signature et d'authentification personnes physiques : • OID=1.3.6.1.4.1.48620.41.1.7.3.2.1.1: pour les certificats de signature qualifié ETSI EN 319411-2 • OID = 1.3.6.1.4.1.48620.41.1.7.3.2.2.1: pour les certificats d'authentification ETSI EN 319411-1 NCP+

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de cachet pour les organisations et d'unité d'horodatage
L'objectif de la présente PC est également de définir les exigences concernant les certificats de : • Cachet de personne morale (OID = 1.3.6.1.4.1.48620.41.1.7.3.2.4.1) • Unité d'horodatage (OID = 1.3.6.1.4.1.48620.41.1.7.3.2.5.1)

Dans toutes les phases de leur cycle de vie, l'Entité cliente, propriétaire d'un tel certificat, pourra s'authentifier sur le portail des services du Prestataire, générer un cachet ou signer numériquement des messages, des documents ou formulaires électroniques, assurant ainsi leur origine, leur intégrité, et, lorsque cela est applicable, leur non-répudiation. La mise en œuvre de ce certificat est assurée par un service automatisé (ensemble de serveurs informatiques) dûment autorisé à utiliser la clé privée de signature représentant la personne morale du Client.

Cette Politique de Certification est écrite en conformité aux normes :

- ETSI EN 319 401
- ETSI EN 319 411-1 NCP+
- ETSI EN 319 411-2

Les certificats produits respectent la norme X.509v3 et leur utilisation est dédiée au mécanisme de signature électronique qualifiée pour des personnes physiques.

La structure de la présente PC s'appuie sur les références suivantes :

- Le RFC 3647 de l'IETF « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework » ;
- Les Politiques de Certification Type du Référentiel Général de Sécurité (RGS) émises par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

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

1.1.1 Service de signature électronique BE INVEST INTERNATIONAL S.A.

Le Prestataire propose plusieurs solutions de signature :

- Une solution de signature électronique permettant la délivrance, entre autres, de certificats qualifiés ;
- Une solution de cachet électronique multicanal ;
- Une solution de signature électronique multicanale.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le Prestataire propose une solution de signature électronique auprès de ses Clients qui peuvent alors proposer sous leur étiquette directe ou sous l'étiquette du Prestataire la délivrance d'un certificat qualifié de signature électronique, généré et installé sur un support cryptographique matériel.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

La vérification du demandeur du certificat électronique est réalisée par l'Autorité d'Enregistrement, selon l'une des modalités prévues au paragraphe 3.2.3 de la présente Politique de Certification, notamment en présence physique ou au moyen d'un procédé d'identification admis par la réglementation applicable.

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

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

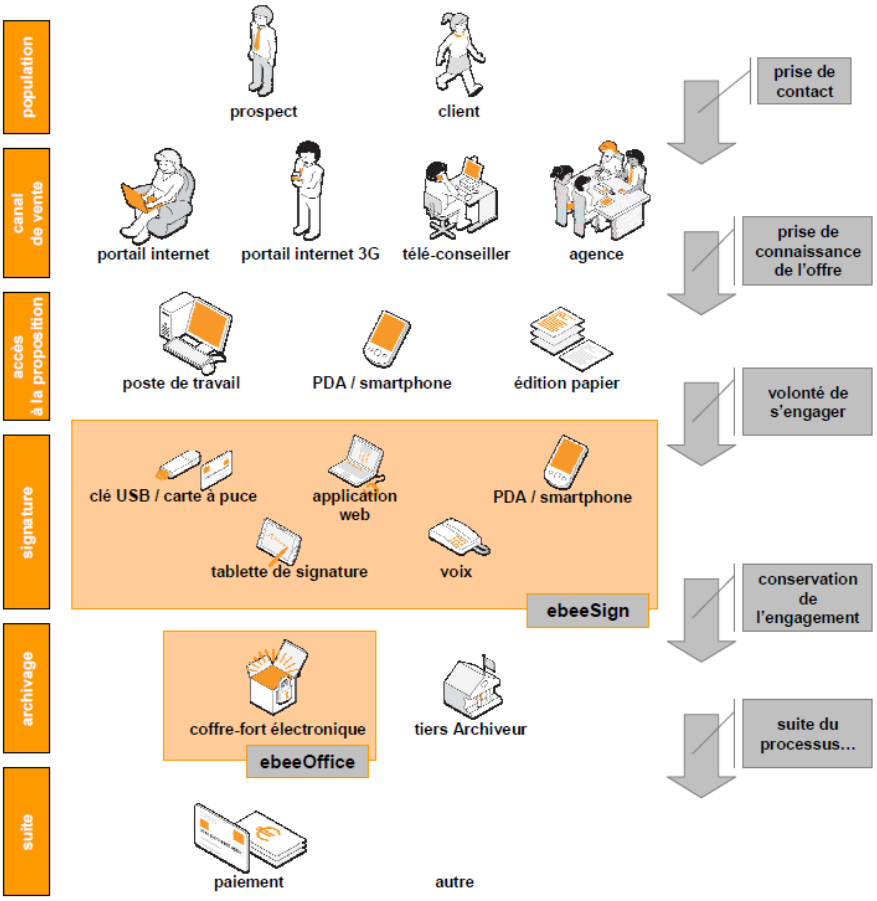


Figure 1 - Illustration du principe de contractualisation multicanal

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

Public

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

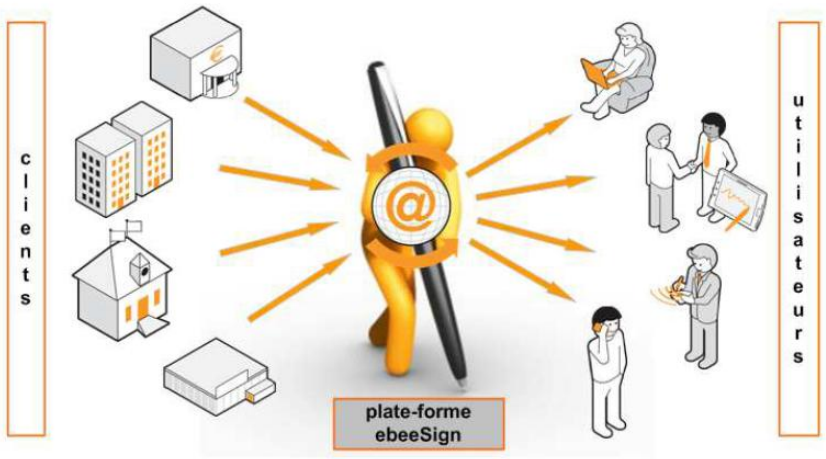


Figure 2 Les Clients et les Utilisateurs du Service de signature électronique du Prestataire

Certificats de cachet pour les organisations et d'unité d'horodatage
Dans le cadre de ce Service, le Client dispose d'un certificat de signature cachet : ○ Identifié par l'OID 1.3.6.1.4.1.48620.41.1.7.3.2.4.1 pour les certificats cachet signature ○ Identifié par l'OID 1.3.6.1.4.1.48620.41.1.7.3.2.5.1 pour les certificats cachet horodatage et objet de la présente PC qui sera utilisé par les composants du service de signature cachet électronique pour apposer une signature numérique de type cachet de signature ou d'horodatage sur les documents présentés aux Utilisateurs dans le cadre de transactions de contractualisation et de signature.

1.2 Identification du document

Ce document est la PC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » de l'Infrastructure de Gestion de Clés (IGC) du Prestataire pour les certificats de signature et d'authentification de personne physique.

Son identifiant d'objet (OID) est le suivant : 1.3.6.1.4.1.48620.41.1.7.3.2.

Cette référence figure dans l'ensemble des Certificats de signature de personne physique et de cachets émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » (pour de plus amples informations, se référer au paragraphe ***9.12.2***).

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de certification (AC)

L'***Autorité de Certification (AC)*** « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » a en charge la fourniture des prestations de gestion des Certificats de signature tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation) et est, à ce titre, identifiée dans ces Certificats en tant qu'émetteur.

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » appartient à la hiérarchie de confiance du Prestataire (ensemble des AC regroupées au sein de son IGC). A ce titre, la gestion de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ainsi que de l'AC Racine est assurée par le Prestataire.

1.3.2 Autorité de Gouvernance (AG)

L'Autorité de Gouvernance (***AG***) est l'autorité responsable de l'ensemble des services de l'IGC du Prestataire, elle a un pouvoir décisionnaire au sein de l'IGC. Elle définit et fait appliquer les PC et DPC.

Concrètement, il s'agit d'un ou plusieurs représentants du Prestataire ayant un mandat spécifique pour assurer cette fonction.

1.3.3 Service de stockage sécurisé des Bi-clés des Clients

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » met en œuvre un service de stockage sécurisé des Bi-clés des Clients.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Ce service n'est pas mis en place pour ce type de certificats.

Ce service est hébergé dans les locaux du Prestataire à accès très restreint et met en œuvre des modules cryptographiques matériels.

Certificats de cachet pour les organisations et d'unité d'horodatage
Le HSM répond aux exigences du standard FIPS 140-2 level 3, ou critères communs EAL4+. Chaque Client bénéficie : • D'une partition cryptographique qui est totalement dédiée au stockage de sa ou de ses Bi-clé(s) ; ou • D'un accès exclusif à ses clés cryptographiques Seule l'application de création de eSeal électronique, ou d'horodatage peut communiquer avec le Module cryptographique matériel pour une demande de signature cachet. À aucun moment la clé privée de signature du Client ne peut être exportée du Module. La création du Bi-clé Client a lieu lors d'une Cérémonie de Clés, et après validation de la demande du Représentant Client. L'activation du Bi-clé de création de eSeal d'un Client par l'application de signature n'est possible qu'après enregistrement sécurisé de l'application au niveau du Module cryptographique et ne peut se réaliser que sous le contrôle du Client. Le service de stockage sécurisé des Bi-clés des Clients assure que la clé privée ne peut être utilisée que pour la création de eSeal.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

1.3.4 Autorité d'Enregistrement (AE)

L'***Autorité d'enregistrement (AE)*** est un ensemble de ressources (informatiques et humaines).

1.3.4.1 Rôle de l'AE

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
L'AE a pour rôle de gérer les relations entre l'AC et les Porteurs de certificats. Dans le cadre de la présente PC, l'Autorité d'Enregistrement est : - Le Prestataire si le porteur est en relation directe avec ce dernier. Toutes les opérations sont alors réalisées par les équipes du Prestataire ; - Un Client du Prestataire (AE déléguée) qui souhaite délivrer à un porteur avec lequel il est en relation directe un certificat qualifié de signature, ou d'authentification émis par l'AC du Prestataire. A ce titre le Client est responsable, conformément aux clauses contractuelles entre le Prestataire et ses Clients, de réaliser les opérations de vérification de l'identité du demandeur et de délivrance du certificat et du support cryptographique au futur porteur.

Certificats de cachet pour les organisations et d'unité d'horodatage
L'AE a pour rôle de gérer les relations entre l'AC et les Clients, Porteurs de certificats. Dans le cas du Service de signature électronique, c'est le Prestataire qui est chargé de la relation avec les Clients, et de leur identification et authentification. Cependant, le Prestataire s'autorise dans le futur à mettre en place des AED pour les offres cachet.

1.3.4.2 Missions de l'AE

Dans tous les cas, l'AE assure :

- La prise en compte et la vérification des informations, notamment d'informations personnelles, présentées par le Porteur, et la constitution de son dossier d'enregistrement ;
- L'établissement et la transmission de la demande de Certificat à la fonction adéquate de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ;
- L'archivage des pièces du dossier d'enregistrement ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles du Porteur qui lui sont confiées, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

L'archivage du dossier peut se faire par l'envoi vers la composante chargée de l'archivage.

1.3.4.3 Niveau de garantie attendu

C'est l'AE qui détermine le niveau de garantie attendu dans le processus d'identification de ses Porteurs et elle en est responsable contractuellement.

A minima, le Prestataire exige de la part de ses Autorités d'Enregistrement que :

- La vérification de l'identité du demandeur d'un certificat se fasse selon l'un des procédés suivants :

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

- par la présence physique du futur Porteur, ou du représentant autorisé de la personne morale, devant l'AE, l'AED ou un Mandataire de Certification, sur la base de preuves et de procédures appropriées — les justificatifs recevables et les modalités de contrôle sont précisés au paragraphe 3.2.3.1 —, conformément au droit national et en conformité avec l'article 24, paragraphe 1 bis, du règlement (UE) n° 910/2014 modifié ;
- au moyen d'un certificat de signature électronique qualifiée ou d'un certificat de cachet électronique qualifié en cours de validité, dès lors que l'AE s'assure que ce certificat a été émis conformément à l'une des méthodes de vérification d'identité admises par l'article 24, paragraphe 1 bis, points a), c) ou d), du règlement (UE) n° 910/2014 modifié. Les Autorités de Certification acceptées à cet effet font l'objet d'une analyse préalable et sont inscrites sur une liste tenue à jour par le Prestataire.

- Les informations contenues dans le formulaire de demande de certificat soient validées en présence du futur porteur et soient conformes aux justificatifs fournis par le futur porteur ;
- Le formulaire de demande soit signé par le futur Porteur ;
- Le futur porteur prenne connaissance et signe les Conditions Générales d'Utilisation du certificat.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le Prestataire exige également de la part de ses Autorités d'Enregistrement que : • Le porteur accepte explicitement le certificat et le support cryptographique qui vient de lui être délivré.

Elle établit en conséquence les procédures nécessaires pour assurer ce niveau de garantie et s'assure de leur mise en œuvre opérationnelle.

L'AE s'engage également au maintien opérationnel des moyens qui sont mis à sa disposition pour transmettre les demandes de Certificats, et au respect des règles communes d'authentification et de contrôle des flux établies entre l'AE et l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

1.3.5 Autorités d'Enregistrement Déléguée (AED)

L'AED est une entité en relation contractuelle avec le Prestataire, et qui exerce la fonction d'AE (paragraphe 1.3.4 par délégation de l'AC du Prestataire). Dans ce document le terme AE s'applique également à une AED.

1.3.6 Client et Représentant Client

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le Client est l'entité cliente du Prestataire ayant décidé de délivrer des certificats qualifiés de signature, et d'authentification émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », et qu'il délivre à ses propres clients. Le Client est contractuellement lié au Prestataire.

Certificats de cachet pour les organisations et d'unité d'horodatage
Le Client est l'entité cliente ayant décidé de souscrire au Service du Prestataire, qu'il utilise pour ses propres besoins ou qu'il met à disposition des Utilisateurs. Le Client, Porteur du Certificat, est représenté par une personne physique mandatée à le représenter : le Représentant Client (RC). Le RC est une personne physique qui est responsable de l'utilisation du Certificat de signature de personne morale (Certificat de type cachet) pour le service identifié dans le Certificat et de la clé privée correspondant à

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

ce Certificat, pour le compte de l'entité également identifiée dans ce Certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RC peut être le représentant légal de l'entité ou une personne dûment désignée par ce dernier. Cette désignation doit faire l'objet d'un mandat écrit et signé, dans lequel le représentant légal délègue explicitement à une personne physique les responsabilités liées, en tout ou partie, à la demande, à l'acceptation, à l'usage et à la révocation des certificats.

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

Il est à noter que le certificat étant attaché à un service et non au RC, ce dernier peut être amené à changer en cours de validité du Certificat : départ du RC de l'entité cliente, changement d'affectation et de responsabilités au sein de l'entité, etc.

Le Client doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur. L'AC peut être amenée à révoquer un certificat de signature de personne morale pour lequel il n'y a plus de RC explicitement identifié.

Dans le cas de certificats d'horodatage du Prestataire, le RC est une personne physique liée au Prestaire.

1.3.7 Le Porteur de Certificat

Le porteur est l'utilisateur final à qui l'AE a remis un certificat électronique après contrôle d'identité et vérification de son dossier.

Le porteur est une personne physique qui est :

- Soit un client unitaire du Prestataire ;
- Soit un client d'un des Clients du Prestataire.

Suivant les cas les Porteurs peuvent faire des demandes de certificats :

- Dans le contexte de leurs activités professionnelles, il s'agit dans ce cas d'une demande de certificat entreprise. Le certificat fait apparaître dans le champ « Subject » ses informations d'identité et ses informations d'entreprise ;
- Dans le contexte personnel, il s'agit dans ce cas d'une demande de certificat particulier. Le certificat fait apparaître dans le champ « Subject » les seules informations d'identité.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le certificat est remis sous la forme d'un support cryptographique détenu par le porteur.

1.3.8 Applications utilisatrices des certificats

Une application utilisatrice de certificat est une application qui souhaite :

- Soit établir une signature électronique ;
- Soit vérifier une signature électronique.

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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

L'application utilisatrice peut également authentifier électroniquement le porteur du certificat.

Les applications peuvent être notamment :

- Le service de vérification de signature du Prestataire ou d'un partenaire du Prestataire qui permet à partir d'une information ou d'un document signé à l'aide d'un certificat émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », de vérifier et d'afficher un statut sur l'état du certificat utilisé et de la signature ;
- L'application Acrobat Reader™ d'Adobe™ qui permet d'afficher un document au format PDF signé par un certificat émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », ainsi que le cartouche d'information sur les signatures associées au document. Cette application doit être correctement configurée pour accepter les certificats de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

En plus de ces applications communes, les applications spécifiques suivantes sont identifiées :

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le portail d'authentification du Prestataire ou de ses clients, dans le cadre de l'accès de l'utilisateur à un des services de dématérialisation proposé par le Prestataire ou un de ses clients ou partenaires.

Certificats de cachet pour les organisations et d'unité d'horodatage
Le service d'horodatage du Prestataire qui met en œuvre des certificats sur les unités d'horodatage.

1.3.9 Autres participants

1.3.9.1 L'Opérateur de Service de Certification (OSC)

La fonction d'Opérateur de Service de Certification est assurée, pour le compte du Prestataire, par la société be ys Trusted Solutions France, sous-traitant de BE INVEST International S.A., dans le cadre d'un contrat qui définit les responsabilités des parties et les niveaux de service attendus. BE INVEST International S.A. demeure responsable, à l'égard des Porteurs, des parties utilisatrices et de l'organe de contrôle, de l'ensemble des activités ainsi confiées.

L'Opérateur du Service de Certification est chez le Prestataire, il a la charge de :

- Définir l'infrastructure technique de l'IGC ;
- Assurer le paramétrage et l'administration des composants ;
- Assurer l'exploitation, le maintien en condition opérationnelle et la supervision des composants.

1.3.9.2 Le Mandataire de Certification

Le recours à un Mandataire de Certification (MC) n'est pas obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC.

Dans le cas où l'AE y a recours, le MC doit être formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'IGC.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicable

1.4.1.1 Bi-clés et Certificats des Clients

Les domaines d'utilisation de certificat sont variables suivant la typologie :

Les certificats émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » 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 conforme à la norme EN 319 411-2 QCP-n-qscd, utilisés par Service de signature électronique du Prestataire, grâce auquel l'Utilisateur peut signer les formulaires ou documents présentés par le Client, générant ainsi une signature qualifiée.

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 de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ne peuvent être utilisés que :

- Pour la signature de Certificats finaux ;
- Pour la signature de Certificats de cachet et d'unité d'horodatage ;
- De certificats de répondeurs OCSP et de LCR.

1.4.2 Domaines d'utilisation interdits

Toutes les autres utilisations des certificats émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ne sont pas couverts par la présente PC.

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

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

L'entité en charge de l'administration et de la gestion de la politique de certification est l'AG.

L'AG est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.

A cette fin, elle met en œuvre et coordonne une organisation dédiée, qui statue à échéance régulière, sur la nécessité d'apporter des modifications à la PC.

1.5.2 Point de contact

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

Autorité de Gouvernance IGC be-ys

Adresse électronique	Adresse postale
gouvernance.igc@be-ys.com	BE INVEST International S.A. 17 rue Léon Laval L-3372 Leudelange G.D. de Luxembourg

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

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

Un document interne précise, au sein de l'organisation du Prestataire, l'entité qui assure cette responsabilité.

1.5.4 Procédure d'approbation de la conformité de la DPC

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

L'AG est responsable de la gestion (mise à jour et révisions) de la DPC.

Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place.

L'AG est responsable de la mise en œuvre des pratiques décrites dans la DPC.

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Terme	Définition
	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 à 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), 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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Terme	Définition
	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)
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)

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Terme	Définition
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. § ***1.3.7***)
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
Utilisateur	Voir « Application utilisatrice »

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

2.1 Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des Clients et des Applications utilisatrices de certificats et des Porteurs, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats.

La mise à disposition des informations sur l'état des certificats se base sur un mécanisme de LCR (Liste de Certificats Révoqués) accessible via un lien HTTP. Les adresses de publication sont fournies dans le paragraphe ***7*** « ***Profils des certificats, OCSP et des LCR*** ».

2.2 Informations devant être publiées

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » diffuse sur son site http://pki.almerys.com les informations suivantes :

- La présente PC, qui contient en particulier les profils de certificat et de LCR, les délais et fréquences de publication, le glossaire qui contient les acronymes et les définitions applicables, les adresses principales de diffusion) ;
- Les certificats en cours de validité des AC de la hiérarchie de rattachement de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », les différentes PC correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine ;
- La LCR et la LAR correspondantes ;
- Les conditions générales d'utilisation des Certificats.

Ce site est disponible **24h/24 et 7J/7**.

Ces informations sont disponibles sur le site web dédié à l'infrastructure de confiance : http://pki.almerys.com/

2.3 Délais et fréquences de publication

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

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

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

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est du niveau de confidentialité « Public ».

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et aux personnes dûment autorisées après authentification par un moyen d'authentification forte.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Type de noms

Les noms utilisés dans les Certificats émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » sont conformes aux spécifications de la norme X.500.

Dans chaque Certificat X.509v3, l'AC émettrice (issuer) et le Client, le service et/ou le Porteur (subject) sont identifiés par un « Distinguished Name » DN dont le format est précisé dans le paragraphe ***7*** « ***Profils des certificats, OCSP et des LCR*** » de ce présent document.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner le porteur de certificat sont, quel que soit le cas, toujours explicite.

Les informations d'identité du Porteur ou de l'Organisation sont explicites et correspondent aux éléments présentés sur le justificatif d'identité du Porteur ou de l'organisation fourni au moment de la demande de certificat. En particulier :

- l'attribut O du champ « subject DN » contient la raison sociale du Client ;
- le premier attribut OU contient le numéro d'enregistrement SIREN/SIRET en France (ou en dehors de la France, de son équivalent reconnu par les autorités compétentes du pays du client) assurant l'unicité de la référence Client ;
- L'attribut OI contient le numéro d'enregistrement du client dans un référentiel reconnu (par exemple, le numéro d'enregistrement SIREN/SIRET, ou numéro de TVA intra-communautaire).

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le champ CN contient le prénom et le nom. Le champ SerialNumber contient un identifiant unique qui correspond à une référence du Porteur vis-à-vis du Prestataire. Le champ « givenName » (G) contient le premier prénom, le prénom d'usage, ou les prénoms de l'état civil du porteur. Le champ « surname » (SN) contient le nom de l'état civil ou le nom d'usage du porteur.

Certificats de cachet pour les organisations et d'unité d'horodatage
De plus, l'attribut CN du champ « subject » (DN) du Client identifie le service du Client pour lequel le certificat va être utilisé.

Le format exact du « Subject » (DN) des Certificats des Porteurs est précisé dans le paragraphe ***7*** de ce présent document décrivant le profil des certificats et des LCR.

3.1.3 Anonymisation ou pseudonymisation des Clients Type de noms

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

3.1.4 Règles d'interprétation des différentes formes de nom

Les règles d'interprétation des différentes formes de nom sont explicitées dans le paragraphe ***7*** de ce présent document décrivant le profil des Certificats et des LCR.

3.1.5 Unicité des noms

Le Prestataire maintient un référentiel identifiant de manière unitaire chacun des Porteurs de Certificats émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

Cet identifiant fait partie intégrante du DN d'un certificat Porteur et est positionné dans le champ « SerialNumber ».

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
L'identifiant est généré par l'AC et le Prestataire garantit que cet identifiant ne peut être attribué à un autre Porteur. A noter que l'unicité d'un Certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au Certificat et non pas au Client et ne permet donc pas d'assurer une continuité de l'identification dans les Certificats successifs d'un Client donné.

Certificats de cachet pour les organisations et d'unité d'horodatage
L'identifiant est une référence unique inscrite dans les attributs CN et « Organisation Identifier= <NTRFR><SIREN> » du champ subject DN. Durant toute la durée de vie de l'AC, un DN attribué à un client ne peut être attribué à un autre client. Des précisions sont fournies, dans la DPC associée à cette PC, répondant à cette exigence en respectant les spécifications sur le DN définies dans les profils de Certificats (conformément au paragraphe ***7***). A noter que l'unicité d'un Certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au Certificat et non pas au Client et ne permet donc pas d'assurer une continuité de l'identification dans les Certificats successifs d'un Client donné.

3.1.6 Identification, authentification et rôle des marques déposées

L'AE s'assurera avec un soin raisonnable de la pertinence des noms et marques déposées apparaissant dans une demande de certificat.

En particulier, l'AE vérifiera notamment les informations liées à l'entreprise dans le cas d'un certificat « entreprise » ou « cachet ».

En cas de litige sur l'interprétation de ces paramètres, une résolution amiable des conflits est privilégiée.

3.2 Validation initiale de l'identité

L'enregistrement d'une demande de certificat se fait directement par l'AE. La vérification d'identité du futur Porteur s'effectue obligatoirement selon l'un des procédés suivants :

- Par la présence physique du futur Porteur, ou du représentant autorisé de la personne morale, devant l'autorité d'enregistrement (AE ou AED) ou un Mandataire de Certification, sur la base de preuves et de procédures appropriées — les justificatifs recevables et les modalités de contrôle sont précisés au paragraphe 3.2.3.1 —, conformément au droit national et en conformité avec l'article 24, paragraphe 1 bis, du règlement (UE) n° 910/2014 modifié ;

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

- Au moyen d'un certificat de signature électronique qualifiée ou d'un certificat de cachet électronique qualifié en cours de validité, dès lors que l'AE s'assure que ce certificat a été émis conformément à l'une des méthodes de vérification d'identité admises par l'article 24, paragraphe 1 bis, points a), c) ou d), du règlement (UE) n° 910/2014 modifié.

Ces méthodes sont mises en œuvre conformément aux actes d'exécution adoptés en application de l'article 24, paragraphe 1 quater, du règlement (UE) n° 910/2014, tel que modifié, lesquels désignent la norme ETSI TS 119 461 comme norme de référence.

La fonction d'autorité d'enregistrement est exercée par BE INVEST International S.A. au travers de son établissement stable situé en France, opérant sous la dénomination commerciale « Be Ys Corporation France ». Cet établissement est dépourvu de personnalité juridique propre : BE INVEST International S.A. demeure la seule entité juridiquement responsable à l'égard des Porteurs, des parties utilisatrices et de l'organe de contrôle.

Le Mandataire de Certification doit être préalablement enregistré par l'AE, conformément au paragraphe ***3.2.3.4.1*** « ***Enregistrement d'un Mandataire de Certification*** ».

L'AE doit être de confiance et authentifié par l'AC, en particulier, le Prestataire s'assure que les autorités d'enregistrement mettent en place les mesures de sécurité nécessaires.

Les modalités pratiques de validation de l'identité du Porteur ou du Client sont déterminées par le Prestataire et font partie, dans le cas de l'AED, du contrat avec le Client.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

3.2.1 Méthode pour prouver la possession de la clé privée

Selon la typologie de certificat, la méthode pour prouver la possession de la clé privée varie :

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
La clé privée du Porteur est générée lors de la phase de personnalisation du support cryptographique du Porteur avant la remise de ce support. Cette opération de personnalisation intervient qu'après validation par l'AE de la demande de certificat, c'est-à-dire à la suite des étapes de vérification du contenu de la demande. A la fin de l'étape de personnalisation, un code aléatoire est généré pour permettre l'activation de la clé privée. Le processus de remise de ce code garantit que seul le Porteur en a connaissance.

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

3.2.2 Validation de l'identité d'un organisme

La validation 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

La méthode de validation d'un individu dépend de la typologie du certificat.

La vérification de l'identité du demandeur d'un certificat qualifié est réalisée par le Prestataire ou par l'intermédiaire d'un tiers, sur la base de l'une des méthodes suivantes, ou, lorsque nécessaire, d'une combinaison de celles-ci :

- au moyen d'un certificat de signature électronique qualifiée ou d'un certificat de cachet électronique qualifié, émis conformément aux méthodes admises par l'article 24, paragraphe 1 bis, du règlement modifié (UE) n° 910/2014 ;
- par la présence physique de la personne physique, ou du représentant autorisé de la personne morale, sur la base de preuves et de procédures appropriées, conformément au droit national et en conformité avec l'article 24, paragraphe 1 bis, du règlement modifié (UE) n° 910/2014.

Le Demandeur peut être :

- Le porteur lui-même dans le cas d'un certificat de personne physique ;
- Le représentant client dans le cas d'un certificat de cachet.

3.2.3.1 Enregistrement d'un Porteur « Personne Physique »

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

La vérification de l'identité d'un Porteur peut être réalisée au moyen d'un certificat de signature électronique qualifiée en cours de validité, dès lors que la signature apposée sur la demande de certificat est valablement vérifiée et que l'Autorité d'Enregistrement s'assure que le certificat qualifié utilisé a été émis conformément à l'une des méthodes de vérification d'identité admises par l'article 24, paragraphe 1 bis, points (a), (c) ou (d), du règlement (UE) n° 910/2014.

Dans tous les autres cas, la validation de l'identité d'un Porteur pour l'obtention d'un certificat « particulier » se base sur les informations et la photo contenue sur le justificatif d'identité présenté par le Porteur. Les justificatifs recevables sont la Carte Nationale d'Identité, un Passeport ou un Permis de séjour. Les documents présentés doivent être en cours de validité au moment de la demande.

Les informations également nécessaires pour procéder à une demande de certificat de ce type sont :

- Nom prénom du porteur ;
- Le lieu de naissance du Porteur ;
- La date de naissance du Porteur ;
- Une adresse électronique et un numéro de téléphone portable, et éventuellement une adresse postale ;
- Si applicable l'attribut du porteur.

Le Porteur doit également prendre connaissance et accepter en apposant sa signature les Conditions Générales d'Utilisation. 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 »

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
En sus des éléments identifiés au paragraphe ***3.2.3.1***, un Porteur souhaitant obtenir un certificat « entreprise » devra fournir une pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci. La demande de certificat d'entreprise doit être co-signée par le représentant légal. Le certificat de cachet est destiné à être utilisé par une personne morale. Toutefois, le porteur technique (utilisateur effectif de la clé privée) peut être une personne physique désignée par la personne morale. Cette personne physique, appelée "Représentant Client", agit en vertu d'un mandat formel établi par le représentant légal, selon les modalités définies en section 3.2.5.

3.2.3.3 Enregistrement d'un Client

Certificats de cachet pour les organisations et d'unité d'horodatage
L'AE demande une preuve de l'habilitation du RC à demander un certificat pour l'entité morale qu'il représente, sauf si le RC est le représentant légal de l'entité cliente.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

- Toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro d'identification de l'entreprise figurant dans le certificat (par exemple, SIREN en France ou numéro de TVA intracommunautaire) ;
- Tout document attestant de la qualité du signataire de la demande de certificat, un document officiel d'identité en cours de validité du représentant de l'entité cliente comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie ;
- Le numéro de téléphone mobile du RC, l'adresse postale et/ou l'adresse électronique permettant à l'AC de contacter le RC ;
- Les conditions générales d'utilisation des certificats signées.

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

3.2.3.4 Mandataire de Certification

3.2.3.4.1 Enregistrement d'un Mandataire de Certification

L'enregistrement du MC se fait par l'envoi d'un dossier d'enregistrement à l'AE.

Le dossier d'enregistrement, d'un MC, comprend :

- Une demande de Mandataire de Certification signé, par un représentant légal de l'entité désignant le MC. Ce mandat doit être signé également par le MC ;
- Un engagement signé du MC, de respecter et de faire respecter l'ensemble des dispositions contractuelles, décrivant la mission du MC, et notamment son engagement à signaler sans délais à l'AE son départ de l'entité ;
- Un justificatif d'existence de l'entreprise portant le numéro SIREN de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou répertoire des métiers) ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
- Une copie du justificatif d'identité du MC ;
- Une copie du justificatif d'identité du RL.

3.2.3.4.2 Mandataire de Certification

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques entreprise
La validation de l'identité d'un Porteur par le MC s'effectue selon les paragraphes ***3.2.3.1*** et ***3.2.3.2***.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Le MC doit déposer auprès de l'AE : • Une demande de certificat avec toutes les informations nécessaires selon les paragraphes ***3.2.3.1*** et ***3.2.3.2*** ; • Les pièces justificatives de l'identité du Porteur : une photocopie d'un justificatif d'identité du Porteur ; • Les CGU certificats signé par le porteur ; • Les pièces justificatives de l'entité (Entreprise) de rattachement du porteur si différente de celle du MC (dans le cas où le MC est mandaté par le RL d'un groupe, alors que le porteur est rattaché à une filiale par exemple) ; • Tout document attestant de la qualité de Représentant légal de l'entreprise, et son justificatif d'identité si l'entreprise est différente de celle du MC.

3.2.4 Informations non vérifiées du Porteur

Sans objet dans le cadre de la présente PC.

3.2.5 Validation de l'autorité du demandeur

Dans tous les cas, l'AE valide au préalable que le demandeur est bien un de ses clients. De plus, l'AE s'assure que le demandeur est bien :

- Le futur porteur ou une personne mandatée par celle-ci dans le cas des certificats de personnes physiques ;
- Le représentant client dans le cas d'un certificat de cachet.

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

Si le demandeur n'est pas le représentant légal de l'organisation, un mandat signé par celui-ci doit être fourni, accompagné d'une copie de pièce d'identité du mandant et du mandataire. L'Autorité d'Enregistrement vérifie l'authenticité du mandat et la capacité du représentant légal à engager l'entité. Le mandat est établi pour une période donnée et peut être utilisé pour plusieurs certificats.

3.2.6 Critères d'intéropérabilité

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

3.3 Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la Bi-clé de signature ou d'authentification d'un Client entraîne automatiquement la génération et la fourniture d'un nouveau Certificat de signature et d'une nouvelle bi-clé.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
L'ancienne carte du porteur est détruite.

La vérification de l'identité dans le cadre d'un renouvellement de clés est la même que lors de l'enregistrement initial. Un nouveau Certificat ne peut pas être fourni au Client sans renouvellement de la bi-clé correspondante (conformément au paragraphe ***4.6*** « ***Renouvellement d'un certificat*** » présent dans ce présent document).

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

3.3.1 Identification et validation pour un renouvellement courant

Lors des renouvellements, l'AE doit identifier le Client selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent. Un nouveau dossier de demande de certificat est alors mis en œuvre.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Un nouveau support cryptographique sera remis au Porteur.

3.3.2 Identification et validation pour un renouvellement des clés après révocation

Lors des renouvellements, l'AE doit identifier le Client selon la même procédure que pour l'enregistrement initial, un nouveau dossier de demande de certificat est alors mis en œuvre et un nouveau support cryptographique sera remis au Porteur.

3.4 Identification et validation d'une demande de révocation

Les personnes autorisées à faire une demande de révocation de certificat sont :

- Le Porteur ou le demandeur de certificat ;
- L'AE ou l'AED ;
- Le MC ;
- Le centre de support ;
- L'AC ou l'AG.

Certificats de cachet pour les organisations et d'unité d'horodatage
La demande peut être réalisée: • Soit par le Client du service ; • Soit par le responsable du service.

En cas de révocation d'urgence, le porteur ou le demandeur du certificat peut demander la révocation de son certificat en contactant par téléphone le service de gestion des demandes de révocation d'urgence disponible 24H/24 et 7j/7 et suivre la procédure associée, tels qu'indiqué sur la page web publique http://pki.beys.com/revoquer.html ou http://pki.almerys.com/revoquer.html.

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

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le Porteur ou demandeur du certificat ne peut pas accéder aux services de révocation directement. Lorsqu'il souhaite procéder à la révocation de son certificat, il doit : • Soit contacter l'AE en se rendant auprès de son agence, ou par téléphone. Dans ce cas l'AE identifiera le Porteur en utilisant une authentification fiable (par exemple utilisation d'un code fourni lors de la création du certificat) ou bien révoquera d'elle–même le certificat concerné ; • Soit contacter le service téléphonique de révocation d'urgence. Dans ce cas le service téléphonique identifiera le Porteur avant de procéder à la révocation du certificat.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

3.4.2 Demande faite par l'Autorité d'Enregistrement

Lorsque l'AE (ou AED) doit traiter la demande de révocation, elle peut :

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

3.4.2.1 Demande faite par un Mandataire de Certification

Dans le cas d'une demande de révocation effectuée par un MC, le MC peut contacter l'AE pour la révocation du porteur, ou révoquer de son propre chef le certificat concerné.

3.4.3 Demande faite par le centre de support

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
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 ; • Soit transmettre la demande de révocation à l'AE correspondante (conformément au paragraphe ***3.4.2***).

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

3.4.4 Par le responsable du Service

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

Certificats de cachet pour les organisations et d'unité d'horodatage
Si un Client ne souhaite plus faire appel au Service proposé par le Prestataire et met fin à la relation contractuelle établie entre lui et le Prestataire, le responsable du Service est habilité à demander la révocation des Certificats émis au nom de ce Client ou s'assurer qu'aucune requête de signature ne sera plus acceptée par le Service pour l'un quelconque de ces Certificats.

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

En cas d'urgence, l'AC ou l'AG peut procéder à la révocation d'un certificat.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Un certificat ne peut être demandé que par le futur Porteur du certificat en tant que : • Client direct du Prestataire ; • Client d'un Client du Prestataire ayant souscrit à une offre du Prestataire. Dans le cas d'un certificat « entreprise » la demande de certificat doit être signée par le représentant de l'entreprise à laquelle le porteur est affilié.

Certificats de cachet pour les organisations et d'unité d'horodatage
Un certificat ne peut être demandé que par un RC dûment mandaté, ou le représentant légal de l'entité cliente.

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

Le Demandeur est garant des informations et des justificatifs qu'il fournit à l'AE qui :

- Complète le formulaire de demande en présence du Demandeur ;
- Valide les justificatifs présentés (conformément au paragraphe ***3.2.3.3)*** ;
- Fait signer le formulaire de demande et les Conditions Générales d'Utilisation au Demandeur ;
- Valide la demande et déclenche les opérations techniques de demande de certificat.

Des précisions sont fournies dans la DPC associée à la présente PC.

4.2 Traitement d'une demande de certificat

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

L'AE doit valider l'identité du Porteur ou du RC en s'assurant de la cohérence des justificatifs présentés. Elle vérifie notamment que les pièces présentées sont bien en cours de validité.

4.2.2 Acceptation ou rejet de la demande

Tant que le formulaire de demande n'est pas validé par l'AE, il est possible de modifier la saisie. La validation du formulaire intervient nécessairement après le processus d'identification et de validation de la demande.

Tant que le formulaire de demande n'est pas validé par l'AE, aucune demande de certificat n'est déclenchée.

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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

4.2.3 Durée d'établissement du certificat

Une fois que le formulaire de demande est validé par l'AE, la phase de personnalisation du support cryptographique ou de génération par le service de stockage sécurisé des Bi-clés est déclenchée et amène à la délivrance du certificat. Cette phase s'effectue par l'AE.

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

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

La phase de personnalisation du support cryptographique ou de création de la bi-clé par le service de stockage sécurisé de Bi-clés et l'association du moyen d'authentification consiste pour l'AE à :

- Se connecter sur les interfaces de gestion des supports cryptographiques ;
- Déclencher les opérations de demande de certificat auprès de l'IGC.

Les phases suivantes sont alors automatiques et consistent à :

- Générer une bi-clé sur le support cryptographique ou dans le service de stockage sécurisé de Bi-clés ;
- Générer une demande de certificat transmise auprès de l'IGC ;
- Génération du certificat par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ;
- Installer le certificat sur le support cryptographique ou dans le service de stockage sécurisé de Bi-clés.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
En parallèle un code d'activation est généré pour permettre l'accès à la clé privée du support cryptographique et ce code est transmis selon le cas : • Sur un support papier sécurisé ; • Par SMS. Dans tous les cas le Porteur peut modifier ce code.

Certificats de cachet pour les organisations et d'unité d'horodatage
Pour donner suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche le processus de génération de la Bi-Clé et du Certificat du Client lors de la KC Client. Le RC, un autre représentant dûment mandaté par le Client, ou un huissier assiste à la KC Client et s'assure du bon déroulement de la KC Client. La durée du Certificat est de 3 ans. Le paragraphe ***7.1*** « ***Profil du certificat de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2*** » détaille le format utilisé par l'AC pour les certificats.

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'AE remet lors du face à face le support cryptographique au Porteur.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de cachet pour les organisations et d'unité d'horodatage
L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » renvoie à l'AE et au Client du Service un statut sur l'opération de génération du Bi-clé et du Certificat Client. La DPC associée à la présente PC précise les différentes informations qui sont mises à disposition.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Lors de la remise du support au Porteur, ce dernier doit signer un procès-verbal de réception du support cryptographique. Ce procès-verbal est conservé par l'AE puis transmis à l'AC.

Certificats de cachet pour les organisations et d'unité d'horodatage
L'acceptation du Client a lieu : • Lors de la KC Client (en cas de présence du RC ou du représentant légal) : o Une fois le Certificat créé, le profil et les propriétés du Certificat sont validés par le RC, son représentant en séance. Cette validation est enregistrée dans le script de déroulement de la KC Client ; o Le Certificat et une copie du script de la KC sont remis au RC à l'issue de la KC ce qui vaut acceptation finale du certificat et valide le bon déroulement de la KC Client. • Après transmission du PV du script de la KC par lettre recommandée au client (en cas d'absence du RC ou du représentant légal le jour de la KC). o Une fois le Certificat créé, le profil et les propriétés du Certificat sont validés par huissier dans le script de la KC ; o Le Certificat, et le PV du script de la KC sont envoyés au client. La non-contestation du client dans les deux semaines vaut acceptation finale du certificat et valide le bon déroulement de la KC Client.

4.4.2 Publication du certificat

Les certificats émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ne sont pas publiés.

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

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » informe l'AE concernée de la délivrance du certificat. L'information est transmise par courriel dans une boîte générique propre à l'AE.

4.5 Usages de la Bi-clés et du certificat

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

L'utilisation de la clé privée du Porteur et du Certificat associé est strictement limitée à celle décrite au paragraphe ***1.4***.

L'usage autorisé de la Bi-clé du Porteur et du Certificat associé est précisé dans le Certificat lui-même, via les extensions concernant les usages des clés (conformément au paragraphe ***7.2*** pour le détail du profil du Certificat).

Les Porteurs et Clients doivent respecter strictement les usages autorisés des Bi-clés et des Certificats. Dans le cas contraire, leur responsabilité serait engagée. D'une manière générale, tout usage non autorisé explicitement est interdit.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
L'utilisation d'un Certificat qualifié nécessite obligatoirement l'utilisation du support cryptographique remis par l'Autorité du Prestataire pour que la signature réalisée soit déclarée conforme au Règlement eIDAS.

Certificats de cachet pour les organisations et d'unité d'horodatage
La clé privée et le certificat ne peuvent être utilisés que pour la création de eSeal sous le contrôle du Client ou de l'application du Client.

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

L'utilisation de la clé publique et du certificat par les Applications utilisatrices du certificats appliquent les mêmes règles que celles décrites dans le précédent paragraphe ***4.5.1*** ainsi qu'aux paragraphes ***1.4*** « ***Usage des certificats*** » et ***1.3.8*** « ***Applications utilisatrices des certificats*** ».

Les applications utilisatrices de certificats doivent respecter strictement les usages autorisés des Certificats. Dans le cas contraire, leur responsabilité peut être engagée.

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

La clé privée de l'AC Racine est utilisée :

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

Le certificat de l'AC Racine est utilisé :

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

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

La clé privée de l'AC est utilisée :

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

Le certificat de l'AC est utilisé :

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

4.5.5 *Publication du certificat*

La clé privée d'un répondeur OCSP est utilisée pour signer les réponses OCSP, tout autre usage est interdit.

Le certificat d'un répondeur OCSP est utilisé par les utilisateurs pour vérifier l'origine et l'intégrité d'une réponse OCSP.

4.6 Renouvellement d'un certificat

Le renouvellement d'un Certificat – i.e. la délivrance d'un nouveau Certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations restant identiques au Certificat précédent (y compris la clé publique du porteur), cf. [RFC36 47] – n'est pas autorisé dans le cadre de la présente PC.

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

Un changement de Bi-clé peut être effectué à la suite d'une révocation du Certificat existant (conformément au paragraphe ***4.9*** « ***Révocation et suspension*** des certificats » présent dans ce présent document), ou lors de l'expiration du certificat du porteur.

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

Les Bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Par ailleurs, une Bi-clé et un Certificat peuvent être renouvelés par anticipation, à la suite de la révocation du Certificat du Porteur (conformément au paragraphe ***0*** «

Causes possibles d'une révocation »).

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

- Un certificat valide, arrivant prochainement à expiration ;
- Un certificat expiré ;
- Un certificat révoqué.

Le Porteur ou le RC est notifié de l'arrivée à expiration future de son certificat. Il est alors invité à se présenter auprès de son AE pour procéder à une nouvelle demande de certificat. L'obtention d'un nouveau certificat nécessite obligatoirement la constitution d'un nouveau dossier d'enregistrement.

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

La demande d'un nouveau certificat à la suite d'un changement de la Bi-clé applique les mêmes règles que celles décrites dans le 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 des clés*** ».

Les actions de l'AC sont les mêmes que celles décrites dans le paragraphe ***4.3*** « ***Délivrance du certificat*** ».

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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*** ».

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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 PC.

4.9 Révocation et suspension des certificats

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ne met pas en œuvre de processus de suspension de ses Certificats.

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de Porteur

Les circonstances suivantes peuvent être à l'origine de la révocation des Certificats du Porteur :

- Le Certificat est devenu obsolète à la suite d'un changement des données du Porteur ou du Client figurant dans le Certificat ;
- Les informations du Porteur (y compris son titre ou attribut) ou du Client figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le Certificat ;
- Les modalités applicables d'utilisation du Certificat n'ont pas été respectées par le Porteur ;
- Le Porteur, le Client du Prestataire, l'AE ou l'AC n'ont pas respecté leurs obligations découlant de la présente PC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier de demande de Certificat ;
- La clé privée du Porteur ou du Porteur est suspectée de compromission, est compromise, est perdue ou est volée ;
- Le Porteur ou une entité autorisée demande la révocation du Certificat (notamment dans le cas d'une destruction ou altération du support cryptographique du Porteur) ;
- Le Certificat de signature de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » est révoqué (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante) ;
- Eventuellement si aucune disposition particulière n'a été négociée entre le Prestataire et le client du Prestataire avant la fin de relation contractuelle / hiérarchique / réglementaire entre l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et le Client du Service – et donc avec ses Porteurs – et cela avant la fin de validité des certificats,
- Evénements (décès du représentant légal de l'entité cliente, cessation d'activité du Client, etc.) initialisés par le processus de gestion des identités et des droits d'accès.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Le certificat peut également être révoqué dans le cas suivant : le support cryptographique du porteur est perdu.

Certificats de cachet pour les organisations et d'unité d'horodatage
Le certificat peut également être révoqué dans les cas suivants : • Fin de relation contractuelle / hiérarchique / réglementaire entre l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et le Client du Service – et donc avec ses Utilisateurs – avant la fin de validité des certificats ; • Le remplacement d'un RC n'a pas été mis en œuvre par le Client.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ou l'AE en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau Certificat notamment), le Certificat concerné doit être révoqué.

4.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » pour la génération de Certificats et de LCR) :

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

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de Porteurs et cachet

La modification d'un certificat d'AC respecte les mêmes règles que celles décrites dans le paragraphe ***3.4*** « ***Identification et validation d'une demande de révocation*** ».

4.9.2.2 Certificat d'une composante de l'IGC

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

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

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat Porteur ou Cachet

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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*** ».

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

- L'identité du Porteur utilisée dans le Certificat (Raison sociale, SIREN, etc.) ;
- L'identification du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le Certificat à révoquer (n° de série, ...) ;
- La cause de révocation. Cette cause de révocation n'est pas inscrite dans la LCR mais peut être enregistrée dans la base de données du Service.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » révoque le support affecté au Porteur, ce qui entraîne la révocation automatique de tous les certificats du porteur.

Le certificat (son numéro de série) apparaît alors comme révoqué dans la LCR. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC (conformément au paragraphe ***4.9.9*** « ***Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats*** »). Opérationnellement, l'opération de révocation est décrite dans la DPC correspondante.

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du Certificat. Dans tous les cas, et quel que soit le demandeur de la révocation, le Porteur ou le RC est notifié.

L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du Certificat. Les causes de révocation des Certificats ne sont pas publiées.

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

La DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » précise les procédures à mettre en œuvre en cas de révocation d'un Certificat d'une composante de l'IGC.

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

4.9.4 Délai accordé pour formuler la demande de révocation

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

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

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

4.9.5.1 Révocation d'un certificat Porteur ou de Cachet

Par nature une demande de révocation doit être traitée en urgence.

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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Dans tous les cas les services support de cette fonction sont assurés 24h/24 et 7j/7 et le traitement de la demande de révocation est assurée durant les jours et les heures ouvrés.

Par défaut, l'AE s'engage à réaliser la révocation dans les 24 heures.

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

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

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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

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

4.9.7 Fréquence d'établissement des LCR

La fréquence d'établissement des LCR est au maximum de 24 heures (durée maximale pendant laquelle aucune révocation naturelle n'a eu lieu). La durée de validité est de 72 heures.

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

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

4.9.8 Délai maximum de publication d'une LCR

Une LCR est publiée dès sa génération et dans un délai maximum de 60 minutes.

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

Le Prestataire a mis en place un dispositif OCSP. L'adresse du système est précisée dans le profil des certificats émis. L'accès au service OCSP est disponible à la demande pour les professionnels via des VPN sur le SI du Prestataire, l'OCSP est également accessible via internet.

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

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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 PC.

4.9.12 Exigences spécifiques en cas de compromission de la clée privée

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

Pour les Certificats d'AC, outre les exigences présentées dans le paragraphe ***4.9.3.2*** « ***Révocation d'un certificat d'une composante de l'IGC*** », la révocation à la suite d'une compromission de la clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC.

4.9.13 Causes possibles d'une suspension

Sans objet dans le cadre de la présente PC.

4.9.14 Origine d'une demande de suspension

Sans objet dans le cadre de la présente PC.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet dans le cadre de la présente PC.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet dans le cadre de la présente PC.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC fournit aux Applications utilisatrices de certificats les moyens de vérifier et valider préalablement à son utilisation, le statut d'un certificat et de sa chaîne de certification, c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état des Certificats de l'ACR.

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

Le chapitre ***7*** « ***Profils des certificats, OCSP et des LCR*** » fournit les informations de format sur les LCR, ainsi que les URL de publication des LCR/LAR.

4.10.2 Disponibilité de la fonction

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

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

4.10.3 Dispositifs optionnels

Sans objet dans le cadre de la présente PC.

4.11 Fin de la relation entre le Porteur et l'AC

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

4.12 Séquestre de clé et recouvrement

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

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet dans le cadre de la présente PC.

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

Sans objet dans le cadre de la présente PC.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

Le Responsable de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » s'engage à mettre en œuvre et maintenir le niveau de sécurité physique exigé pour les locaux d'exploitation des composantes de l'IGC.

5.1.1 Situation géographique et contruction des sites

En fonction de la sensibilité des composants de l'IGC interne du Prestataire, les sites sont définis au niveau 1 de la politique de sécurité du Prestataire : impact vital (majeur pour l'entreprise).

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

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

Les mesures permettent également de respecter les engagements pris dans la PC ou dans les engagements contractuels avec les Clients du Prestataire, en matière de disponibilité des services.

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », les accès aux locaux sont contrôlés conformément au niveau de zonage des locaux de niveau 1 : « accès très restreint ».

Pour les fonctions de génération des Certificats, de génération des éléments secrets du Client, et de gestion des révocations, ainsi que toutes les fonctions identifiées comme critiques dans l'analyse de risques, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. De plus, le contrôle en entrée et en sortie est permanent en heures non ouvrées (HNO).

Chaque entrée et sortie dans la zone sécurisée fait l'objet d'une surveillance indépendante. Tout personnel non-autorisé doit obligatoirement être accompagné d'une personne autorisée. Chaque entrée et sortie fait l'objet d'une traçabilité.

Ces exigences sont également reportées contractuellement avec le Client, lorsque ce dernier est responsable de ces fonctions.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC définissent un périmètre de sécurité physique où sont installées ces machines. Tout local utilisé en commun entre la composante concernée et une autre composante (de ou hors de l'IGC) est en dehors de ce périmètre de sécurité.

L'ouverture de la porte est commandée par un système de contrôle d'accès.

Les AC Racines sont opérées dans un espace physiquement isolé des autres opérations. L'accès à cet espace doit permettre son accès qu'aux personnes autorisées à accéder aux clés de l'AC Racine.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » telles que fixées par leurs fournisseurs.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection mis en place par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » permettent de protéger son infrastructure contre les dégâts des eaux.

5.1.5 Prévention et protection incendie

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » met en place des moyens de protection et de lutte contre les incendies.

5.1.6 Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) utilisés au sein de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » sont traités et conservés conformément aux besoins de sécurité pour les actifs sensibles (en confidentialité, intégrité et disponibilité).

En particulier, les supports font l'objet de mesures contre les dommages, le vol, les accès non autorisés et l'obsolescence. Ces mesures s'appliquent durant toute la période de rétention du contenu de ces supports.

5.1.7 Mise hors service des supports

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

5.1.8 Sauvegardes hors site

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

Les sauvegardes sont testées régulièrement.

5.2 Mesures de sécurité procédurales

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

Les procédures et politiques de sécurité sont communiquées aux employés suivant le besoin d'en connaître.

Des procédures sont établies et appliquées pour toutes les opérations des personnels en rôle de confiance pouvant impacter la fourniture du service.

5.2.1 Rôles de confiance

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

- **Officier de Sécurité de l'IGC** *(PKI Security Officer)* est chargé de la mise en œuvre de la politique de sécurité de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ». Il gère les contrôles d'accès physiques aux équipements des systèmes de l'entité. Il est habilité à prendre connaissance des documents conservés, et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Responsable d'application** est chargé, au sein de la composante de l'IGC concernée, de la mise en œuvre des différentes PC et DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ». Sa responsabilité couvre l'ensemble des fonctions rendues par les applications et des performances correspondantes.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

- **Ingénieur système** est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'entité. Il assure l'administration technique des systèmes et des réseaux de l'entité. Il est également chargé des opérations de restauration.
- **Opérateur** au sein de la composante de l'IGC concernée réalise, dans le cadre de ses attributions, l'exploitation des applications pour les services délivrés par la composante de l'IGC.
- **Contrôleur** est une personne désignée qui a pour rôle de procéder à l'analyse des journaux et des incidents liés à l'IGC. Le contrôleur est indépendant des autres rôles de confiance.
- **Opérateur d'enregistrement** est une personne responsable pour vérifier les informations nécessaires à la délivrance d'un certificat et approuver les demandes de certificat.
- **Opérateur de révocation** est une personne responsable pour toutes les opérations de changement d'un statut de certificat.

5.2.2 Nombre de personnes requises par tâches

La DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.), en particulier, les personnes requises pour la cérémonie des clés.

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC fait vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants, notamment :

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

Ces contrôles sont décrits dans la DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et sont conformes à la Politique de Sécurité du Prestataire.

Les rôles d'opérateurs, d'administrateurs et de contrôleurs sont directement gérés par le Prestataire. Les administrateurs ont la charge de la gestion des comptes. Ils effectuent les modifications et/ou suppressions des accès sans délais.

Les opérations réalisées par les personnels en rôle de confiance sont tracées.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des services offerts.

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et sont conformes à la Politique de Sécurité du Prestataire.

Pour les différents rôles de confiance, il est recommandé qu'une même personne ne détienne pas plusieurs rôles et les cumuls suivants sont interdits :

- Contrôleur et tout rôle d'enregistrement ;
- Administrateur système/réseau et officier de sécurité.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.3 Validation initiale de l'identité d'une personne physique représentant une personne morale

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

5.3.1 Qualifications, compétences et habilitations requises

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

Le responsable de l'AC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de l'IGC, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC ainsi que des mesures de protection des données personnelles.

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » informe toute personne intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC ;
- Des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

Cette nomination est réalisée de façon formelle par le responsable de la sécurité de l'AC et est accepté par écrit par la personne nommée dans un rôle de confiance.

Les qualifications, compétences et habilitations requises pour la cérémonie des clés sont définies dans une procédure spécifique.

Les responsabilités des personnels dans les rôles de confiance sont attribuées de façon à séparer les rôles et responsabilité, éviter les conflits d'intérêt et réduire les opportunités de modification ou de mauvaise utilisation, volontaire ou involontaire, des systèmes de l'IGC.

Les accès et habilitation sont attribués et configurés suivant la politique du moindre privilège.

5.3.2 Procédures de vérification des antécédents

Les personnels amenés à travailler au sein d'une composante de l'IGC, et en fonction du contexte applicable, sont amenés à remettre une attestation sur l'honneur de non-condamnation, un extrait de casier judiciaire, ou un engagement de confidentialité.

Les personnes disposant d'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 aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, au sein de la composante de l'IGC dans laquelle il opère.

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, les procédures, l'organisation, etc. en fonction de la nature de ces évolutions.

De plus, la formation continue inclut une formation annuelle aux nouvelles menaces et aux procédures de sécurité appliquées.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.3.5 *Fréquence et séquence de rotation entre différentes attributions*

La présente PC ne prévoit pas d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

5.3.6 *Sansctions en cas d'actions non autorisées*

Le Prestataire applique des sanctions disciplinaires appropriées à tout membre du personnel qui contrevient aux politiques, procédures ou règles de sécurité applicables aux composantes de l'IGC et aux services couverts par la présente PC.

Ces sanctions s'inscrivent dans le cadre d'un processus disciplinaire formalisé, communiqué et maintenu, applicable aux violations des politiques de sécurité des réseaux et des systèmes d'information du Prestataire.

Ce processus disciplinaire :

a) prend en compte les exigences légales, réglementaires, statutaires, contractuelles et métier applicables ;

b) est porté à la connaissance des personnels concernés, selon leur rôle et leur niveau d'habilitation ;

c) définit les modalités de constatation, signalement, analyse, décision, escalade, traitement et traçabilité des manquements ;

d) garantit la mise en œuvre de mesures proportionnées à la gravité du manquement constaté ;

e) fait l'objet d'une revue à intervalles planifiés et est mis à jour en tant que de besoin, notamment en cas d'évolution légale ou réglementaire, ou de changement significatif dans les opérations ou les risques.

Les modalités opérationnelles de mise en œuvre de ce processus sont précisées dans la Politique de Sécurité du Prestataire et, le cas échéant, dans la DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

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

Le personnel des prestataires externes intervenant dans les locaux du Prestataire et/ou sur les composantes de l'IGC respecte également les exigences présentées dans le paragraphe ***5.3*** « ***Validation initiale de l'identité d'une personne physique représentant une personne morale*** ».

Ceci est traduit en clauses adéquates dans les contrats concernés avec les prestataires.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.3.8 Documentation fournie au personnel

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

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer des événements sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'événements à enregistrer

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

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

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

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs...).

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

- Réception d'une demande de Certificat (initiale et renouvellement) ;
- Validation d'une demande de certificat ;
- Evénements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...) ;
- Procès-verbal de remise d'un support cryptographique au Porteur ;
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

- Génération des Certificats des Porteurs ;
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR ;
- Evénements liés à la dissémination des certificats.

Chaque enregistrement d'un événement dans un journal contient lorsque cela est applicable les champs suivants :

- Type de l'événement ;
- Nom de l'exécutant ou référence du système déclenchant l'événement ;
- Date et heure de l'événement ;
- Résultat de l'événement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements.

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

- Dans la mesure du possible : demandeur et destinataire de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'événement ;
- Toute information caractérisant l'événement (par exemple, pour la génération d'un Certificat, le numéro de série de ce Certificat).

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

5.4.2 Fréquence de traitement des journaux d'événements

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

5.4.3 Période de conservation des journaux d'événements

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

5.4.4 Protection des journaux d'événements

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

Les composants de l'IGC mettent en œuvre un procédé de chaînage puis de scellement pour garantir l'exhaustivité et l'intégrité de ces éléments.

5.4.5 Procédure de sauvegarde des journaux d'événements

Tous les événements sont écrits en base de données et font l'objet des procédures de sauvegarde des infrastructures du Prestataire.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.4.6 *Système de collecte des journaux d'événements*

Tous les événements sont écrits de manière centralisée dans une base de données.

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

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

5.4.8 *Evaluation des vulnérabilités*

L'AC met en œuvre une gestion des vulnérabilités de systèmes de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » en conformité avec la Politique de Sécurité du Prestataire.

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

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

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

5.5 Archivage des données

5.5.1 *Types de données à archiver*

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

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les agréments contractuels avec d'autres AC ;
- Les LCR tels qu'émises ou publiées ;
- Les récépissés ou notifications (à titre informatif) ;
- Les dossiers d'enregistrement des Porteurs et des RC.

5.5.2 *Période de conservation des archives*

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

- Personnel ;
- Trafic ;
- Connexion ;
- Facturation.

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

Les durées d'archivage sont les suivantes :

- PC = durée de vie de l'AC ;

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

- Documents organisationnels de cérémonies des clés = durée de vie de l'AC ;
- DPC = durée de vie de l'AC.

Les autres informations ci-dessous :

- Dossiers d'enregistrement des porteurs ;
- Certificats émis par l'AC ;
- Dernière LCR émis par l'AC après expiration ;
- Journaux d'événements.

Sont conservées pendant 7 ans après expiration des certificats. Le Prestataire a mis en place les mesures nécessaires pour que ces archives soient conservées sur les durées mentionnées même en cas d'arrêt d'activité.

5.5.3 Protection des archives

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

- Être protégées en intégrité ;
- Être accessibles aux personnes autorisées ;
- Pouvoir être relues et exploitées.

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

5.5.4 Procédure de sauvegarde des archives

La procédure est précisée dans la DPC. Le niveau de protection des sauvegardes est au moins équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

Les certificats sont datés au moment de leur génération et cette information est archivée avec le certificat correspondant. Le chapitre ***0*** « ***Horodatage / Système de*** datation », présent dans ce présent document, précise les exigences en matière de datation / horodatage.

5.5.6 Système de collecte des archives

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

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérables dans un délai inférieur à 2 jours ouvrés, étant noté que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

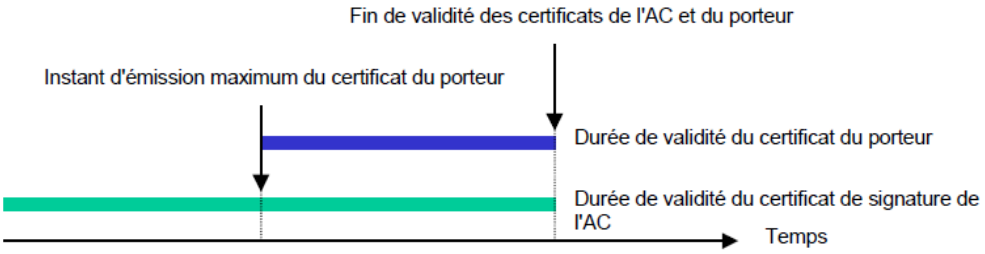
Les conditions de récupération des archives sont précisées dans la DPC.

5.6 Changement de clé d'AC

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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation



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

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission et sinistre

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

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

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », l'événement déclencheur est la constatation de cet incident. L'AG de l'IGC du Prestataire en est immédiatement informée. Le cas de l'incident majeur est impérativement traité dès la détection et la publication de l'information de révocation du Certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible.

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

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

Conformément à la Politique de Sécurité du Prestataire, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité de ses fonctions sensibles, et découlant :

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

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

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante de l'IGC du Prestataire est traité conformément au précédent paragraphe ***5.7.2*** « ***Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)*** ».

En particulier, en cas de compromission d'une clé d'AC, le Prestataire :

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

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

5.7.4 Capacités de continuité d'activités suite à un sinistre

Les différentes composantes de l'IGC du Prestataire disposent des moyens raisonnablement nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences décrites dans le paragraphe ***5.7.2*** « ***Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)*** » de la présente PC.

Le Prestataire dispose d'un plan de continuité d'activité à jour afin de réagir efficacement en cas de désastre et de restaurer le système dans les délais précisés dans ce plan. Ce plan comprend en particulier les cas de compromission de clé privée d'AC ou de perte des moyens d'activation de la clé.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC du Prestataire peut être amenée à cesser son activité en tout ou partie, ou à la transférer à une autre entité.

Le Prestataire a provisionné les moyens nécessaires en cas de cessation d'activité. Ces moyens sont décrits dans un plan d'arrêt d'activité tenu à jour par le Prestataire.

La compromission de la Bi-clé de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » entraîne immédiatement sa cessation d'activité et la révocation de tous les Certificats émis en cours de validité. Pour retrouver le niveau de service, la création d'une nouvelle AC et de nouveaux Certificats sont obligatoires.

5.8.1 Transfert d'activité ou cesstion d'activité affectant une composante de l'IGC du Prestataire

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » s'engage, entre autres obligations :

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

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » s'engage à respecter les points suivants :

1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des Clients ou des applications utilisatrices de certificats, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » doit les en aviser aussitôt que nécessaire et, au moins, sous le délai de 3 mois ;
2) L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » doit communiquer aux Clients et aux Porteurs les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » devra communiquer aux Clients et aux Porteurs les modalités des changements survenus. L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les Clients et les Porteurs ;
3) L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » doit tenir informés les Clients et autres entités de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

LePrestataires'engage à notifier l'organe de contrôle , ainsi que toutes les autorités pertinentes, en cas de fin de vie de l'IGC ainsi qu'à mettre l'information disponible pour des tiers utilisateurs des certificats.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.8.2 Cessation d'activité affectant l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 »

La cessation d'activité peut être totale ou partielle (*par exemple : cessation d'activité pour une famille de Certificats donnée seulement*). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC « « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », ou une entité tierce qui reprend les activités, lors de l'expiration du dernier Certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ou, en cas d'impossibilité, toute entité qui lui serait substituée par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assure la révocation des Certificats et la publication des LCR conformément aux engagements pris dans sa PC.

Lors de l'arrêt du Service, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » :

1) Révoque tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;
2) Informe (*par exemple par récépissé*) tous les Porteurs des certificats révoqués ou à révoquer ;
3) Détruit la clé privée lui ayant permis d'émettre des Certificats ainsi que toutes ces copies ;
4) Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
5) Révoque son Certificat ;
6) Transfert à un tiers l'obligation de disponibilité des informations publiée, en particulier de de sa clé publique.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique certifié Fips 140-2 Niveau 3 et également conformément au paragraphe ***6.2.1*** « ***Standards et mesures de sécurité pour les modules cryptographiques*** » présent dans ce présent document.

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

Le script de « Cérémonie des clés » indique :

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

La cérémonie se fait en présence :

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

La cérémonie fait l'objet d'un PV signé des participants attestant qu'elle s'est déroulée conformément à la procédure prévue et démontrant que l'intégrité et la confidentialité de la génération de la paire de clé a été assurée.

La génération des clés d'AC s'accompagne de la génération de différents secrets et éléments sensibles. Ces secrets sont des données permettant de gérer de manière sécurisée (personne ne peut posséder l'intégralité du secret), et ultérieurement à la Cérémonie des Clés, les opérations sur le HSM cryptographique, notamment, de pouvoir redémarrer, sauvegarder, et restaurer la sauvegarde de la partition HSM.

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

Le renouvellement du Certificat et des clés de l'AC suit les mêmes principes que ceux de la première génération des clés d'AC.

L'émission d'un certificat par l'AC Racine est réalisée obligatoirement par deux personnels autorisés disposant d'un rôle de confiance.

6.1.1.2 Clés des Porteurs et des Clients

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les clés des Porteurs sont générées sur des sites de personnalisation 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 QSCD (Qualified Signature Creation Device) pour les certificats d'OID 1.3.6.1.4.1.48620.41.1.7.3.1.1.1 (certificats de signature qualifiés ETSI EN 319411-2) ; • qualifié QSCD (Qualified Signature Creation Device) pour les certificats d'OID 1.3.6.1.4.1.48620.41.1.7.3.2.1.1 (certificats d'authentification ETSI 319411-1 NCP+). La génération des clés de signature du Porteur est effectuée dans des circonstances parfaitement contrôlées, par des personnels habilités de l'Autorité d'Enregistrement. Après 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 le Prestataire afin de prendre les mesures nécessaires en cas de perte ou de non-renouvellement de la qualification. Ces mesures sont documentées dans la DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

Certificats de cachet pour les organisations et d'unité d'horodatage
Le Service de stockage sécurisé de Bi-clé de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » 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 critères communs EAL4+. Ce module est hébergé dans les locaux à accès très restreint du Prestataire. La génération des clés de signature Client est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre d'une « Cérémonies des Clés Client » (ou encore Key Ceremony – KC Client). Cette cérémonie se déroule suivant des scripts, organisationnels et techniques, préalablement définis. La génération des clés de signature Client s'accompagne de la génération de différents secrets et éléments sensibles. Ces secrets sont des données permettant de gérer et de manipuler de manière sécurisée (personne ne peut posséder l'intégralité du secret), et ultérieurement à la Cérémonie des Clés, la clé privée de signature du Client, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signature Client. Le Client n'a pas la charge de la génération des Bi-clés cryptographiques. Cette génération est à la charge du Prestataire conformément à la description ci-dessus et notamment pour les certificats d'horodatage.

6.1.2 Transmission de la clé privée à son propriétaire

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
La clé privée du Porteur est transmise au moment de la remise du support cryptographique au Porteur. La qualification SSCD ou QSCD de ce support garantit que la clé privée ne peut pas être exportée.

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

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

Cependant, les différents secrets générés lors de la KC Client permettant d'obtenir une sauvegarde sécurisée (chiffrée et répartie) de la Bi-clé de signature du Client peuvent être remis en totalité au RC.

Il est alors de la responsabilité du RC de choisir les Détenteurs de secrets auxquels vont être attribués les secrets. Ces Détenteurs doivent pouvoir être mobilisés s'il est nécessaire de réinstaller les secrets Client (installation d'un nouveau Module, reprise sur incident).

6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise à l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » dans la demande de génération de Certificat. La clé est protégée en intégrité et l'origine est authentifiée grâce à l'utilisation d'une enveloppe au format PKCS#10 qui est signée par la clé privée associée à la clé publique.

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

Les clés publiques de vérification de signature de l'AC sont mises à disposition des utilisateurs de certificats et consultables publiquement tel que défini dans le paragraphe ***2***.

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

6.1.5 Tailles des clés

Les tailles de clés sont les suivantes :

- Certificat de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » : 4096 bits (algorithme RSA) ;
- Certificats des Porteurs et des Clients : supérieure ou égale à 3072 bits (algorithme RSA).

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

L'équipement de génération de Bi-clé utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la Bi-clé. Ces paramètres sont rappelés dans le chapitre ***7*** « ***Profils des certificats, OCSP et des LCR*** ».

Certificats de cachet pour les organisations et d'unité d'horodatage
L'équipement est configuré pour respecter au minimum une configuration FIPS 140-2 niveau 3 ou critères communs EAL4+ qui interdit les algorithmes et paramètres considérés comme faibles, ainsi que l'exportation en clair de la clé privée de Signature du Client.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du Certificat associé est strictement limitée à la signature de Certificats et de LCR. L'utilisation des certificats est décrite dans le paragraphe ***1.4*** « ***Usage des certificats*** ».

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

6.2.1.2 Dispositifs de création de signature des Porteurs et des Clients

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les dispositifs remis aux Porteurs sont qualifiés SSCD (au niveau renforcé) ou QSCD sous une ou plusieurs références autorisées par l'Organe de Contrôle dans la rubrique qualification produit.

Certificats de cachet pour les organisations et d'unité d'horodatage
Les dispositifs de création de signature des Clients pouvant être utilisés sont des modules cryptographiques matériels certifiés FIPS 140-2 niveau 3 ou critères communs EAL4+ pour les certificats de signature avec gestion sécurisée par le Prestataire. Sa configuration opérationnelle minimale est conforme au standard FIPS 140-2 niveau 3. Le Service de stockage sécurisé des Bi-clés de l'AC est chargé du maintien opérationnel et de la sécurité de ces Modules.

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

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

- Pour l'exportation / l'importation hors / dans un module cryptographique : les systèmes sont configurés pour interdire l'exportation en clair de la clé privée, assurant ainsi sa non compromission ;
- Pour la génération de la bi-clé (cf. §***6.1.1.1***) : utilisation d'un module cryptographique matériel sécurisé pour la génération et le stockage de la clé privée, et le partage des secrets assure qu'aucun acteur ne puisse accéder ou interpréter un des secrets ;
- Pour l'activation de la clé privée (cf. §***6.2.8***) : les flux de requêtes de certificats et de révocation (mise à jour de la LCR) sont maîtrisés pour s'assurer que seuls les services autorisés puissent être enregistrés ; l'action d'autorisation et de configuration de ces flux nécessite la présence d'au minimum 2 Officiers PKI ;
- Pour la destruction (cf. §***0***) : les procédures de destruction permettent de s'assurer que personne ne pourra utiliser la clé privé.e

6.2.3 Séquestre de la clé privée

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

6.2.4 Copie de secours de la clé privée

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les clés privées des Porteurs ne font pas l'objet d'une copie de secours. La perte du support du Porteur nécessite une révocation des certificats contenus sur le support et une nouvelle demande de la part du Porteur. Un nouveau support lui sera alors remis.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de cachet pour les organisations et d'unité d'horodatage
Les clés privées des Clients font l'objet d'une sauvegarde hors des modules cryptographiques sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

La partition contenant la clé privée d'AC fait l'objet de copies de secours hors des modules cryptographiques sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

L'installation et la restauration des clés d'AC dans un module cryptographique requièrent le contrôle simultané de deux personnels en rôle de confiance.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivées. Les clés privées des 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

Pour les clés privées d'AC, tout transfert se fait sous forme chiffrée, conformément aux indications du paragraphe ***6.2.4*** « ***Copie de secours de la clé privée*** ». La procédure de transfert de la clé privée nécessite la présence d'au moins deux rôles de confiance.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
Les clés privées des Porteurs ne peuvent faire l'objet d'un transfert en dehors du dispositif SSCD/QSCD.

Certificats de cachet pour les organisations et d'unité d'horodatage
Pour les clés privées de signature des Clients, tout transfert se fait sous forme chiffrée, conformément aux indications de la section ***6.2.4*** « ***Copie de secours de la clé privée*** ».

6.2.7 Stockage de la clé privée dans un module cryptographique

Le stockage de la clé privée dans un module cryptographique applique les mêmes règles que celles présentées dans le paragraphe ***6.2.1*** « ***Standards et mesures de sécurité pour les modules cryptographiques*** ».

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clé privée d'AC

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 de l'AC par plusieurs personnes*** ».

6.2.8.2 Clés privées des Porteurs et des Clients

L'activation est réalisée de façon sécurisée.

Certificats de signature et authentification sur support cryptographiques pour des personnes physiques
L'activation de la clé privée du Porteur est contrôlée via des données ou des actions d'activation (cf. §***6.4*** « ***Données d'activation*** ») propres au Porteur.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de cachet pour les organisations et d'unité d'horodatage
L'activation de la clé privée du Client est contrôlée via des données ou des actions d'activation (cf. §***6.4*** « ***Données d'activation*** ») propres au Client.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clé privée d'AC

La désactivation de la clé privée d'AC dans les modules cryptographiques est automatique dès que l'environnement du module évolue de manière sensible : choc, déconnexion, etc.

Les modalités de désactivation sont propres à la technologie du module ; elles sont détaillées dans la documentation constructeur. Il s'agit dans ce cadre de désactiver la partition contenant la clé privée correspondante.

6.2.9.2 Clés privées des Porteurs et des Clients

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

Certificats de cachet pour les organisations et d'unité d'horodatage
L'activation des clés privées des Clients peut être temporairement suspendue ou définitivement interdite en cas de non-respect des termes contractuels définis entre l'AC et le Client du Service. La désactivation de la clé privée des Clients dans les Modules cryptographiques matériels est automatique dès que l'environnement du module évolue de manière sensible : choc, déconnexion, etc. Les modalités de désactivation sont propres à la technologie du module ; elles sont détaillées dans la documentation constructeur.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

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

6.2.10.2 Clés privées des Porteurs et des Clients

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.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

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

6.2.11 Niveau d'évaluation sécurité du module cryptographique

Le niveau d'évaluation 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 de l'AC et des Porteurs sont archivées dans le cadre de l'archivage des Certificats correspondants.

6.3.2 Durées de vie des Bi-clés et des certificats

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

La durée de validité des Certificats des Porteurs est de 3 ans. Elle ne peut excéder la durée de validité restante du certificat de l'AC émettrice ; le cas échéant, la date de fin de validité du Certificat est alignée sur celle du certificat de l'AC. Le champ notAfter du Certificat porte la date ainsi obtenue.

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 phase d'initialisation et de personnalisation de ce module.

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du 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. Ce code PIN peut être saisi 3 fois avant blocage de l'accès à la clé privée du support. La remise à zéro de ce compteur nécessite la saisie d'un code de déblocage. 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.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Certificats de cachet pour les organisations et d'unité d'horodatage
Les données d'activation sont hors périmètre de l'AC. Elles sont générées et protégées par be-invest en intégrité et en confidentialité jusqu'à la remise au destinataire. Ce dernier a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.2 Protection des données d'activation

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

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

6.4.2.2 Protection des données d'activation correspondant aux clés privées des Porteurs

La protection des données d'activation correspondant aux clés privées des Porteurs est identique à celle présentée dans le paragraphe ***6.4.1.2*** « ***Génération et installation des données d'activation correspondant à la clé privée du Porteur*** ».

6.5 Mesures de sécurités des systèmes informatiques

6.5.1 Politique de sécurité des réseaux et des systèmes d'information

Le Prestataire définit, documente, met en œuvre et maintient une politique de sécurité des réseaux et des systèmes d'information, approuvée par la Direction et applicable aux services couverts par la présente PC. Les mesures associées, les rôles et responsabilités, ainsi que les documents applicables, sont précisés dans la Politique de Sécurité du Prestataire, la PSSI et la DPC.

6.5.2 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ». Il répond en particulier aux objectifs de sécurité suivants :

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

- Eventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle doit être cohérente avec la Politique de Sécurité.

Pour atteindre ces objectifs de sécurité, le Prestataire utilise des systèmes et des produits fiables permettant de mettre en œuvre de façon sécurisé les différents processus de l'IGC. Les systèmes et produits sont choisis et/ou développés en prenant en compte les exigences de sécurité.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système sont mis en place. Ces dispositifs permettent :

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

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

6.5.3 Niveau de qualification des systèmes informatiques

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

6.6 Mesures de sécurté des systèmes 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 du Prestataire est documentée.

La configuration du système des composantes de l'IGC du Prestataire ainsi que toute modification et mise à niveau sont documentées. 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.

Tout développement doit être cohérent avec la Politique de Sécurité du Prestataire et avec les exigences contenues dans la présente PC.

6.6.2 Mesures liées à la gestion de la sécurité

6.6.2.1 Mise à jour des composantes

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

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

6.6.2.2 Analyse de risques

Le Prestataire a réalisé une analyse de risque pour identifier, analyser et évaluer les risques pesant sur l'IGC en prenant en compte les risques techniques et métier. A la suite de cette analyse de risque, 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.

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

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

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

6.6.2.2.1 Scan de vulnérabilité

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

6.6.2.2.2 Test d'intrusion

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

6.7 Mesures de sécurité réseau

6.7.1 Segmentation en zone

Fondé sur les résultats de l'analyse de risque, le Prestataire a segmenté son réseau en zone séparées (fonctionnellement, logiquement ou physiquement). Des mesures de contrôle similaires sont mise en place pour l'ensemble des éléments d'une même zone. Chaque système de l'IGC est exploité dans une zone réseau sécurisée et est installé suivant des procédures et une configuration assurant une exploitation sécurisée.

Les systèmes les plus critiques, tels que les AC Racines, sont opérés dans les zones les plus sécurisées.

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

6.7.2 Interconnexions

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

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

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

6.7.3 Connexions

Seuls les personnels en rôle de confiance ont accès aux zones réseaux sécurisées.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Toute connexion d'un compte permettant de créer directement un certificat n'est possible qu'après une authentification multi-facteur. Les réseaux permettant d'opérer et d'administré l'IGC sont séparés. Le réseau d'administration est dédié à cet usage.

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

6.7.4 Disponibilité

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

6.8 Horodatage / Système de datation

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil du certificat de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 »

Le tableau suivant fournit les valeurs des attributs du Certificat de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » émis par l'AC racine « ALMERYS ROOT CA ».

Le format de ce certificat ainsi que ses attributs respectent le profil X.509v3 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

tbsCertList		Valeur
version		2 (c'est-à-dire version 3)
serialNumber		Nombre aléatoire
signature		
► algorithm		Sha256withRSAEncryption
► parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN=ALMERYS ROOT CA OU=0002 432701639 O=ALMERYS C=FR
validity		
► notBefore		Date de création
► notAfter		Date de fin de validité (= notBefore + 10 ans)
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		OI = VATLU-LU29222134 CN = BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 O = BE INVEST International S.A. C = LU
subjectPublicKeyInfo		
► algorithm ➥ algorithm ➥ parameters		rsaEncryption) RSAParams : NULL
► subjectPublicKey		DER encoded RSAPublicKey (4096 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
▶ authorityKeyIdentifier	Non	Hash de la clé publique de l'issuer
▶ subjectKeyIdentifier	Non	Hash de la clé publique du sujet
▶ keyUsage	Oui	keyCertSign (5), cRLSign (6)
▶privateKeyUsagePeriod		Extension non utilisée
▶certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.7.3.2
▶ basicContraints ➥ cA ➥ pathLenConstraint	Oui	 True None
▶ cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almerysrootca.crl
Private extensions		
▶ authorityInfoAccess	Non	[1] : accessMethod : id-ad-calssuers accessLocation : URL=http://pki.almerys.com/almerysrootca.cer
▶subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption, clé de 4096 bits
parameters		NULL

7.2 Profil des certificats Porteurs

Le tableau suivant fournit les valeurs par défaut des attributs d'un Certificat Porteur émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

Le format de ce Certificat ainsi que ses attributs respectent le profil X.509v3 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

7.2.1 Profils eIDAS support cryptographique

tbsCertList		Valeur
version		2 (c'est-à-dire version 3)

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
serialNumber		Nombre aléatoire à longueur fixe.
signature		
► algorithm		Sha256withRSAEncryption
► parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		2.5.4.97 = VATLU-LU29222134 CN = BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 O = BE INVEST International S.A. C = LU
validity		
►notBefore		Date de création
►notAfter		Date à laquelle la période de validité du Certificat prend fin (voir § 6.3.2)
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		CN = <Prénom><Nom> SerialNumber = UI:LU-<Identifiant Porteur unique> GN = <Prénom> SN =<Nom> OU = organisation unit [1] OI = NTR<code pays> -<SIREN ou SIRET ou équivalent>[2] ou VAT<code pays>-<Numéro de TVA intracommunautaire> O = <Raison sociale Porteur>[3] C = <code pays>
subjectPublicKeyInfo		
►algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams : NULL
►subjectPublicKey		DER encoded RSAPublicKey,3072 bits minimum
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
►authorityKeyIdentifier	Non	**hash de la clé publique de l'issuer**
► subjectKeyIdentifier	Non	**hash de la clé publique de l'issuer**

[1] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

[2] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

[3] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur	
▶keyUsage	Oui	Certificat d'authentification	Certificat de signature qualifiée
		digitalSignature	nonRepudiation (contentCommitment)
▶privateKeyUsagePeriod		Extension non utilisée	
▶certificatePolicies	Non	*Certificat d'authentification*	*Certificat de signature qualifiée*
		Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.7.3.2.2.1	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.7.3.2.1.1
▶ Qualified Certificate Statements	Non	Extension non utilisée	- id-etsi-qcs-QcCompliance true
			-id-etsi-qcs-QcSSCD true
			-id-etsi-qcs-QcPDS Langue=EN URL = http://pki.almerys.com/intermediate/be-yssignatureandauthenticationcanc2/PDS/be-yssignatureandauthenticationcanc2-PDS.pdf
			-id-etsi-qcs-QcType id-etsi-qct-esign
▶SubjectDirectoryAttribute[4]	Non	Extension non utilisée	T= <Titre du Porteur >[5] C = FR
▶basicContraints ↪cA ↪pathLenConstraint	Non	false None	
▶extKeyUsage	Non	Client Authentication	Extension non utilisée
▶cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/be-yssignatureandauthenticationcanc2.crl	
Private extensions			
▶authorityInfoAccess	Non	[1] : accessMethod : id-ad-calssuers	

[4] Extension utilisée pour indiquer l'attribut du porteur, utilisable uniquement dans le certificat qualifié des porteurs ayant présentés un justificatif de leur attribut lors de leur enregistrement. Extension utilisée notamment pour les certificats qualifiés des professions réglementées

[5] Titre ou attribut du porteur tel indiqué dans le justificatif inclus dans le dossier d'enregistrement

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
		accessLocation : URL=http://pki.almerys.com/ be-yssignatureandauthenticationcanc2.cer [2] accessMethod : id-ad-ocsp accessLocation : URL= http://ocsp.almerys.com
►subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.2.2 Profils eIDAS Cachet

tbsCertList		Valeur
version		2 (c'est-à-dire version 3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
► algorithm		Sha256withRSAEncryption
► parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		2.5.4.97 = VATLU-LU29222134 CN = BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 O = BE INVEST International S.A. C = LU
validity		
►notBefore		Date de création
►notAfter		Date à laquelle la période de validité du Certificat prend fin (voir § 6.3.2)
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName		CN = <Service> OU = <organisation unit > OI = NTR<code pays> -<SIREN ou SIRET ou équivalent > ou VAT<code pays>-<Numéro de TVA intracommunautaire>[6] O = <raison sociale du porteur >[7]

[6] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

[7] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
C=countryName		C = <code pays>
subjectPublicKeyInfo		
▶algorithm ⮑algorithm ⮑parameters		 rsaEncryption RSAParams : NULL
▶subjectPublicKey		DER encoded RSAPublicKey ,3072 bits minimum
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶authorityKeyIdentifier	Non	**hash de la clé publique de l'issuer**
▶ subjectKeyIdentifier	Non	**hash de la clé publique de l'issuer**
▶keyUsage ▶privateKeyUsagePeriod	Oui	 Digital Signature Extension non utilisée
▶certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.7.3.2.4.1
▶ Qualified Certificate Statements	Non	- id-etsi-qcs-QcCompliance true
		-id-etsi-qcs-QcSSCD false
		-id-etsi-qcs-QcPDS Langue=EN URL = http://pki.almerys.com/intermediate/be-yssignatureandauthenticationcanc2/PDS/be-yssignatureandauthenticationcanc2-PDS.pdf
		-id-etsi-qcs-QcType id-etsi-qct-eSeal
▶basicContraints ⮑cA ⮑pathLenConstraint	Non	 false None

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
▶extKeyUsage	Non	Extension non utilisée
▶cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/be-ysauthenticationandsignaturecanc2.crl
Private extensions		
▶authorityInfoAccess	Non	[1] : accessMethod : id-ad-calssuers accessLocation : URL=http://pki.almerys.com/ be-ysauthenticationandsignaturecanc2.cer [2] accessMethod : id-ad-ocsp accessLocation : URL= http://ocsp.almerys.com
▶subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

Variables de l'attribut subject DN :

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

7.2.3 Profils eIDAS Horodatage

tbsCertList		Valeur
version		2 (c'est-à-dire version 3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		2.5.4.97 = VATLU-LU29222134 CN = BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 O = BE INVEST International S.A. C = LU
validity		
▶notBefore		Date de création
▶notAfter		Date à laquelle la période de validité du Certificat prend fin (voir § 6.3.2)
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		CN = <Service horodatage> OU = <organisation unit> OI = NTR<code pays>-<siren ou siret ou equivalent> ou VAT<code pays>-<Numéro de TVA intracommunautaire> O = <raison sociale du porteur> C = <code pays>
subjectPublicKeyInfo		
▶algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams : NULL
▶subjectPublicKey		DER encoded RSAPublicKey (2048 bits) jusqu'au 31/12/2025 au plus tard DER encoded RSAPublicKey (3072 bits minimum) au plus tôt à partir du 01/01/2023 inclus
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶authorityKeyIdentifier	Non	**hash de la clé publique de l'issuer**
▶ subjectKeyIdentifier	Non	**hash de la clé publique de l'issuer**
▶keyUsage	Oui	digitalSignature (0)
▶privateKeyUsagePeriod		Extension non utilisée
▶certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.7.3.2.5.1
▶ Qualified Certificate Statements	Non	- id-etsi-qcs-QcCompliance true
		-id-etsi-qcs-QcSSCD

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
		false
		-id-etsi-qcs-QcPDS Langue=EN URL = http://pki.almerys.com/intermediate/be-yssignatureandauthenticationcanc2/PDS/be-yssignatureandauthenticationcanc2-PDS.pdf
		-id-etsi-qcs-QcType id-etsi-qct-eseal
▶basicContraints ➥cA ➥pathLenConstraint	Non	 false None
▶extKeyUsage	oui	Timestamping
▶cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/be-ysauthenticationandsignaturecanc2.crl
Private extensions		
▶authorityInfoAccess	Non	[1] : accessMethod : id-ad-calssuers accessLocation : URL=http://pki.almerys.com/ be-ysauthenticationandsignaturecanc2.cer [2] accessMethod : id-ad-ocsp accessLocation : http://ocsp.almerys.com
▶subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.3 Profil de LCR

Le tableau suivant fournit les valeurs par défaut des attributs de la Liste de Certificats Révoqués (LCR) émise par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

Le format de cette LCR ainsi que ses attributs respectent le profil X.509v2 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
version		1 (c'est-à-dire version 2)
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		2.5.4.97 = VATLU-LU29222134 CN = BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 O = BE INVEST International S.A. C = LU
thisUpdate		Date de création (référentiel temporel de l'AC)
nextUpdate		Date de fin de validité (= thisUpdate + 72 heures)
revokedCertificates		
▶ userCertificate		n° de série du certificat révoqué
▶ revocationDate		date de révocation du certificat
▶ crlEntryExtensions		
⮡ reasonCode		unspecified (0) *valeur par défaut*
crlExtensions	Critique :	
▶authorityKeyIdentifier	Non	160 bits du haché SHA-1 de la clé publique de l'issuer
▶ issuerAltName	-	Extension non utilisée
▶ cRLNumber	Non	Numéro de séquence de la LCR (incrémental simple).
▶ deltaCRLIndicator	-	Extension non utilisée
▶ freshestCRL	-	Extension non utilisée
▶ ExpiredCertsOnCRL	Non	True
signatureAlgorithm		
algorithm		Sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11), clé de 4096 bits
parameters		NULL

Les certificats de signature qualifiés ETSI EN 319411-2 qui ont été révoqués sont conservés dans la CRL après leur expiration.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

7.4 Profil certificat de l'OCSP

tbsCertList		Valeur
version		2 (c'est-à-dire version 3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
► algorithm		Sha256withRSAEncryption
► parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		2.5.4.97 = VATLU-LU29222134 CN = BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 O = BE INVEST International S.A. C = LU
validity		
►notBefore		Date de création
►notAfter		Date à laquelle la période de validité du Certificat prend fin (voir § 6.3.2)
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		CN = SIGNATURE AND AUTHENTICATION CA NC OCSP <XX>[8] OU = <organisation unit>[9] OI = NTR<code pays>- <SIREN ou SIRET ou équivalent > ou VAT<code pays>-<Numéro de TVA intracommunautaire>[10] O = <Raison sociale Porteur>[11] C = <code pays>
subjectPublicKeyInfo		
►algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams : NULL
►subjectPublicKey		DER encoded RSAPublicKey (2048 bits) jusqu'au 31/12/2022 au plus tard DER encoded RSAPublicKey (3072 bits) au plus tôt à partir du 01/01/2023 inclus
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé

[8] Où <XX> sera remplacé par l'indice du certificat d'OCSP en commençant à « 01 ».

[9] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

[10] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

[11] Les champs o=, oi= et ou= dans le DN sont utilisés uniquement dans le cadre d'un certificat « entreprise ». le champ OU est optionnel.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

tbsCertList		Valeur
Standard extensions	Critique :	
▶authorityKeyIdentifier	Non	**hash de la clé publique de l'issuer**
▶ subjectKeyIdentifier	Non	**hash de la clé publique du sujet**
▶keyUsage	Oui	digitalSignature
▶certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.7.3.2.6.1
▶extKeyUsage	Non	OCSPSigning
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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

8.1 Fréquences et/ou circonstances des évaluations

Pour donner suite à toute modification significative d'une composante de l'IGC, l'AG procède à une analyse de sécurité et fait évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.

L'AG procède également régulièrement à un contrôle de conformité de l'IGC, en tout ou partie. La fréquence de ce contrôle est fournie dans la DPC associée à la présente PC.

8.2 Identités / Qualifications des évaluateurs

L'AG choisit et assigne une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC, et être dûment autorisée à pratiquer les contrôles visés.

8.4 Sujets couverts par les évaluations

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

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un audit de sécurité, l'équipe d'audit rend à l'AG, un avis parmi les suivants : « réussite », « échec », « à confirmer ». Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AG qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du Certificat de la composante, la révocation de l'ensemble des Certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AG et doit respecter ses politiques de sécurité internes ;
- En cas de résultat « à confirmer », l'AG remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus ;
- En cas de réussite, l'AG confirme à la composante contrôlée la conformité aux exigences de la PC et de la DPC.

8.6 Communication des résultats

Les modalités de communication concernant les résultats des audits de conformité sont précisées dans la DPC.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

8.7 Autres éléments de conformité

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

Les informations suivantes sont fournies dans les différents documents contractuels établis entre les parties : (i.e. Prestataire, les Clients du service, et éventuellement les fournisseurs assurant en tout ou partie certaines fonctions de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ou de l'AE) :

- Les conditions de facturation du Service proposé par le Prestataire ;
- Les responsabilités ;
- Les responsabilités financières ;
- Le montant des indemnités.

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

9.2 Responsabilité financière

La responsabilité financière est décrite dans le précédent paragraphe **9.1**.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

La classification des informations se décompose en :

- Secret (niveau 4 de la Politique de Sécurité) ;
- Confidentiel (niveau 3 de la Politique de Sécurité) ;
- Interne (niveau 2 de la Politique de Sécurité).

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

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

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

- La DPC de l'AC ;
- Les journaux d'événements des composantes de l'IGC ;
- Les causes de révocations, sauf accord explicite de publication du Porteur ;
- Les dossiers d'enregistrement des Porteurs.

9.3.2 Informations hors du périmètre des informations confidentielles

Par défaut, en complément des informations déjà explicitement listées dans le paragraphe précédent ***9.3.1*** ainsi que dans le paragraphe ***9.4*** « ***Protection des données à caractère personnel*** » présent dans ce document, une information est considérée comme confidentielle à l'exception des informations publiées dont la liste est fournie

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

à l'article **2.2** « ***Informations devant être publiée*** », et n'est diffusée qu'avec le consentement explicite de l'AG de l'IGC du Prestataire aux personnes ayant le besoin d'en connaître.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

9.3.3 *Responsabilités en termes de protection des informations confidentielles*

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

9.4 Protection des données à caractère personnel

9.4.1 *Politique de protection des données à caractère personnel*

Toute collecte et tout traitement de données à caractère personnel par l'AE et l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » sont réalisés dans le strict respect de la réglementation en vigueur, et en particulier le règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit « Règlement Général sur la Protection des Données [RGPD] ».

9.4.2 *Informations à caractère personnel*

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des Certificats des Porteurs (qui sont considérées comme confidentielles sauf accord explicite du Porteur) ;
- Les informations d'enregistrement du Porteur, et du MC.

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

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

Le Porteur et le Client sont responsables du respect de la réglementation en vigueur dite [RGPD].

Le traitement des données à caractère personnel est sous la responsabilité du président du directoire du groupe BeYs.

Pour la conformité au [RGPD], le Prestataire a mis en place une organisation centrée sur le Délégué à la Protection des Données DPO.

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

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

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

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

9.4.6 *Autres circonstances de divulgation d'informations personnelles*

Sans objet dans le cadre de la présente PC.

9.5 Droits sur la propriété intellectuelle et industrielle

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (*par exemple : logiciels, pages web, bases de données, textes originaux, …*) est sanctionnée conformément aux dispositions des lois Luxembourgeoises.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC et les documents qui en découlent ;
- Respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- Se soumettre aux audits de sécurité et aux contrôles de conformité demandés par les parties prenantes dûment identifiées et habilitées ;
- Respecter les accords ou contrats qui les lient entre elles ou avec les Clients ;
- Documenter leurs procédures internes de fonctionnement ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité ;
- Se conformer aux dispositions de la Loi du 17 juillet 2020 portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique du Luxembourg.

9.6.1 Autorité de Certification

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » a pour obligation de :

- Pouvoir démontrer aux Applications utilisatrices de ses Certificats qu'elle a émis un Certificat pour un Porteur donné et que ce Porteur a accepté le Certificat, conformément aux exigences du paragraphe ***4.4*** « ***Acceptation du certificat*** » ;
- Protéger les clés privées de signature des Clients et de signature déporté des porteurs conformément aux exigences de la présente PC ;e
- Garantir et maintenir la cohérence de la DPC avec la PC.

9.6.2 Autorité de gouvernance

L'AG est responsable de la conformité de la PC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », avec les exigences émises dans la PC de l'ACR. L'AG assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la PC de l'ACR, par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ou l'une des composantes de l'IGC. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées aux opérations et/ou activités de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC de l'ACR.

De plus, l'AG reconnaît engager sa responsabilité en cas de faute ou de négligence de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ou de l'une des composantes de l'IGC, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données à caractère personnel des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des Certificats de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 ».

Par ailleurs, l'AG reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des Certificats délivrés par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » ou l'une des composantes de

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

l'IGC. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

9.6.3 Autorité d'enregistrement (AED)

Outre ses responsabilités décrites dans l'introduction du paragraphe 9.6 « Interprétations contractuelles et garanties », ainsi que dans les paragraphes ***1.3.4*** « ***Autorité d'Enregistrement (AE)*** » et ***4*** « ***Exigences opérationnelles sur le cycle de vie des certificats*** », l'AE (AED) doit :

- Conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées ;
- Assurer que les processus de gestion des demandes de certificats sont conformes aux règles énoncées par l'AC. Cette règle est notamment applicable dans le cas où l'AE est un Client du Prestataire ;
- Et prendre toutes les mesures raisonnables pour s'assurer que les Porteurs qui la requêtent sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des Certificats ou encore de l'équipement et des logiciels éventuellement utilisés.

9.6.3.1 Mandataire de Certification

Outre ses responsabilités décrites dans le paragraphe ***1.3.9.2*** « ***Le Mandataire de Certification*** », Le MC doit :

- Effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC ;
- Respecter les parties de la présente PC et de la DPC qui lui incombent ;
- Signaler à l'AC, si possible préalablement mais au moins sans délai, son départ, ou la fin de sa mission de MC.

9.6.4 Porteurs

Le Porteur doit :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat ;
- Satisfaire à une identification selon l'un des procédés suivants :
    - Par la présence physique devant l'AE (AED) ou le MC, sur la base de preuves et de procédures appropriées — les justificatifs recevables et les modalités de contrôle sont précisés au paragraphe 3.2.3.1 —, conformément au droit national et en conformité avec l'article 24, paragraphe 1 bis, du règlement (UE) n° 910/2014 modifié ;
    - Au moyen d'un certificat de signature électronique qualifiée ou d'un certificat de cachet électronique qualifié en cours de validité, émis conformément à l'une des méthodes de vérification d'identité admises par l'article 24, paragraphe 1 bis, points a), c) ou d), du règlement (UE) n° 910/2014 modifié.
- Accepter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AE de toute modification concernant les informations contenues dans son Certificat ;
- Faire, sans délai, une demande de révocation de son Certificat auprès de l'AE en cas de suspicion de compromission de sa clé privée (ou de ses données d'activation).

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

Le porteur doit, de plus, gérer de manière sécurisée les secrets et éléments sensibles qui lui sont remis à l'issue de la procédure de génération de son certificat, en particulier le porteur doit garder sa clé privée ou son moyen d'authentification sous son contrôle exclusif.

Après renouvellement d'un certificat, le porteur doit détruire son ancien support cryptographique le cas échéant.

BE INVEST INTERNATIONAL S.A.
17, rue Léon Laval, L-3372 Leudelange
© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

9.6.5 *Client, Représentant Client*

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

Le RC, qui représente le Client, doit :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat ;
- Assister à la KC Client ;
- Gérer de manière sécurisée les secrets et éléments sensibles qui lui sont remis à l'issue de la KC Client, et désigner les Détenteurs de secrets Client ;
- Autoriser l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » à héberger sa clé privée de signature dans les conditions décrites dans la présente PC ;
- Accepter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AE de toute modification concernant les informations contenues dans son Certificat ;
- Faire, sans délai, une demande de révocation de son Certificat auprès de l'AE en cas de suspicion de compromission de sa clé privée (ou de ses données d'activation).

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

9.6.6 *Applications utilisatrices de certificats*

Les applications utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un Certificat a été émis ;
- Contrôler que le Certificat émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- Vérifier la signature électronique de l'AC « BE YS LU CA NC » émettrice du Certificat en parcourant la chaîne de certification jusqu'à l'ACR « almerys Root CA », celle-ci devant correspondre à l'ancre de confiance identifiée dans le "service digital identifier" de l'entrée appropriée de la Liste de Confiance de l'Union européenne (EU Trusted List) relative au prestataire de services de confiance qualifié concerné, conformément à ETSI TS 119 612 ;
- Vérifier et respecter les obligations des Applications utilisatrices de certificats exprimées dans la présente PC ;
- Contrôler la validité des Certificats (dates de validité, statut de révocation).

9.6.7 *Autres participants*

Sans objet dans le cadre de la présente PC.

9.7 Limite de garantie

Pour la limite de garantie se référer au paragraphe ***9.1*** « ***Tarifs*** ».

9.8 Limite de responsabilité

Sous réserve des dispositions d'ordre public applicables, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » du Prestataire ne pourra pas être tenue responsable d'une utilisation non autorisée ou non conforme des Certificats, des données d'activation, des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » du Prestataire décline en particulier sa responsabilité pour tout dommage résultant :

- D'un emploi des Bi-clés pour un usage autre que ceux prévus avec le Client ;
- De l'usage de Certificats expirés ;
- D'un cas de force majeure (cad pour tout dommage dû à une cause indépendante de sa volonté, y compris, mais sans s'y limiter émeutes, pillages, sabotages, attaques ou actions criminelles; les dommages causés par des événements accidentels et incontrôlables, attribuables à des tiers (y compris, sans limitation, les incendies, les explosions, les accidents d'avion); catastrophes naturelles; les phénomènes atmosphériques (y compris, sans limitation, les inondations, les pluies, les vents, les tempêtes, les incendies, les ouragans, l'activité volcanique); l'échec des fournisseurs tiers à effectuer; conflits de travail ou actes gouvernementaux).

L'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » du Prestataire décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les Certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.

En aucun cas, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre les Clients et les Porteurs, notamment quant au contenu des documents soumis à signature cachet via le Service de signature électronique, ou le service d'horodatage du Prestataire.

Pour la tarification se référer au paragraphe ***9.1*** « ***Tarifs*** ».

9.9 Indemnités

Pour les indemnités se référer au paragraphe ***9.1*** « ***Tarifs*** ».

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La PC de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » reste en application au moins jusqu'à la fin de vie du dernier Certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

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

Pour donner suite à la publication interne au sein de l'IGC d'une nouvelle version de la PC de l'AC Racine du Prestataire ou de la présente PC, l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » dispose d'un délai de 1 an pour se mettre en conformité.

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

9.10.3 Effets de la fin de validité et clauses restant applicables

À la suite de l'arrêt de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et donc à la fin de validité de cette politique les exigences des paragraphes suivants doivent rester applicables jusqu'à la fin de vie du dernier certificat émis :

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

§	Intitulé
2	***Responsabilités concernant la mise à disposition des informations devant être publiées***
3.4	***Identification et validation d'une demande de révocation***
4.5	***Usages de la Bi-clés et du certificat***
4.8	***Modification du certificat***
4.9	***Révocation et suspension des certificats***
Erreur ! Source du renvoi introuvable.	*Erreur ! Source du renvoi introuvable.*

9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AG devra au plus tard un mois avant le début de l'opération, faire valider ce changement, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » et de ses différentes composantes.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

Tout projet de modification de la présente PC doit rester conforme aux exigences de la politique de sécurité de l'IGC du Prestataire, de la PC de l'ACR et respecter les engagements avec les Clients et les Porteurs existants. En cas de changement important, l'AG de l'IGC du Prestataire pourra faire appel à une expertise technique pour en contrôler l'impact.

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

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

9.12.2 Circonstances selon lesquelles l'OID doit être changé

L'OID du type de Certificat émis par l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 » étant inscrit dans les Certificats qu'elle émet, toute évolution de la PC ayant un impact majeur sur les Certificats déjà émis (*par exemple, augmentation des exigences en matière d'enregistrement des Porteurs, qui ne peuvent donc pas s'appliquer aux Certificats déjà émis*) doit se traduire par une évolution de l'OID, afin que les Applications utilisatrices puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13 Dispositions concernant la résolution de conflits

Pour toute demande d'information ou réclamation relative au service Certificats de l'AC « BE-YS SIGNATURE AND AUTHENTICATION CA NC 2 », il convient de contacter le service Autorité de Certification par mail à l'adresse suivante : gouvernance.igc@be-ys.com.

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

9.14 Juridictions compétentes

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

9.15 Conformité aux législations et réglementations

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

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

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Conformité aux législations et réglementations

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
[RGPD]	Règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[REG_eIDAS]	Règlement eIDAS

10.2 Conformité aux législations et réglementations

Renvoi	Document
[ETSI_319401]	General Policy Requirements forTrust Service Providers
[ETSI_319411-1]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI_319411-2]	Policy and security requirements forTrust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI_119461]	ETSI TS 119 461 V2.1.1 (2025-02) Policy and security requirements for trust service components providing identity proofing
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - 11/2003
[PROG_ACCRED]	COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance
[CC]	Norme ISO/IEC 15408 : Critères communs version 2.1
[X.509]	Information Technology–Open Systems Interconnection – The Directory: Authentication Framework, Recommendation X.509, version 3
[RFC822]	Standard for the format of Arpa internet text messages, August 13, 1982, Revised by David H. Crocker
[RFC5280]	Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280 May 2008
[ROLES_IGC]	Rôles des exploitants d'une infrastructure de gestion de clés, CISSI, version 1.2 de janvier 2001
[DCSSI_ALGO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.0 du 3 mai 2004 N°1064 SGDN/DCSSI/SDS/AsTeC du 3 mai 2004

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation

Renvoi	Document
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)
[CWA14167-4]	CWA 14167-4 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSO-PP)
[CWA14169]	CWA 14169 (2003-08) Secure Signature Creation Device, version « EAL 4 +»

© Tous droits réservés BE INVEST INTERNATIONAL S.A. - Toute reproduction ou diffusion même partielle interdite sans autorisation