Politique de Certification de l'AC "BE-YS USER SIGNING CA NA", certificats de signature à usage unique et réutilisable

PL
Politique

Référentiel :	Sous-Référentiel :	Référence :	Statut :
Sécurité	PKI	PPKIG034-A 1.3.6.1.4.1.48620.41.1.4.1.1	Validé
Validé par :	**Fonction :**	**Date :**	**Signature :**
SPA	Responsable d'AC	30/11/2023	
Approuvé par :	**Fonction :**	**Date[•] :**	**Signature :**
VGE	Autorité de Gouvernance IGC	30/11/2023	
Diffusion auprès de :	Service juridique		
En accès pour :	Public. Mise à disposition sur site web (http://pki.almerys.com)		
Localisation :	-		

Sommaire

Date de péremption	N/A	Responsable de l'actualisation	Autorité de Gouvernance IGC

Version	Date	Modifications	Auteur
1.a	23/04/2020	creation	MMI
1.b	09/09/2023	Ajout profil de certificat persistant	EVI
1.c	28/09/2023	Ajout de la révocation par l'AED	SPA

[•] Date d'entrée en vigueur

Sommaire détaillé

AVERTISSEMENT

1. INTRODUCTION

1.1 PRESENTATION GENERALE

Dans le cadre de ses offres de services de dématérialisation et de confiance, be-invest met à disposition des Clients de son Service de signature électronique pour le compte de leurs Utilisateurs une Autorité de Certification spécifique, be-ys User Signing CA NA.

Dans ce cadre, le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification (AC) « be-ys User Signing CA NA ». Cette AC est habilitée à délivrer des Certificats de signature pour les Utilisateurs du Service de signature électronique be-invest mis à leur disposition par les Clients.

L'objectif de la présente PC est de définir les exigences concernant les Certificats de signature dans toutes les phases de leur cycle de vie. Le Porteur d'un tel Certificat pourra signer des messages, des documents ou des formulaires électroniques, assurant ainsi leur non-répudiation et leur intégrité.

Les Certificats produits respectent la norme X.509v3 et leur utilisation est dédiée au mécanisme de signature. L'AC « be-ys User Signing CA NA » émet 2 types de certificats : les certificats à usage unique et les certificats réutilisables.

A un certificat de signature est associé de manière univoque une session de signature électronique établie dans le cadre du Service de signature électronique.

La structure de la présente politique de certification s'appuie sur la référence :

- le RFC 3647 de l'IETF « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework »

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

1.1.1. Signature électronique be-ys

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

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

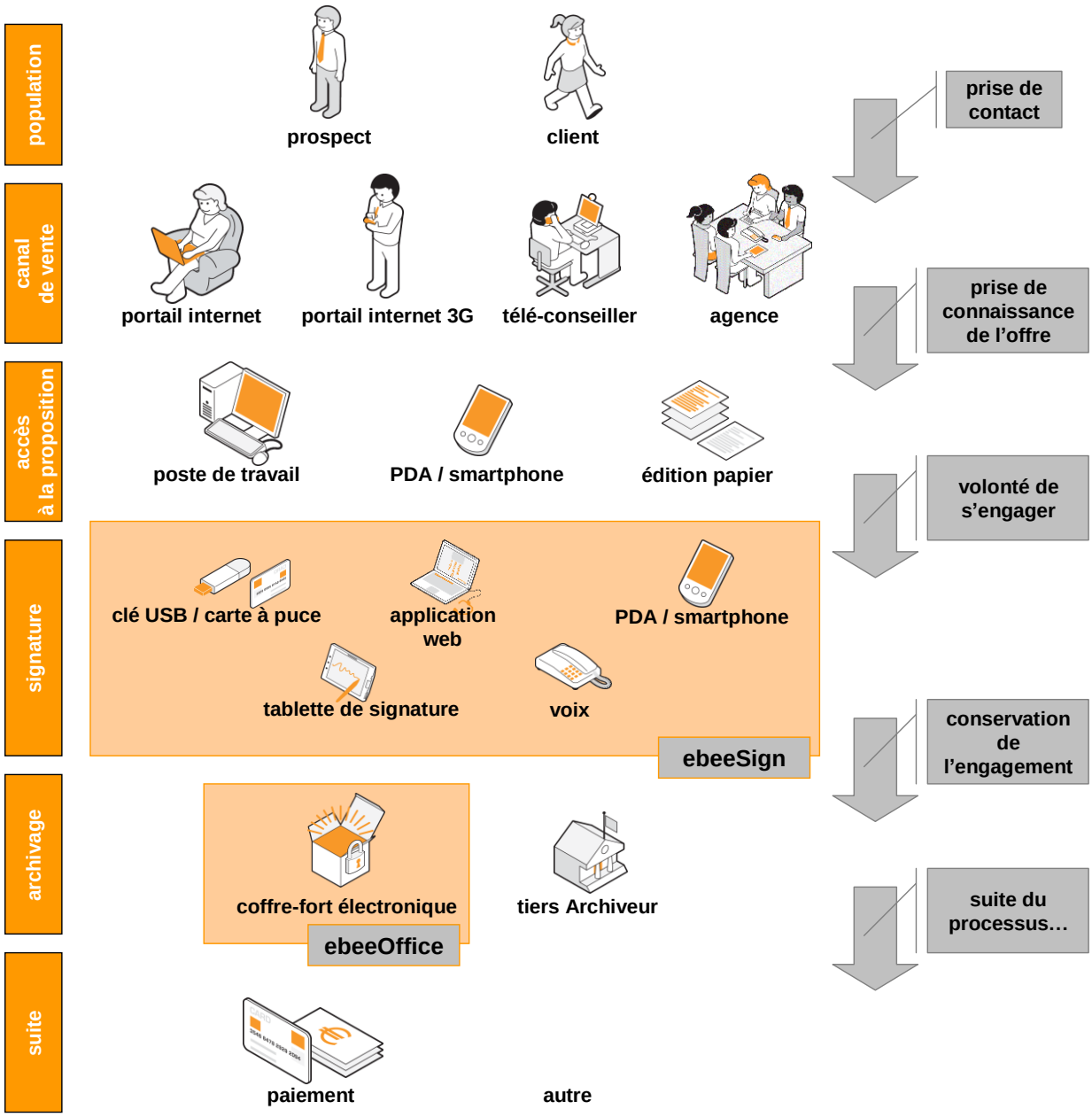
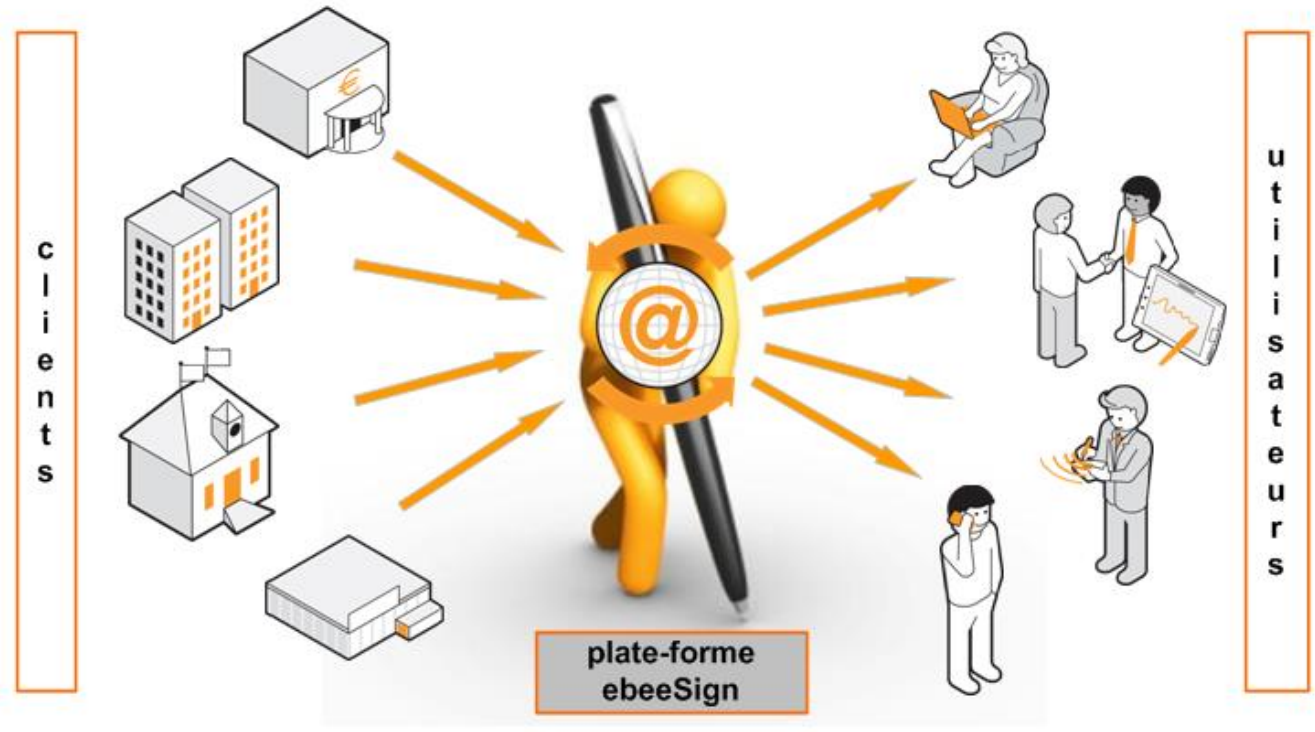


Illustration du principe de contractualisation multicanal

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

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



Les Clients et les Utilisateurs du Service de signature électronique

Dans le cadre de ce Service, l'Utilisateur dispose d'un certificat de signature électronique identifié par l'OID 1.3.6.1.4.1.48620.41.1.4.1.1.1, objet de la présente PC. Ce certificat sera utilisé par les composants du service de signature électronique pour apposer une signature numérique sur les documents présentés par le Client à l'Utilisateur 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 User Signing CA NA » de l'Infrastructure de Gestion de Clés (IGC) be-invest, pour les certificats de signature à usage unique.

Son identifiant d'objet (OID) est le suivant : 1.3.6.1.4.1.48620.41.1.4.1.1.
Cette référence figure dans les Certificats de signature émis par l'AC « be-ys User Signing CA NA » (cf. section 9.12.2).
La référence du document au sein de be-invest est la suivante : PPKIG034-A.

1.3 ENTITES INTERVENANT DANS L'IGC

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

- **Fonction d'enregistrement** - Cette fonction vérifie les informations d'identification du futur Porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. Elle a également en charge, lorsque cela est nécessaire, la revérification des informations du Porteur lors du renouvellement du Certificat de celui-ci. Cette fonction comprend une phase d'identification du demandeur de Certificat effectuée par le Client en tant qu'Autorité d'enregistrement (cf. §1.3.4 « Autorité d'Enregistrement (AE) »), qui transmet ensuite la demande à la fonction adéquate de l'IGC be-ys.

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

- **Fonction de génération des éléments secrets de l'Utilisateur** – Cette fonction génère les éléments secrets à destination de l'Utilisateur et les prépare en vue de leur stockage sécurisé au niveau des Modules cryptographiques matériels du Service de stockage sécurisé de Bi-clé et de la mise à disposition de la fonction d'activation par l'Utilisateur. Il s'agit en particulier de la bi-clé de l'Utilisateur et des informations d'activation de la clé privée de l'Utilisateur.

- **Fonction de remise à l'Utilisateur –** Cette fonction remet à l'Utilisateur les moyens de contrôle de sa clé privée et de son certificat.

- **Fonction de publication** – Cette fonction met à disposition des différentes parties concernées, les politiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux Porteurs et/ou aux Applications utilisatrices de certificats, hors informations d'état des Certificats. La liste complète des Certificats valides des Porteurs n'est pas fournie publiquement.
  La publication des conditions générales de fourniture et d'utilisation des Certificats User Signing, dans le cadre d'un processus métier, sont à la charge des Clients du service de signature électronique.

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

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

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

1.3.1. Autorité de certification (AC)

L'***Autorité de Certification*** (***AC***) « be-ys User Signing CA NA » 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 User Signing CA NA » appartient à la hiérarchie de confiance be-ys (ensemble des AC regroupées au sein de son Infrastructure de Gestion de Clés). A ce titre, la gestion de l'AC « be-ys User Signing CA NA » ainsi que de l'AC Racine est assurée par be-invest.
Les prestations de l'AC « be-ys User Signing CA NA » sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des Bi-clés et des Certificats.

1.3.2. Autorité de Gouvernance (AG)

L'Autorité de Gouvernance (***AG***) est l'autorité responsable de l'ensemble des services de l'IGC be-ys, 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 be-invest ayant un mandat spécifique pour assurer cette fonction.

1.3.3. Service de stockage sécurisé des Bi-clés des Utilisateurs

be-invest met en œuvre un service sécurisé de stockage des Bi-clés des Utilisateurs pour ses clients, les clients AED peuvent également mettre en place leurs propres services sécurisés de stockage des bi-clés.
Dans le cas où le service est hébergé dans les locaux de l'AC et met en œuvre des Modules cryptographiques matériels répondant au minimum aux exigences du standard FIPS 140-2 level 2 ou CC EAL 4+.

Seule l'application de signature électronique peut communiquer avec le Module cryptographique matériel pour une création du Bi-clé de signature de l'Utilisateur. A aucun moment, la clé privée de signature de l'Utilisateur ne peut être exportée du Module.

La création et l'activation du Bi-clé d'un Utilisateur n'intervient que si deux conditions sont remplies :

- le Client a identifié le futur Porteur de Certificat,
- le Porteur s'est identifié pour accéder au Service de signature électronique en ligne et a validé les informations qui lui sont présentées à la signature.

Seul le Porteur a la capacité d'utiliser son certificat de signature.

1.3.4. Autorité d'Enregistrement (AE)

L'***Autorité d'enregistrement (AE), l'Autorité d'enregistrement déléguée (AED) :*** est un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC et les Utilisateurs, Porteurs de certificats *User Signing*. Dans le cas du Service de signature électronique, ce sont les Clients du service qui sont chargés de la relation avec les Utilisateurs, et de leur identification et authentification.

L'AC peut déléguer les fonctions d'AE à un client ou un partenaire via un contrat de délégation d'AE, dans ce cas les fonctions, obligations, et responsabilité de l'AE, incombe à l'AED.

A ce titre, le Client agissant en tant qu'AED assure :

- la prise en compte et la vérification des informations, notamment de données à caractère personnel, présentées par l'Utilisateur, futur Porteur de certificat et la constitution de son dossier d'enregistrement ;
- l'établissement et la transmission de la demande de Certificat de signature à la fonction adéquate de l'AC « be-ys User Signing CA NA » grâce au module client *de signature ou un Service d'enregistrement en ligne*;
- l'archivage des pièces du dossier d'enregistrement ;
- la conservation et protection en confidentialité et en intégrité des données à caractère personnel de l'Utilisateur qui lui sont confiées, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

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

L'AED s'engage également :

- Au maintien opérationnel des moyens lui permettant d'utiliser le module *de signature* ou le Service d'enregistrement en lignemis à sa disposition afin que ce dernier puisse transmettre les demandes de Certificats User Signing,
- Au respect des règles communes d'authentification et de contrôle des flux établies entre l'AE et l'AC « be-ys User Signing CA NA ».

1.3.5. Module client *de signature*

be-invest met à disposition du Client un module de signature ou un Service d'enregistrement en ligne, lequel a la charge de transmettre la demande de génération de Bi-clé et de Certificat si les trois conditions cumulatives suivantes sont réunies :

- Authentification du Client ;
- Validation par le Client (AED) des informations d'identification du futur Porteur de certificat ;
- Double identification du futur Porteur pour accéder au Service de signature électronique en ligne be-invest et validation par le futur Porteur des informations qui lui sont présentées à la signature.

La demande de génération du Bi-clé et du Certificat de l'Utilisateur est effectuée automatiquement auprès des fonctions adéquates de l'AC. be-invest est responsable du bon fonctionnement de son module de signature et de son Service d'enregistrement en ligne ainsi que de leur disponibilité et de l'intégrité des informations transmises par le Client, conformément aux accords contractuels passés avec le Client.

1.3.6. Utilisateur, Porteur de certificat

L'Utilisateur, Porteur de certificat, ne peut être qu'une personne physique représentant le cas échéant une personne morale, à laquelle est remis un Certificat individuel (avec l'identité de l'Utilisateur inscrite dans le Certificat) après contrôle de son identité par l'AE et validation de ses informations par l'AE dans le module de signature ou sur le Service d'enregistrement en ligne.

Le Porteur utilise son Certificat pour signer des informations présentées par le Client qui a fait la demande de Certificat User Signing via le module de signature ou le Service d'enregistrement en ligne.
L'application de signature électronique supporte plusieurs types de format de présentation des informations du Client, et notamment le format PDF (norme ISO 32000).

1.3.7. Applications utilisatrices des certificats

Une Application utilisatrice de certificat est un processus qui exploite les certificats émis par l'AC par exemple un service de vérification d'une signature. Il s'agit donc une application informatique qui est sous la responsabilité d'une personne physique ou morale.

Les applications peuvent être notamment :

- le Service de signature électronique qui permet de présenter les informations devant être signées par l'Utilisateur, ainsi que les informations sur la signature associée ;
- le service de vérification de signature qui permet à partir d'une information ou d'un document signé à l'aide d'un certificat User Signing, de vérifier et d'afficher un statut sur l'état du Certificat utilisé et de la signature ;

1.3.8. Autres participants

Sans objet pour la présente PC.

1.4 USAGE DES CERTIFICATS

1.4.1. Domaines d'utilisation applicables

1.4.1.1. Bi-clés et certificats des porteurs

Le seul domaine d'utilisation applicable de la présente PC pour les Bi-clés et les Certificats User Signing est le Service de signature électronique, grâce auquel l'Utilisateur peut signer les formulaires ou documents présentés par le Client.

Remarque : la présentation des documents ou des informations à signer peut-être à la charge du Client ou être déléguée à be-invest par le Client.

Cependant, les processus de génération de Certificat et de Bi-clé de signature sont, soit sous la charge be-invest, soit sous celle d'une AE ou d'une AED et cela quel que soit le contexte du Client. Les processus de vérification de l'identité des Utilisateurs et de gestion des demandes de Certificats et de signatures via le module de signature ou le Service d'enregistrement en ligne sont à l'entière charge du Client (AED).

1.4.1.2. Bi-clés et certificats d'AC

Les Bi-clés et Certificats de l'AC « be-ys User Signing CA NA » ne peuvent être utilisés que pour la signature de Certificats User Signing et de LCR.

1.4.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des Bi-clés et des Certificats sont définies au chapitre 4.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par ses Porteurs et ses Applications utilisatrices de Certificats.
A cette fin, elle communique à tous les Porteurs et Applications utilisatrices de certificat potentiels les termes et conditions relatives à l'utilisation du Certificat.

1.5 GESTION DE LA PC

1.5.1. Entité gérant la PC

L'entité en charge de l'administration et de la gestion de la politique de certification est l'AG. Elle 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
Email : gouvernance.igc@be-ys.com

be-invest – 17 rue Léon Laval –
L-3372 LEUDELANGE LUXEMBOURG

1.5.3. Entité déterminant la conformité des pratiques avec cette PC

Afin de déterminer la conformité des pratiques de l'AC avec la présente PC, l'AG s'appuie sur les ressources internes ou externes be-invest spécialisées dans l'audit et l'évaluation de la sécurité des services et des produits. Un document interne précise, au sein de l'organisation be-invest, l'entité qui assure cette responsabilité.

Pour les exigences portant sur l'AE, ce sont les Clients qui sont chargés de mesurer l'adéquation de la conformité de ses pratiquesavec la PC, sous réserve que la présente PC lui soit bien communiquée. L'AG peut également demander à auditer l'AE pour mesurer cette conformité ou obtenir auprès des Clients les documents permettant de s'en assurer.

1.5.4. Procédure d'approbation de la conformité des pratiques de l'AC à la PC

L'approbation de conformité des pratiques de l'ACpar rapport à cette PC fait l'objet d'une procédure interne.

1.6 ACRONYMES ET DEFINITIONS

1.6.1. Acronymes

Les acronymes utilisés dans le référentiel de l'IGC be-ys sont les suivants :

AC	Autorité de Certification [Certification Authority (CA)]
AE	Autorité d'Enregistrement [Registration Authority (RA)]
AH	Autorité d'Horodatage [Time-stamping Authority (TA)]
AG	Autorité de Gouvernance [Governance Authority (GA)]
ANSSI	Agence nationale de la sécurité des systèmes d'information
CC	Critères Communs [Common Criteria (CC)]
CEN	Comité Européen de Normalisation
CSP	Cryptographic Service Provider
DN	Distinguished Name
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés [Public Key Infrastructure (PKI)]
KC	Cérémonie des clés (Key Ceremony)
LAR	Liste des certificats d'AC Révoqués [Authority Revocation List]
LCR	Liste des Certificats Révoqués [Certificate Revocation List (CRL)]
OC	Opérateur de Certification [Certification Operator (CO)]
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification [Certification Policy (CP)]
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure – X.509
PP	Profil de Protection [Protection Profile (PP)]
PSCE	Prestataire de Services de Certification Electronique
RAE	Responsable d'Autorité d'Enregistrement
RSA	Rivest Shamir Adelman
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

1.6.2. Définitions

Les termes utilisés dans le référentiel de l'IGC be-ys sont les suivants :

Applications utilisatrices :
Services applicatifs exploitant les Certificats émis par l'AC « be-ys User Signing CA NA »,

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

Autorité de Certification (AC) :
Entité qui délivre et est responsable des Certificats électroniques émis et signés en son nom conformément aux règles définies dans la PC ainsi qu'aux pratiques de l'AC..
Dans le cadre de la présente PC, il s'agit de l'AC « be-ys User Signing CA NA ».

Autorité de Certification Racine (ACR) :
Entité qui dispose d'une IGC lui permettant d'enregistrer, de générer, d'émettre et de révoquer des Certificats d'AC (dont l'AC « be-ys User Signing CA NA »), conformément à la PC définie par son AG ainsi qu'aux pratiques de l'AC. L'ACR be-ys est auto-certifié, c'est-à-dire que son certificat est auto-signé.
L'ACR be-ys est l'AC « Almerys Root CA ».

Autorité d'Enregistrement (AE), :
Entité disposant d'un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC et les Porteurs de certificat conformément au paragraphe 1.3.4 de la présente PC.
L'AE a pour rôle de vérifier l'identité du futur Porteur de certificat.
Dans le cadre de la présente PC, l'AE est le Client du service de signature électronique be-ys. Pour assurer les demandes de génération de Bi-Clés et de Certificats pour ses Utilisateurs, elle s'authentifie et communique les informations nécessaires aux fonctions adéquates de l'IGC via le module de signature ou le Service d'enregistrement en ligne mis à sa disposition dans le cadre de la fourniture de son Service de signature électronique.

Autorité d'Enregistrement Déléguée (AED) : 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. L'AED a notamment pour rôle de vérifier l'identité du futur Porteur de Certificat.

Autorité de Gouvernance (AG) :
Entité responsable de l'ensemble des fonctions de l'IGC 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**. Le Bi-clé de ce Certificat doit être généré avec toutes les précautions nécessaires pour éviter sa compromission.

Certificat électronique :
Fichier électronique attestant qu'un Bi-clé appartient à la personne physique ou morale ou à l'élément matériel identifié, directement ou indirectement (pseudonyme), dans le Certificat. Il est délivré par une AC. En signant le Certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel et le Bi-clé. Le Certificat est valide pendant une durée donnée précisée dans celui-ci.

Dans le cadre de la présente PC, le Certificat désigne un Certificat de signature électronique à usage unique ou réutilisable délivré pour une personne physique représentant le cas échéant une personne morale.

Chiffrement :
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-ys, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des Utilisateurs. Dans le cadre de la présente PC, le Client joue le rôle de l'AED et gère les demandes de Certificats User Signing des Utilisateurs qu'il transmet aux fonctions adéquates de l'IGC via le module de signature Client ou le Service d'enregistrement en ligne mis à sa disposition par be-ys.

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

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

Horodatage :
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 mandataires de certification, d'une entité d'archivage, d'une entité de publication…

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

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

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

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

Non-répudiation :

Impossibilité pour un Porteur ou un Utilisateur de nier sa participation à un échange d'information ; cette participation porte tant sur l'origine de l'*information* (*imputabilité*) que sur son contenu (*intégrité*).

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

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

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

Politique de Certification (PC) :
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 :
Un Porteur de certificats ne peut être qu'une personne physique.
Il s'agit de l'Utilisateur qui doit respecter les conditions qui lui incombent définies dans la présente PC et dans les CGUs.

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).

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

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

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

Transaction de signature :

Période de courte durée (une quinzaine de minutes) pendant laquelle un Utilisateur dûment identifié peut signer électroniquement les documents qui lui sont présentés par le Service de signature électronique.

Utilisateur :
Personne physique, utilisatrice d'un service mis à disposition par un Client et notamment du Certificat à usage unique.
L'identification et l'authentification de l'Utilisateur sont à la charge du Client (rôle d'AE).

Voir également Porteur de certificat.

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

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Pour la mise à disposition des informations devant être publiées à destination des Porteurs et des Applications utilisatrices de certificats, l'AC « be-ys User Signing CA NA » 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 plusieurs liens HTTP. Les adresses de publication sont fournies dans la section 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ».

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

L'AC « be-ys User Signing CA NA » diffuse les informations suivantes :

- la présente PC, qui contient en particulier les profils de certificat et de LCR, les délais et fréquences de publication, le glossaire qui contient les acronymes et les définitions applicables, les adresses principales de diffusion ;
- les Certificats en cours de validité des AC de la hiérarchie de rattachement de l'AC User Signing, les différentes PC correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'ACR ;
- la liste des références de Certificats révoqués de signature des Porteurs et des AC ;
- les formulaires nécessaires pour la gestion des Certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.) ;
- les conditions générales d'utilisation des Certificats.

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

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Pour la PC, la publication est effective dès que nécessaire afin d'assurer, à tout moment, la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

Pour les certificats d'AC, ils sont diffusés préalablement à toute émission de Certificats et/ou de LCR correspondants sous un délai de 72 heures après la génération du certificat.

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

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

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

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

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'AC « be-ys User Signing CA NA », et aux personnes dûment autorisées.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1. Type de noms

Les noms utilisés dans les Certificats de signature émis par l'AC « be-ys User Signing CA NA » sont conformes aux spécifications de la norme X.500.
Dans chaque Certificat X.509v3, l'AC émettrice (issuer) et le Porteur (subject) sont identifiés par un « Distinguish Name » DN dont le format est précisé dans la section 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ».

3.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les Utilisateurs, Porteurs de certificats de signature, sont explicites :

- l'attribut CN du champ subject DN de l'Utilisateur est construit à partir des nom et prénom de l'Utilisateur et d'une référence unique propre à une Transaction de signature. Ces éléments sont présentés dans la demande de Certificat effectuée par le Client via le module de signature ou le Service d'enregistrement en ligne; le prénom correspond au premier prénom de l'état civil du porteur (tel que inscrit dans la pièce d'identité du porteur, il n'y a pas d'obligation à mentionner les autres prénoms dans le certificat, mais s'ils le sont, ils doivent l'être dans le même ordre que sur la pièce d'identité), suivi d'un espace, suivi au choix du nom de famille, ou du nom d'usage figurant sur la pièce d'identité du porteur.
- les attributs O et OU du champ subject DN identifie le Client ainsi que le service pour lequel le Certificat sera utilisé.

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

3.1.3. Anonymisation ou pseudonymisation des Utilisateurs

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

3.1.4. Règles d'interprétation des différentes formes de nom

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

3.1.5. Unicité des noms

Afin d'assurer la continuité d'une identification unique de l'Utilisateur au sein du domaine de l'AC « be-ys User Signing CA NA » et pour éviter toute ambiguïté, le DN du champ « subject » de chaque Certificat d'Utilisateur permet d'identifier de façon unique l'Utilisateur correspondant au sein du domaine de l'AC grâce à la référence unique inscrite dans l'attribut CN du champ subject DN en plus des prénom et nom de l'Utilisateur. Cette référence est le numéro de Transaction de signature calculé par le Service de signature électronique, il est unique et aléatoire. A chaque Transaction de signature est associé un ensemble de données de l'Utilisateur permettant son identification.
Durant toute la durée de vie de l'AC, un DN attribué à un Porteur de certificats 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 à l'Utilisateur et ne permet donc pas d'assurer une continuité de l'identification dans les Certificats successifs d'un Utilisateur donné.

3.1.6. Identification, authentification et rôle des marques déposées

Les nom et prénom sont présentés par l'Utilisateur lors de son enregistrement auprès de l'AE (i.e. le Client).
En cas de litige sur l'interprétation de ces paramètres, une résolution amiable des conflits est privilégiée.

De la même manière, les éventuelles étapes d'authentification permettant au Client de rapprocher des éléments d'authentification ou de sur-authentification à des éléments d'identification sont à la charge du Client.

3.2 VALIDATION INITIALE DE L'IDENTITE

L'enregistrement d'un Utilisateur se fait directement auprès de l'AE.
Les modalités pratiques de validation de l'identité de l'Utilisateur sont déterminées par le Client. Les seuls éléments d'identité qui doivent être transmis à l'AC dans la requête de Certificat via le module de signature ou le Service d'enregistrement en ligne sont les nom et prénom de l'Utilisateur.

3.2.1. Méthode pour prouver la possession de la clé privée

La clé privée de signature de l'Utilisateur est stockée de manière sécurisée par le Service de stockage sécurisé des Bi-clés des Utilisateurs be-ys (cf. §1.3.3 « Service de stockage sécurisé des Bi-clés des Utilisateurs »). Les modalités de vérification de la possession de la clé privée par l'Utilisateur dépendent des méthodes d'enregistrement et d'activation de la clé privée par l'Utilisateur. Ces modalités sont explicitées, pour chaque Client, dans les conditions particulières d'utilisation du Service de signature électronique acceptées par les parties. En effet, les moyens mis en œuvre pour effectuer cette vérification peuvent varier en fonction du contexte Client, et un choix est effectué parmi les modalités proposées par le Service de signature électronique be-ys.

3.2.2. Validation de l'identité d'un organisme

Sans objet dans le cadre de la présente PC.

3.2.3. Validation de l'identité d'un individu

La validation de l'identité d'un Utilisateur est à la charge du Client. Les modalités de vérification sont décrites dans le contrat de service entre be-invest et le Client.

3.2.4. Informations non vérifiées de l'Utilisateur

Le choix de la vérification ou non des informations fournies par l'Utilisateur est à la discrétion du Client AED.

3.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée par le Client dans le cadre de ses processus métier.

3.2.6. Critères d'interopérabilité

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 « Almerys Root CA ».

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

Cette section ne n'applique que pour les certificats réutilisables

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.

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

3.3.1. Identification et validation pour un renouvellement courant

Cette section ne n'applique que pour les certificats réutilisables

L'AE doit identifier l'Utilisateur 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.

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

Cette section ne n'applique que pour les certificats réutilisables

Lors des renouvellements, l'AE doit identifier l'Utilisateur selon la même procédure que pour l'enregistrement d'un nouveau porteur,
Une nouvelle procédure de demande de certificat pour le porteur est alors initiée par l'AE

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

3.4.1. Demande faite via les moyens informatiques

3.4.1.1. Par le Porteur

Le Porteur peut demander la révocation de son Certificat lors de l'étape d'acceptation de son Certificat. Cette étape a lieu en ligne au cours de la Transaction de signature électronique : s'il ne valide pas les informations contenues dans son certificat (cf. §4.4.1 « Démarche d'acceptation du certificat »), cela implique la fin de la Transaction de signature et la révocation de son Certificat.

Dans le cadre des certificats réutilisables, le porteur ou le demandeur du certificat peut demander la révocation de son certificat en contactant le service de gestion des demandes de révocation de l'AE à laquelle il est rattaché

Il peut également contacter le service de l'AC disponible 24H/24 et 7j/7 et suivre la procédure associée, tel qu'indiqué sur la page web publique en utilisant les liens suivants :
http://pki.be-ys.com/revoquer.html ou http://pki.almerys.com/revoquer.html.

3.4.1.2. Par le responsable du service de signature électronique

Sans objet dans le cadre de la présente PC.

3.4.2. Demande faite via Service support

Sans objet dans le cadre de la présente PC.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1. Origine d'une demande de certificat

Un Certificat ne peut être demandé que par un Client (AE) au nom d'un Utilisateur dans le cadre d'un service ou processus métier qu'il propose à ses Utilisateurs.

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

L'établissement de la demande de Certificat est effectué par le Client (AE) via le module client de signature ou le Service d'enregistrement en ligne mis à sa disposition, lequel transmet automatiquement la demande, si elle est correcte, à la fonction adéquate de l'IGC.

La connexion établie entre le système d'information du Client et celui de be-ys est sécurisée grâce à un système d'authentification mutuelle, basée sur l'utilisation de Certificats électroniques, qui permet d'identifier les parties, de chiffrer le canal de communication, et de faire des vérifications d'intégrité des flux échangés.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

La vérification de l'identité de l'Utilisateur est un prérequis indispensable à toute demande de Certificat ; les modalités de cette vérification étant laissées à la discrétion du Client, en fonction de son contexte métier.

Une fois le processus d'identification validé, le Client peut procéder à une demande de Certificat et de Signature via le module de signature Client ou le Service d'enregistrement en ligne qui comprend, au minimum les informations suivantes :

- les nom et prénom de l'Utilisateur,
- une référence unique et associée à la Transaction de signature,
- les données d'identification du Client
    - complétées par la validation du profil de Certificat d'authentification du module de signature client mis à sa disposition pour se connecter à la plate-forme de signature électronique, et qui comprend lui-même des éléments d'identification du Client, ou par la validation de la requête reçue du portail de gestion du Service de signature électronique ;
    - d'autre part, il est indispensable de fournir des données d'identification qui permettront de mettre en œuvre une identification à 2 facteurs
- les informations ou documents qui devront être signés par l'Utilisateur,
- des informations de contexte et de configuration propres à l'interface de programmation utilisée et aux options choisies par le Client.

4.2.2. Acceptation ou rejet de la demande

A réception du flux de demande de Certificat et de signature, l'AC « be-ys User Signing CA NA » :

- vérifie que le Client est enregistré et habilité à émettre des demandes,
- les éléments fournis sont complets et intègres, et en cas de succès, transmet la demande de Certificat proprement dite à la fonction de l'AC chargée de la génération des clés et des Certificats des Utilisateurs.

4.2.3. Durée d'établissement du certificat

La durée d'établissement des Certificats est maîtrisée, et compte tenu de la spécificité des processus synchrones de signature mis en œuvre par la plupart des Clients, l'AC vise une durée d'établissement la plus courte possible.

A titre d'information, l'AC fournit les temps moyens constatés d'établissement de Certificats.

4.3 DELIVRANCE DU CERTIFICAT

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

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE via le module de signature Client ou le Service d'enregistrement en ligne, l'AC déclenche le processus de génération de la Bi-clé et du Certificat de signature de l'Utilisateur.

Le Certificat a une durée de vie maximale définie dans le chapitre « Profil du certificat User Signing » qui détaille le format utilisé par l'AC pour ce type de Certificats.

Le Bi-clé et le Certificat sont alors stockés par le Service de stockage sécurisé. La section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques » précise les caractéristiques des modules utilisés pour générer et stocker la Bi-clé de signature.

Le Certificat, ou les informations sur le certificat, est présenté à l'Utilisateur lors de la présentation des informations ou des documents signés grâce à son Certificat.

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

L'AC « be-ys User Signing CA NA » renvoie au Client un statut sur l'opération de certification.

En cas de succès, le Certificat peut être remis au Client de manière indépendante, via le flux établi entre le Client et le service de signature ou le Service d'enregistrement en ligne.

Le Certificat est mis à disposition en tant qu'élément de preuve pouvant être intégré dans le dossier de preuve associé à la transaction de certification et de signature initiée par le Client et constitué par be-ys.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1. Démarche d'acceptation du certificat

L'acceptation du Certificat par l'Utilisateur est explicite : les informations du Certificat lui sont présentées en ligne après consultation des documents ou informations à signer et acceptation des Conditions générales d'utilisation du Service :

- En cas d'acceptation, le Certificat et la Bi-clé de signature de l'Utilisateur sont utilisés pour signer les documents ou informations présentés par le Client ;
- En cas de refus, la Transaction de signature est annulée si une transaction a été initiée et le Certificat de l'Utilisateur est révoqué.

Dans le cadre des certificats réutilisables, l'AED peut implémenter un processus différent avec l'accord de l'AC.

Les informations minimales du Certificat présentées à l'Utilisateur sont les données à caractère personnel contenues dans le certificat, i.e. ses prénom et nom contenus dans le champ CN, ainsi que les dates de début et de fin de validité du certificat.

4.4.2. Publication du certificat

Les Certificats de signature ne sont pas publiés.

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

L'AC « be-ys User Signing CA NA » informe l'AE de la délivrance du Certificat. Cf. section 4.3.2 « Notification par l'AC de la délivrance du certificat ».

4.5 USAGES DE LA BI-CLE ET DU CERTIFICAT

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

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

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

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

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

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

Cf. chapitre précédent et sections 1.4 « Usage des certificats » et 1.3.7 « 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.

4.6 RENOUVELLEMENT D'UN CERTIFICAT

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

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

Dans le cadre des certificats réutilisables, un changement de Bi-clé peut être effectué suite à une révocation du Certificat existant (voir article. "Révocation et suspension des certificats") ou lors de l'expiration du certificat du porteur.

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

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

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

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

Voir : « Origine d'une demande de certificat »

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

Dans le cadre des certificats réutilisables, la procédure de traitement d'un nouveau certificat suite à un changement de bi-clé est la même qu'un nouveau certificat. Un dossier d'enregistrement complet devra être fait par l'AE pour l'utilisateur

4.7.4. Notification de l'établissement du nouveau certificat

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

4.7.5. Démarche d'acceptation du nouveau certificat

Voir section 4.4.1 « Démarche d'acceptation du certificat »

4.7.6. Publication du nouveau certificat

Voir section 4.4.2 « Publication du certificat »

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

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

4.8 MODIFICATION DU CERTIFICAT

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

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

L'AC « be-ys User Signing CA NA » ne met pas en œuvre de processus de suspension ses certificats

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats de Porteurs

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

- les informations du Porteur figurant dans son certificat ne sont pas en conformité avec son identité,
- un problème technique a lieu lors de la transaction de signature électronique, et le service de signature révoque le certificat dans le cadre de la suppression de la transaction ;
- le Certificat de signature de l'AC « be-ys User Signing CA NA » est révoqué (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante).
- Le Porteur ou une entité autorisée demande la révocation du Certificat
- Le porteur a perdu son moyen d'authentification
- Le moyen d'authentification du Porteur est compromis ou n'est plus maintenu sous le contrôle exclusif du porteur
- L'AED cesse ses activités

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC « be-ys User Signing CA NA » en a connaissance, les Certificats concernés sont révoqués.

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 User Signing CA NA » pour la génération de Certificats, de LCR et/ou de réponses OCSP) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC ;
- cessation d'activité de l'entité opérant la composante ;
- révocation du certificat de l'ACR.

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats de Porteurs

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

- le Porteur, s'il constate que les données de son Certificat ne sont pas conformes à son identité,
- l'AC « be-ys User Signing CA NA », émettrice du Certificat.
- L'AED pour les certificats dont elle a validé l'identité des porteurs

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 de Porteur

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

A l'initiative du Porteur (cf. §4.9.2 « Origine d'une demande de révocation »), le Service de Signature électronique transmet la demande de révocation à la fonction de gestion des révocations de l'AC User Signing. La demande de révocation de Certificat comprend au minimum :

- l'identification du Certificat concerné via au minimum :
  - son numéro de série,
  - l'identification de l'émetteur (champ DN de l'émetteur du certificat),

Une fois la demande contrôlée, la fonction de gestion des révocations de l'AC « be-ys User Signing CA NA » révoque le Certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via le mécanisme de Liste de Certificats Révoqués (LCR) mis en œuvre par l'AC « be-ys User Signing CA NA ».

Le Porteur, demandeur de la révocation, est informé en ligne du bon déroulement de l'opération et de la révocation effective du Certificat. Cette révocation met fin à la Transaction de signature, et il est redirigé vers la page d'accueil du Service de signature en ligne.

L'opération est enregistrée dans les journaux d'événements.
Les causes de révocation des Certificats ne sont pas publiées.

Ce processus ne s'applique pas aux demandes de révocation dont l'origine est l'AC ou l'AED.

4.9.3.2. 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, il doit formuler sa demande de révocation sans délai.

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

4.9.5.1. Révocation d'un certificat de Porteur

Dans le cas du Service de signature électronique, la demande de révocation émise par le Porteur est traitée immédiatement dans un flux de communication synchrone entre le Service de signature ou le Service d'enregistrement en ligne et la fonction de révocation de l'AC « be-ys User Signing CA NA ».
La demande de révocation est donc traitée en quelques secondes. La fonction de révocation doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme aux engagements contractuels établis entre be-invest et le Client.

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, de LCR / LAR et/ou de réponses OCSP) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

L'application utilisatrice d'un Certificat de 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.

4.9.8. Délai maximum de publication d'une LCR

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

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

be-invest 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 via internet.
Les résultats retournés par l'OCSP et les LCR sont consistants modulo les délais de publication des LCRs.

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

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

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

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

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.

4.9.13. Causes possibles d'une suspension

Sans objet pour la présente PC.

4.9.14. Origine d'une demande de suspension

Sans objet pour la présente PC.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet pour la présente PC.

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

Sans objet pour la présente PC.

4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.10.1. Caractéristiques opérationnelles

L'AC fournit aux Applications utilisatrices de certificats de signature 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 et 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 [RFC3280], 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 be-invest et le Client.

4.10.3. Dispositifs optionnels

Sans objet pour la présente PC.

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

Cette section s'applique uniquement aux certificats de signature électronique réutilisables.
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 SEQUESTRE DE CLE 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 pour la présente PC.

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

Sans objet pour la présente PC.

5. MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

Le Responsable de l'AC « be-ys User Signing CA NA » s'engage à mettre en œuvre et maintenir le niveau de sécurité physique exigé pour les locaux d'exploitation des composantes de l'IGC.

5.1.1. Situation géographique et construction des sites

En fonction de la sensibilité des composants de l'IGC interne be-ys, les sites sont définis au niveau 1 de la politique de sécurité : 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 la climatisation ;
- la vulnérabilité aux dégâts des eaux ;
- la prévention et la protection incendie.

Les mesures permettent également de respecter les engagements pris dans la PC ou dans les engagements contractuels avec les Clients du service de signature électronique, 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 User Signing CA NA », 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 de l'Utilisateur, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. De plus, le contrôle en entrée et en sortie est permanent en heures non ouvrées (HNO).
Chaque entrée et sortie dans la zone sécurisée fait l'objet d'une surveillance indépendante et d'une traçabilité. Tout personnel non-autorisé doit obligatoirement être accompagné d'une personne autorisée.
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 est possible 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 User Signing CA NA » telles que fixées par leurs fournisseurs.

Elles respectent également les exigences du cahier des charges fourni par le prestataire des services, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des Certificats.

5.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection mis en place par l'AC be-ys User Signing CA NA permettent de protéger son infrastructure contre les dégâts des eaux.

5.1.5. Prévention et protection incendie

L'AC be-ys User Signing CA NA 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 User Signing CA NA » sont traités et conservés conformément aux besoins de sécurité définis 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 be-invest.

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 SECURITE PROCEDURALES

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

5.2.1. Rôles de confiance

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

- Officier de Sécurité de l'IGC (PKI Security Officer) – L'Officier de Sécurité est chargé de la mise en œuvre de la politique de sécurité de l'AC « be-ys User Signing CA NA ». Il gère les contrôles d'accès physiques aux équipements des systèmes de l'entité. Il est habilité à prendre connaissance des documents conservés au niveau de l'OC, et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- Responsable d'application – Le responsable d'application est chargé, au sein de la composante de l'IGC concernée, de la mise en œuvre des différentes PC de l'AC « be-ys User Signing CA NA ». Sa responsabilité couvre l'ensemble des fonctions rendues par les applications et des performances correspondantes.

- Ingénieur système – Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'entité. Il assure l'administration technique des systèmes et des réseaux de l'entité. Il est également chargé des opérations de restauration.
- Opérateur – Un opérateur au sein de la composante de l'IGC concernée réalise, dans le cadre de ses attributions, l'exploitation des applications pour les services délivrés par la composante de l'IGC.
- Contrôleur – Personne désignée par le responsable de la composante de l'IGC et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des services fournis par la composante de l'IGC par rapport aux PC « be-ys User Signing CA NA ».
- Opérateur d'enregistrement – Personne responsable pour vérifier les informations nécessaires à la délivrance d'un certificat et approuver les demandes de certificat.
- Opérateur de révocation – Personne responsable pour toutes les opérations de changement d'un statut de certificat.

5.2.2. Nombre de personnes requises par tâches

Une procédure interne à l'IGC décrit 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 clé.

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.

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 conformes à la Politique de Sécurité be-invest.
Pour les différents rôles de confiance, il est recommandé qu'une même personne ne détienne pas plusieurs rôles et les cumuls suivants sont interdits :

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

5.3 ESMESURES DE SECURITE VIS-A-VIS DU PERSONNEL

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé de l'AC « be-ys User Signing CA NA ».

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 User Signing CA NA » doit informer 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 acceptée par écrit par la personne nommée dans un rôle de confiance.

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

5.3.2. Procédures de vérification des antécédents

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

5.3.3. Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, au sein de la composante de l'IGC dans laquelle il opère.
Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4. Exigences et fréquence en matière de formation continue

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

5.3.5. Fréquence et séquence de rotation entre différentes attributions

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

5.3.6. Sanctions en cas d'actions non autorisées

Des sanctions appropriées sont appliquées au personnel qui ne respecterait pas les procédures et politiques de sécurité applicables.
La présente PC ne prévoit pas d'exigences spécifiques à ce sujet.

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

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

5.3.8. Documentation fournie au personnel

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

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'événements consiste à enregistrer des événements sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.
Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1. Type d'événements à enregistrer

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

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

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,
- validation / rejet d'une demande de Certificat,
- événements liés aux clés de signature et aux Certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...),

- publication et mise à jour des informations liées à l'AC (PC, Certificats d'AC, conditions générales d'utilisation, etc.),
- génération des Certificats des Porteurs,
- transmission des Certificats aux Porteurs et aux Clients,
- génération puis publication des LCR.

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 :

- demandeur et destinataire de l'opération (dans la mesure du possible),
- 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 d'alerter les personnels de l'occurrence potentielle d'événements critiques de sécurité.

5.4.3. Période de conservation des journaux d'événements

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

5.4.4. Protection des journaux d'événements

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

5.4.5. Procédure de sauvegarde des journaux d'événements

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

5.4.6. Système de collecte des journaux d'événements

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

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

La présente 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 User Signing CA NA » en conformité avec la Politique de Sécurité be-invest.

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 be-invest dans une période de 48 heures après sa découverte. Selon le résultat de son analyse, be-invest :

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

5.5 ARCHIVAGE DES DONNEES

5.5.1. Types de données à archiver

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

Les données à archiver sont au moins les suivantes :

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

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

5.5.2. Période de conservation des archives

En l'état de la législation et de la réglementation en vigueur (dit le « Règlement Européen sur la Protection des Données »), toute information de type :

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

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

Les durées d'archivage sont les suivantes :

- PC : durée de vie de l'AC,
- documents organisationnels de Cérémonies des clés : durée de vie de l'AC,
- DPC : durée de vie de l'AC,

Les autres informations tels que :

- dossiers de demande de certificat,
- certificats émis par l'AC après expiration,
- dernière LCR émis par l'AC après expiration,
- journaux d'événements après leur génération.

sont conservées par l'AC 7 ans après expiration des Certificats.

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.

5.5.4. Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

5.5.5. Exigences d'horodatage des données

Les Certificats sont datés au moment de leur génération et cette information est archivée avec le Certificat correspondant.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6. Système de collecte des archives

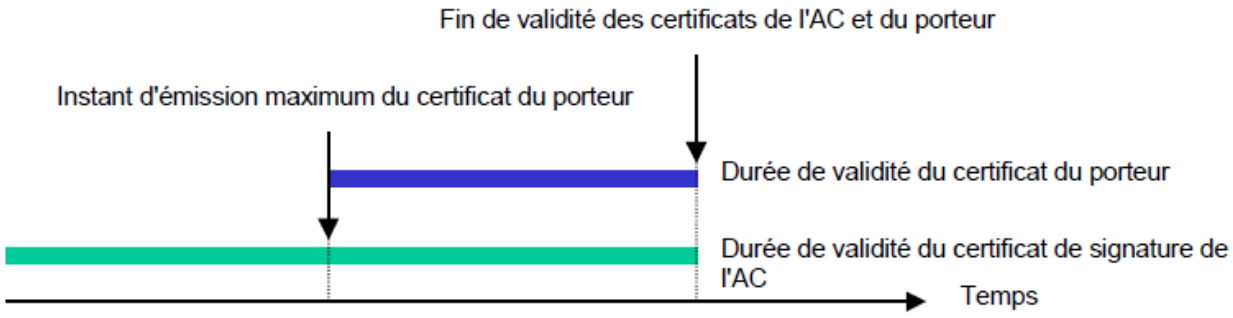
La Politique de Sécurité de l'IGC précise les moyens mis en œuvre pour collecter les archives en toute sécurité.

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 précisé que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 CHANGEMENT DE CLE D'AC

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



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

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

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

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

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

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 User Signing CA NA », l'événement déclencheur est la constatation de cet incident. L'AG de l'IGC be-ys est immédiatement informée. Le cas de l'incident majeur doit être impérativement traité dès sa 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, be-invest notifiera les parties concernées, en particulier l'organe de contrôle et la CNIL, dans les 24 heures après l'identification de l'incident, conformément aux exigences du Règlement eIDAS et, le cas échéant, les clients impactés.

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

Conformément à la Politique de Sécurité be-invest, l'AC « be-ys User Signing CA NA » dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité de ses différentes fonctions, 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 trois (3) ans.

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

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

En particulier, en cas de compromission d'une clé d'AC, be-invest :

- 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, be-invest appliquera les mesures ci-dessus à l'exception de la révocation immédiate de tous les certificats compromis. be-invest 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 be-ys disposent des moyens raisonnablement nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. section 5.7.2 « Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) »).
be-invest dispose d'un plan de continuité d'activité à jour afin de réagir efficacement en cas de désastre et de restaurer le système dans les délais précisé dans ce plan. Ce plan comprend en particulier les cas de compromission de clé privée d'AC ou de perte des moyens d'activation de la clé.

5.8 FIN DE VIE DE L'IGC

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

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

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC be-ys

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC « be-ys User Signing CA NA » s'engage, entre autres obligations, à :

1) 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 Utilisateurs et des informations relatives aux Certificats) ;
2) 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 User Signing CA NA » 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 Porteurs ou des Applications utilisatrices de certificats, l'AC « be-ys User Signing CA NA » doit les en aviser aussitôt que nécessaire et, au moins, sous le délai d'un mois.
2) L'AC « be-ys User Signing CA NA » doit communiquer aux Clients les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux Certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC « be-ys User Signing CA NA » devra communiquer aux Clients les modalités des changements survenus. L'AC « be-ys User Signing CA NA » 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 Porteurs et les Applications utilisatrices de certificats.
3) L'AC « be-ys User Signing CA NA » doit tenir informés les Porteurs de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.
4) be-invest s'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.

Cessation d'activité affectant l'AC « be-ys User Signing CA NA ***»***

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 User Signing CA NA » 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 User Signing CA NA » 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 User Signing CA NA » :

1) détruit la clé privée lui ayant permis d'émettre des Certificats, ainsi que toutes les copies ;
2) prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) révoque son Certificat ;
4) révoque tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;
5) informe (par exemple par récépissé) tous les Porteurs des certificats révoqués ou à révoquer, et/ou le Client des services de signature électronique qui a demandé l'émission de ces Certificats en leur nom.
6) transfert à un tiers l'obligation de disponibilité des informations publiée, en particulier de de sa clé publique

6. MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI-CLES

6.1.1. Génération des bi-clés

6.1.1.1. Clés d'AC

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

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

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

Le script de « Cérémonie des clés » indique :

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

La Cérémonie se fait en présence :

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

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

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

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

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

6.1.1.2. Clés porteurs générées par l'AC

La réception de la requête de Certificat et de signature de la part d'un Client au nom d'un Utilisateur déclenche le processus de création du Bi-clé.

Le Service de stockage sécurisé de Bi-clé de l'AC « be-ys User Signing CA NA » est en charge de la génération des Bi-clés de signature des Porteurs.

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 de l'AC.

Les clés à usage unique sont détruites dans un laps de temps très court, une fois que la Transaction de signature est achevée.

6.1.1.3. Clés porteurs générées par le porteur

Les Utilisateurs, Porteurs des Bi-clés de signature, ne génèrent pas leurs Bi-clés.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée de signature n'est pas transmise à son propriétaire, elle est stockée par le Service de signature électronique.

6.1.3. Transmission de la clé publique à l'AC

La clé publique est transmise à l'AC « be-ys User Signing CA NA » dans la demande de génération de Certificat. La clé est protégée en intégrité et l'origine est authentifiée grâce à l'utilisation d'une enveloppe au format PKCS#10 qui est signée par la clé privée associée à la clé publique.

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

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

6.1.5. Tailles des clés

Les tailles de clés sont les suivantes :

- Certificat de l'AC « be-ys User Signing CA NA » : 4096 bits (algorithme RSA)
- Certificats des Utilisateurs :
  - 2048 bits (algorithme RSA) pour les certificats éphémères
  - 3072 bits (algorithme RSA) pour les certificats réutilisables

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

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

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 / LAR.

L'usage de la clé privée de l'Utilisateur et du Certificat associé est strictement limité au Service de signature (cf. sections 1.4 et 7.2) pour les restrictions dans le format de Certificat User Signing).

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Modules cryptographiques de l'AC

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

6.2.1.2. Dispositifs de création de signature des porteurs

Le dispositif de création de signature des Porteurs est un Module cryptographique matériel certifié FIPS 140-2 niveau 3 ou CC EAL 4+.
Sa configuration opérationnelle minimale est conforme au standard FIPS 140-2 niveau 2.

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

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

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

- pour l'exportation / l'importation hors / dans un module cryptographique : les systèmes sont configurés pour interdire l'exportation en clair de la clé privée, assurant ainsi sa non compromission ;
- pour la génération du Bi-clé (cf. 6.1.1.1) : utilisation d'un module cryptographique matériel sécurisé pour la génération et le stockage de la clé privée, et le partage des secrets assure qu'aucun acteur ne puisse accéder ou interpréter un des secrets ;
- pour l'activation de la clé privée (cf. section 6.2.8) : les flux de requêtes de Certificats et de révocation (mise à jour de la LCR) sont maîtrisés pour s'assurer que seuls les services autorisés puissent être enregistrés ; l'action d'autorisation et de configuration de ces flux nécessite la présence d'au minimum 2 acteurs ayant des fonctions différentes ;
- pour la destruction (cf. section 6.2.10) : les procédures de destruction permettent de s'assurer que personne ne pourra utiliser la clé privée.

6.2.3. Séquestre de la clé privée

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

6.2.4. Copie de secours de la clé privée

Les clés privées des Porteurs ne doivent faire l'objet d'aucune copie de secours par l'AC.

La clé privée d'AC fait l'objet de copies de secours hors des modules cryptographiques sous forme chiffrée et répartie (principe du partage de secrets) 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 de la section 6.2.4.
Les clés privées de signature d'Utilisateur générés par un module cryptographique matériel ne sont jamais exportées.

6.2.7. Stockage de la clé privée dans un module cryptographique

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

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clé privée d'AC

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

6.2.8.2. Clés privées des porteurs

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

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clé privée d'AC

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

6.2.9.2. Clés privées des porteurs

L'Utilisateur ne pourra pas activer la clé privée s'il n'est pas capable de fournir les informations ou de mener à bien les actions qui autorisent l'activation.

La désactivation de la clé a lieu à l'issue de la Transaction de signature par le biais de la destruction du Bi-clé de signature qui est stockée dans le Module cryptographique matériel. Cette destruction a lieu quel que soit l'état final de la transaction.

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

La clé privée de signature d'un Utilisateur est détruite au sein du Module cryptographique qui est en charge de la stocker pour la durée de la Transaction de signature pour laquelle l'Utilisateur a accepté la création d'un Certificat de signature. Cette destruction a lieu à l'issue de la transaction, quel que soit l'état final de la transaction.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

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

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1. Archivage des clés publiques

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

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

Les Certificats des Utilisateurs couverts par la présente PC ont une durée de vie maximum de 3 ans. Les Bi-clés et les Certificats associés ont la même durée de vie

6.4 DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

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

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

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

L'activation de la clé privée de l'Utilisateur est contrôlée via des données ou des actions d'activation propres à l'Utilisateur.

Un Porteur peut obtenir un Certificat de signature User Signing et activer sa clé privée de signature dans le cadre du processus de souscription en ligne mis en œuvre par le Client sous réserve du respect de 2 conditions préalables :

1. La validation de la session (ou Transaction) de signature, établie à l'issue d'une phase d'identification à deux facteurs. Cette identification se base par défaut sur :
    - La fourniture par mail d'une URL personnalisée de signature au Porteur ;
    - L'envoi d'un code à usage unique (OTP) par SMS sur le numéro de téléphone portable du Porteur.

    Note : il est obligatoire de mettre en œuvre deux facteurs d'identification offrant un niveau de sécurité au moins équivalent à celui du processus décrit ci-dessus, mais les modalités d'implémentation peuvent être différentes en fonction du contexte Client.

2. L'action de cliquer sur le bouton « Je signe » lors de la présentation des documents à valider :

    - Permet de générer le Bi-clé de signature du Porteur uniquement pour cette Transaction de signature. Cette Bi-clé est protégé matériellement dans le Module cryptographique matériel conforme au minimum au standard FIPS 140-2 level 2 ou CC EAL4+.

Les données d'identification (par défaut, l'adresse mail et le numéro de téléphone du Porteur) sont transmises au service de signature par le Client qui les a collectés lors de la phase d'enregistrement du Porteur.
L'authentification réussie de la session permet l'activation de la clé privée pour l'action de Signature.

Les méthodes d'enregistrement et d'activation de la clé privée par l'Utilisateur sont explicitées, pour chaque Client, dans les conditions particulières d'utilisation du Service de signature électronique.

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

Les modalités de protection des données d'activation des clés privées des porteurs dépendent de la méthode choisie. Le détail de ces modalités est fourni dans les conditions particulières d'utilisation du service de signature électronique. Dans tous les cas, une identification à deux facteurs est requise pour activer le processus de génération de la Bi-clé et du Certificat de Signature.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini et répond en particulier aux objectifs de sécurité suivants :

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

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle doit être cohérente avec la Politique de Sécurité be-invest.
Pour atteindre ces objectifs de sécurité, be-invest utilise des systèmes et des produits fiables permettant de mettre en œuvre de façon sécurisée 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.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.6.1. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre une fonction de l'IGC be-invest est documentée. La configuration du système des composantes de l'IGC be-invest 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 be-invest 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 be-invest doit être signalée à l'AG pour validation. Elle doit être documentée.
En particulier, be-invest a spécifié et mis-en place des procédures de gestion des mises-à-jour de sécurité, afin que celles-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, be-invest documentera les raisons de non-application d'une mise à jour de sécurité.

6.6.2.2. Analyse de risque

be-invest a réalisé une analyse de risque pour identifier, analyser et évaluer les risques pesant sur l'IGC en prenant en compte les risques techniques et métier. Suite à cette analyse de risque, be-invest 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 be-invest ainsi que dans sa PSSI.

Cette analyse de risque est revue régulièrement, et lors de toute évolution significative d'un système ou d'une composante de l'IGC be-invest.

6.6.2.1. Scan de vulnérabilité

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

6.6.2.1. Test d'intrusion

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

6.7 MESURES DE SECURITE RESEAU

6.7.1. Segmentation en zone

Fondé sur les résultats de l'analyse de risque, be-invest a segmenté son réseau en zone séparées (fonctionnellement, logiquement ou physiquement). Des mesures de contrôle similaires sont mises-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, telles que les AC Racines, sont opérés dans les zones les plus sécurisées.

be-invest 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 garanti 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 be-invest 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.
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'administrer 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, be-invest a mis en place des mesures de redondances permettant d'offrir une haute disponibilité des services critiques.

6.8 HORODATAGE / SYSTEME DE DATATION

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

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 PROFIL DU CERTIFICAT DE L'AC « BE-YS USER SIGNING CA NA »

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

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		3
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 (référentiel temporel de l'AC)
← notAfter		notBefore + 10ans
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		2.5.4.97 = VATLU-LU29222134 CN = BE-YS USER SIGNING CA NA O = BE INVEST International S.A. C = LU
subjectPublicKeyInfo		
← algorithm ⮡ algorithm ⮡ parameters		 rsaEncryption (OID = 1.2.840.113549.1.1.1) RSAParams : NULL
← subjectPublicKey		DER encoded RSAPublicKey (4096 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
← authorityKeyIdentifier	Non	hache de la clé publique de l'issuer
← subjectKeyIdentifier	Non	hache de la clé publique du sujet
← keyUsage	Oui	keyCertSign (5), cRLSign (6)
← privateKeyUsagePeriod		Extension non utilisée
← certificatePolicies		Stratégie du certificat : Identificateur de stratégie =

		1.3.6.1.4.1.48620.41.1.4.1.1
← basicContraints ⮡ cA ⮡ pathLenConstraint	Non	 false None
← cRLDistributionPoints	Non	[1]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almerysrootca.cr
Private extensions		
← authorityInfoAccess		[1] : accessMethod : id-ad-caIssuers accessLocation : URL=http://pki.almerys.com/almerysrootca.cer
← subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption,clé de 4096 bits
parameters		NULL

7.2 PROFIL DU CERTIFICAT USER SIGNING

Le tableau suivant fournit les valeurs par défaut des attributs d'un Certificat User Signing émis par l'AC « be-ys User Signing CA NA ».
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. Profil du certificat

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
← algorithm		Sha256withRSAEncryption
← parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		2.5.4.97 = VATLU-LU29222134 CN = BE-YS USER SIGNING CA NA O = BE INVEST International S.A. C = LU
Validity		
← notBefore		Date de création (référentiel temporel de l'AC)
← notAfter		notBefore + durée [1]
subject GN=givenName SN=surName CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ${Prénom usuel} ${Nom usuel} SerialNumber = UI:LU-<${ID} [2]> GN = ${Prénom usuel} SN = ${Nom usuel} OI = NTR<codepays>- ${SIREN ou equivalent} OU =${ organisation unit} O = ${Client} C = <code pays>
subjectPublicKeyInfo		
← algorithm ➥ algorithm ➥ parameters		 rsaEncryption (OID = 1.2.840.113549.1.1.1) RSAParams : NULL
← subjectPublicKey		DER encoded RSAPublicKey (**2048 bits ou 3072 bits**)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
← authorityKeyIdentifier	Non	hache de la clé publique de l'issuer
← subjectKeyIdentifier	Non	hache de la clé publique du sujet
← keyUsage	Oui	nonRepudiation (1)
← privateKeyUsagePeriod		Extension non utilisée
← certificatePolicies		Stratégie du certificat :

		Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.4.1.1.1.1
← basicContraints ⮑ cA ⮑ pathLenConstraint	Non	 false None
← cRLDistributionPoints	Non	[1]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=https://pki.almerys.com/be-ysusersigningcana.crl
Private extensions		
← authorityInfoAccess	Non	[1] : accessMethod : id-ad-caIssuers accessLocation : URL=https://pki.almerys.com/be-ysusersigningcana.cer
← subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption clé de 4096 bits
parameters		NULL

[1] La durée de vie du certificat est déterminée de la manière suivante :

- 24 heures maximum pour un Certificat à usage unique
- 3 ans maximum pour un Certificat réutilisable

[2] Variables de l'attribut subject DN :

- $ {Nom usuel} ${Prénom usuel} = nom et prénom de l'Utilisateur
- ${ID} = identifiant unique et aléatoire de Transaction de signature. Des contraintes sur le format de cet identifiant peuvent être imposées par l'AC.
- ${Service} = service proposé aux Utilisateurs par le Client, et pour lequel le Certificat est utilisable
- ${SIREN} = SIREN du Client
- ${Client} = raison sociale du Client

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

tbsCertList		Valeur
version		1 (c'est-à-dire version2)
signature		
← algorithm		Sha256withRSAEncryption
← parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		OI = VATLU-LU29222134 CN = BE-YS USER SIGNING CA NA O = BE INVEST International S.A. C = LU
thisUpdate		Date de création (référentiel temporel de l'AC)
nextUpdate		nextUpdate + 72 heures
revokedCertificates		
← userCertificate		n° de série du certificat révoqué
← revocationDate		date de révocation du certificat
← crlEntryExtensions		
↪ reasonCode		unspecified (0) *valeur par défaut*
crlExtensions	Critique :	
← authorityKeyIdentifier	Non	hache de la clé publique de l'issuer
← issuerAltName	-	Extension non utilisée
← cRLNumber	Non	Numéro de séquence de la LCR (incrémental simple).
← deltaCRLIndicator	-	Extension non utilisée
← freshestCRL	-	Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.4 PROFIL CERTIFICAT DE L'OCSP

Sans objet

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.

Dans ce cadre, le Client du service de signature a, quant à lui, la charge des audits et de l'évaluation de l'Autorité d'Enregistrement (AE), en tant que responsable de la gestion de cette AE. Be-invest est donc habilitée, en tant qu'Autorité de Gouvernance de l'AC « be-ys User Signing CA NA », à demander un audit de l'AE, en tout ou partie.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

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

L'AG procède également régulièrement à un contrôle de conformité de l'IGC, en tout ou partie.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

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

8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

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

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

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

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un audit de sécurité, l'équipe d'audit rend à l'AG, un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

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

8.6 COMMUNICATION DES RESULTATS

Les résultats de l'audit ne sont pas communiqués en dehors de l'AG

8.7 AUTRES ELEMENTS DE CONFORMITE

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

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

Les informations suivantes sont fournies dans les différents documents contractuels établis entre les parties : (i.e. be-invest, le Client du service de signature électronique (l'AE), les Utilisateurs du service, et éventuellement les fournisseurs assurant en tout ou partie certaines fonctions de l'AC « be-ys User Signing CA NA » ou de l'AE) :

- les conditions de facturation du service de certification électronique et de signature électronique proposées,
- les responsabilités,
- les responsabilités financières,
- le montant des indemnités.
- l'accès à la fonction sur l'état des certificats n'est pas soumis à tarification.

9.2 RESPONSABILITE FINANCIERE

Cf 9.1 « Tarifs ».

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1. Périmètre des informations confidentielles

La classification des informations se décompose en :

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

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

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

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

- les journaux d'événements des composantes de l'IGC.

9.3.2. Informations hors du périmètre des informations confidentielles

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

9.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire du grand-duché du Luxembourg.

9.4 PROTECTION DES DONNEES A CARACTERE PERSONNEL

9.4.1. Politique de protection des données à caractère personnel

Toutes collectes et tous traitements de données à caractère personnel par l'AE et l'AC « be-ys User Signing CA NA » sont réalisés dans le strict respect de la réglementation en vigueur, et en particulier le règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit « Règlement Général sur la Protection des Données [RGPD].

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les informations d'enregistrement de l'Utilisateur.

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

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

Le Client est responsable du respect de la réglementation en vigueur dite [RGPD].
Le traitement des données à caractère personnel par be-invest est sous la responsabilité de la direction de be-invest international SA. Pour la conformité au [RGPD], be-invest 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 pour la présente PC.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

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

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

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC et les documents qui en découlent,
- respecter et appliquer la partie de la PC 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 Utilisateurs,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1. Autorité de Certification

L'AC « be-ys User Signing CA NA » a pour obligation de :

- pouvoir démontrer aux Applications utilisatrices de ses Certificats qu'elle a émis un Certificat pour un Utilisateur donné et que cet Utilisateur a accepté le Certificat, conformément aux exigences du chapitre 4.4 « Acceptation du certificat » ci-dessus ;
- protéger la clé privée des Porteurs conformément aux exigences de la présente PC ;
- garantir et maintenir la cohérence de la PC avec les pratiques de l'AC.

9.6.2. Autorité de Gouvernance

L'AG est responsable de la conformité de la PC de l'AC « be-ys User Signing CA NA », 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 User Signing CA NA » 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 User Signing CA NA » 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 User Signing CA NA » 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 User Signing CA NA ».

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 User Signing CA NA » ou l'une des composantes de l'IGC. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services.

9.6.3. Autorité d'enregistrement

Outre ses responsabilités décrites dans l'introduction de la section 9.6 et dans les sections 1.3.4 et 4, le Client en tant qu'AE doit :

- conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées ;
- prendre toutes les mesures raisonnables pour s'assurer que les Utilisateurs qui requêtent l'AE sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des Certificats ou encore de l'équipement et des logiciels éventuellement utilisés.

9.6.4. Porteurs de certificats

Le Porteur doit :

- communiquer à l'AE (le Client) des informations exactes et à jour lors de la phase d'identification,
- protéger ses données d'activation de génération du Certificat et de Signature,
- accepter les Conditions Générales d'Utilisation des Certificats User signing.
- 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).

9.6.5. Applications utilisatrices de certificats

Les Applications utilisant les Certificats doivent :

- vérifier et respecter l'usage pour lequel un Certificat a été émis ;
- contrôler que le Certificat émis par l'AC « be-ys User Signing CA NA » 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 User Signing CA NA » émettrice du Certificat en parcourant la chaîne de certification jusqu'à l'ACR « Almerys Root CA » ;
- vérifier et respecter les obligations des Applications utilisatrices de certificats exprimées dans la présente PC ;
- contrôler la validité des Certificats (dates de validité, statut de révocation).

9.6.6. Autres participants

Outre ses responsabilités décrites dans les chapitres 0 et 4, le Service support doit conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées.

9.7 LIMITE DE GARANTIE

Cf 9.1 « Tarifs ».

9.8 LIMITE DE RESPONSABILITE

Cf 9.1 « Tarifs ».

9.9 INDEMNITES

Cf 9.1 « Tarifs ».

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1. Durée de validité

La PC de l'AC « be-ys User Signing CA NA » 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 be-ys peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.
Suite à publication interne au sein de l'AC d'une nouvelle version de la PC AC racine, l'AC « be-ys User Signing CA NA » dispose d'un délai de 1 an pour se mettre en conformité.

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

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

Suite à l'arrêt de l'AC « be-ys User Signing CA NA » et donc à la fin de validité de cette politique, étant donné que le dernier Certificat aura été émis avec une date de fin de validité T_{FIN_VAL}, les exigences des sections suivantes :

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

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

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

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

9.12 AMENDEMENTS A LA PC

9.12.1. Procédures d'amendements

Tout projet de modification de la présente PC doit rester conforme aux exigences de la politique de sécurité de l'IGC be-ys, de la PC de l'ACR et respecter les engagements avec les Utilisateurs existants du service de signature. En cas de changement important, l'AG de l'IGC be-ys 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 précisés dans un document interne de l'IGC .

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 de la PC de l'AC « be-ys User Signing CA NA » étant inscrit dans les Certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les Certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des Utilisateurs, qui ne peuvent donc pas s'appliquer aux Certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les Applications utilisatrices puissent clairement distinguer quels Certificats correspondent à quelles exigences.

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Pour toute demande d'information ou réclamation relative au service Certificats User Signing, 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 COMPETENTES

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

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

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

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

10. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 REGLEMENTATION

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
[RGPD]	Règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[REG_eIDAS]	Règlement européen eIDAS

10.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[ETSI_319411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI_319411-2]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: "Requirements for trust service providers issuing EU qualified certificates"
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - 11/2003
[PROG_ACCRED]	COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance
[CC]	Norme ISO/IEC 15408 : Critères communs version 2.1
[X.509]	Information Technology–Open Systems Interconnection – The Directory: Authentication Framework, Recommendation X.509, version 3
[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
[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 +»